ID: 553366
Sample Name:
GNXG5XLBEH.exe
Cookbook: default.jbs
Time: 19:07:30
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

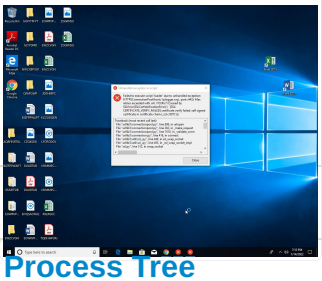
Windows Analysis Report GNXG5XLBEH.exe

Overview

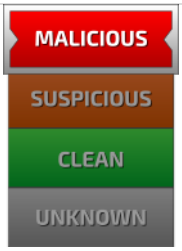
General Information

Sample Name:	GNXG5XLBEH.exe
Analysis ID:	553366
MD5:	6f48e0e76c5dfb3..
SHA1:	981a2937735149..
SHA256:	277ac2c203e37d..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



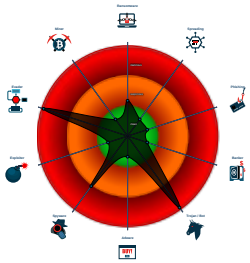
RedLine SmokeLoader Tofsee Vidar

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

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e.…
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Sigma detected: Suspect Svchost A…
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected Vidar stealer

Classification



Process Tree

- **System is w10x64**
- GNXG5XLBEH.exe (PID: 3224 cmdline: "C:\Users\user\Desktop\GNXG5XLBEH.exe" MD5: 6F48E0E76C5DFB3FC3AA45311FA6D0EF)
  - GNXG5XLBEH.exe (PID: 6268 cmdline: "C:\Users\user\Desktop\GNXG5XLBEH.exe" MD5: 6F48E0E76C5DFB3FC3AA45311FA6D0EF)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 5BBC.exe (PID: 6604 cmdline: C:\Users\user\AppData\Local\Temp\5BBC.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 3896 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6604 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 6B9B.exe (PID: 6156 cmdline: C:\Users\user\AppData\Local\Temp\6B9B.exe MD5: 039CCF44EF7B55AEB4D22D211D17774E)
        - 6B9B.exe (PID: 6568 cmdline: C:\Users\user\AppData\Local\Temp\6B9B.exe MD5: 039CCF44EF7B55AEB4D22D211D17774E)
      - 6BA5.exe (PID: 1412 cmdline: C:\Users\user\AppData\Local\Temp\6BA5.exe MD5: 7E58C9178CBD9D56DB805F034EC795CB)
      - BackgroundTransferHost.exe (PID: 240 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
      - 77CC.exe (PID: 5196 cmdline: C:\Users\user\AppData\Local\Temp\77CC.exe MD5: D8DF1D21042865E2220B0D688BAE6DC4)
        - cmd.exe (PID: 5716 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\ceaplexz\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6480 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\evjgtzc.exe" C:\Windows\SysWOW64\ceaplexz\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5984 cmdline: C:\Windows\System32\sc.exe" create ceaplexz binPath= "C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe /d\"C:\Users\user\AppData\Local\Temp\77CC.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2076 cmdline: C:\Windows\System32\sc.exe" description ceaplexz "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 484 cmdline: "C:\Windows\System32\sc.exe" start ceaplexz MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 4864 cmdline: "C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 8058.exe (PID: 5500 cmdline: C:\Users\user\AppData\Local\Temp\8058.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 8058.exe (PID: 5192 cmdline: C:\Users\user\AppData\Local\Temp\8058.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 6632 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6912 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6952 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7024 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7088 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 7156 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5604 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6424 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- ttfssdi (PID: 4512 cmdline: C:\Users\user\AppData\Roaming\ttfssdi MD5: 6F48E0E76C5DFB3FC3AA45311FA6D0EF)
  - ttfssdi (PID: 1284 cmdline: C:\Users\user\AppData\Roaming\ttfssdi MD5: 6F48E0E76C5DFB3FC3AA45311FA6D0EF)
- svchost.exe (PID: 6600 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1064 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6204 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6604 -ip 6604 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- evjgtzc.exe (PID: 4876 cmdline: C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe /d"C:\Users\user\AppData\Local\Temp\77CC.exe" MD5: BBB91EAF2FB4CC1AA911FF4D555EC36D)
  - svchost.exe (PID: 4020 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\6E36.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x3b87:$x1: https://cdn.discordapp.com/attachments/

Memory Dumps

Source	Rule	Description	Author	Strings
0000002B.00000003.399149809.000000000620000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0000001A.00000002.375596550.000000000680000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000002B.00000002.401571286.000000000400000.00000040.00020000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0000002E.00000000.418486488.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000001E.00000002.396801518.000000000210000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.2.6B9B.exe.6415a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
45.2.svchost.exe.2ee0000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
26.0.6B9B.exe.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
30.3.77CC.exe.2190000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
31.2.8058.exe.412f910.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 21 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Svchost Process

Sigma detected: Netsh Port or Application Allowed

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

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 (overwrites its own PE header)

Networking:

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

Uses the Telegram API (likely for C&C communication)

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Found evasive API chain (may stop execution after checking locale)

Checks if the current machine is a virtual machine (disk enumeration)

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Contains functionality to detect sleep reduction / modifications

Found evasive API chain (may stop execution after checking computer name)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Changes security center settings (notifications, updates, antivirus, firewall)

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

Yara detected Tofsee

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

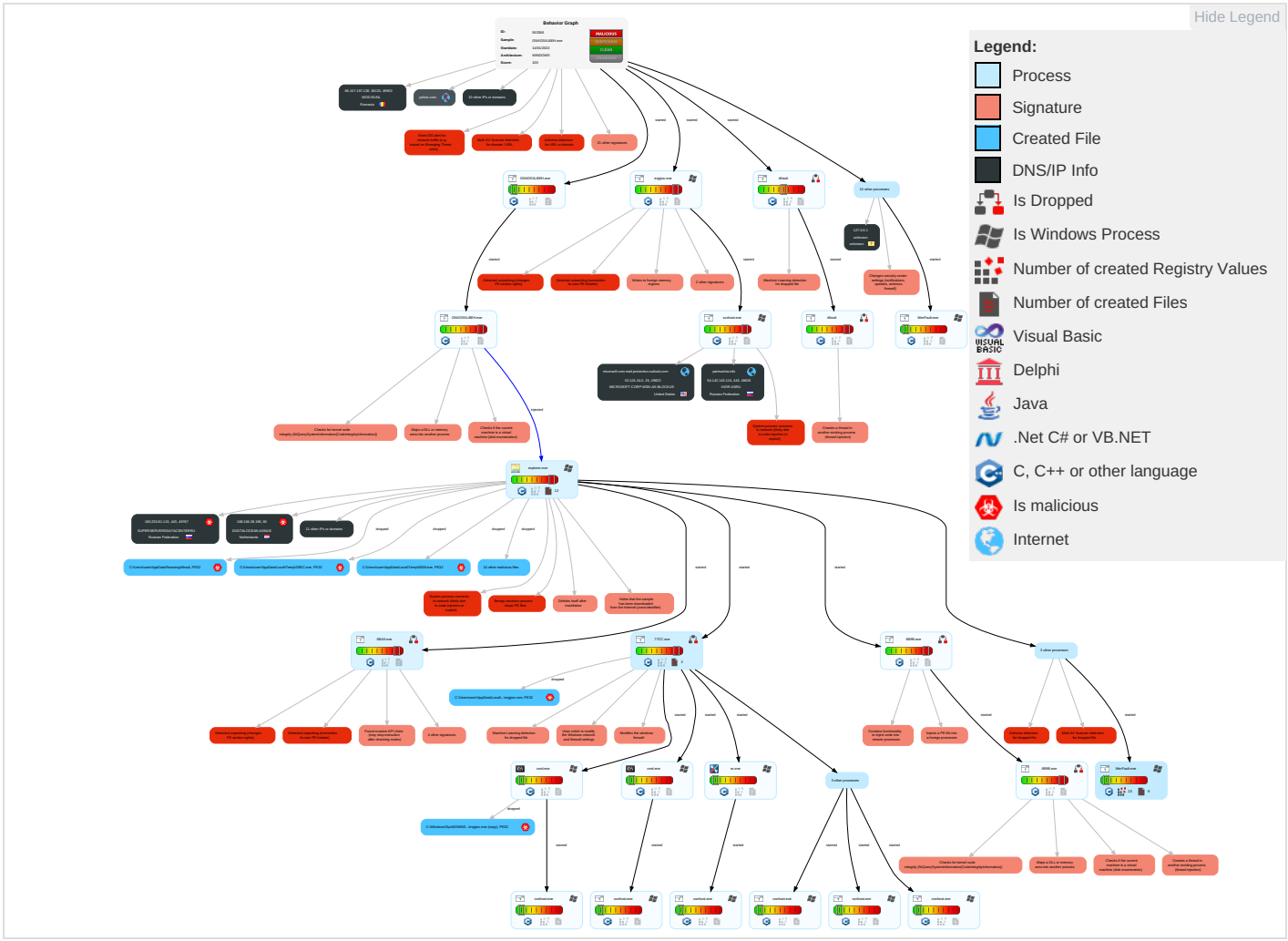
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 3 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Servi
Default Accounts	Native API 5 3 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ingre Trans
Domain Accounts	Exploitation for Client Execution 1	Windows Service 1 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Encr Char
Local Accounts	Command and Scripting Interpreter 3	Logon Script (Mac)	Windows Service 1 4	Software Packing 4 3	NTDS	System Information Discovery 2 3 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non- Port
Cloud Accounts	Service Execution 3	Network Logon Script	Process Injection 7 1 3	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Non- Appli Laye Proto
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 8 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Appli Laye Proto
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Used

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 4 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 4 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

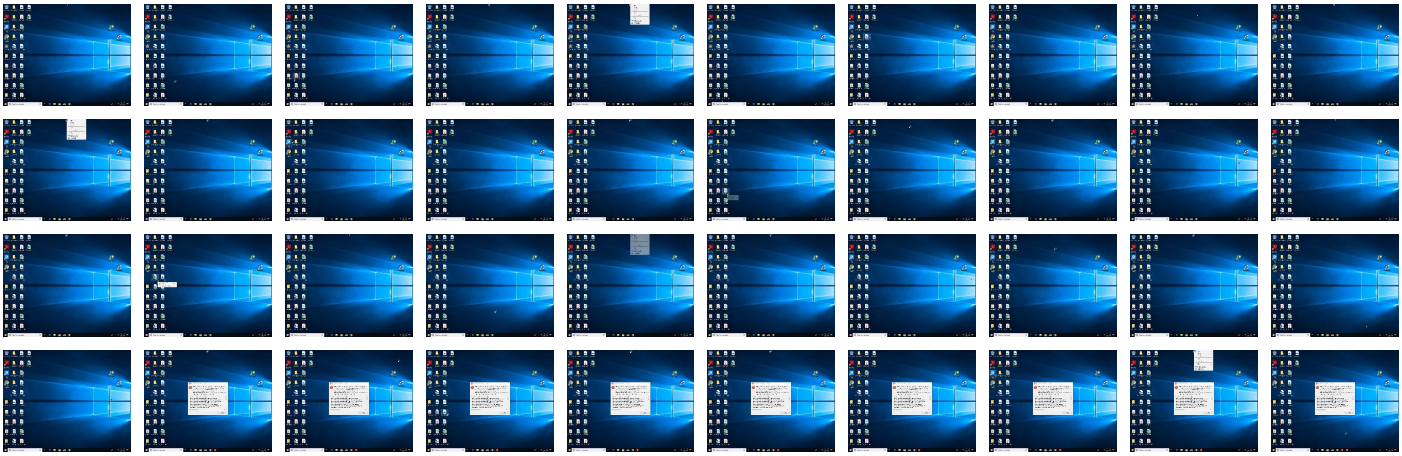
Behavior Graph



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
GNXG5XLBEH.exe	36%	Virustotal		Browse
GNXG5XLBEH.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\8058.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\evjgtzc.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\4955.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\13C.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\8058.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ttfssdi	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\74DE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2205.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5BBC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\77CC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\evjgtzc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1523.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6E36.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D9EC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6B9B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6BA5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6471.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\54D0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2D8F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2205.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2205.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\2D8F.exe	50%	ReversingLabs	Win32.Infostealer.Generic	
C:\Users\user\AppData\Local\Temp\5BBC.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5BBC.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.0.6B9B.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
43.2.evjgtzc.exe.600e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.2.8058.exe.d00000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.0.6B9B.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
26.0.6B9B.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
31.0.8058.exe.d00000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
23.2.6B9B.exe.6415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.6B9B.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.6BA5.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.5BBC.exe.6e0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.5BBC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.8058.exe.d00000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.ttfssdi.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.6B9B.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.2.svchost.exe.2ee0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
30.3.77CC.exe.2190000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.0.5BBC.exe.6e0e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.ttfssdi.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.77CC.exe.2170e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.0.8058.exe.d00000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.1.6B9B.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.1.ttfssdi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.3.evjgtzc.exe.620000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.GNXG5XLBEH.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.6B9B.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
1.0.GNXG5XLBEH.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.ttfssdi.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.5BBC.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.GNXG5XLBEH.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.6BA5.exe.7d0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.2.6B9B.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.2.evjgtzc.exe.660000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
21.0.5BBC.exe.6e0e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
30.2.77CC.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.3.6BA5.exe.7f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.3.5BBC.exe.6f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.ttfssdi.6015a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.GNXG5XLBEH.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.GNXG5XLBEH.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.5BBC.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.ttfssdi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.GNXG5XLBEH.exe.6d15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.8058.exe.d00000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
43.2.evjgtzc.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.0.6B9B.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://81.163.30.181/l2.exe	100%	Avira URL Cloud	malware	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	17%	Virustotal		Browse
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://81.163.30.181/l3.exe	100%	Avira URL Cloud	malware	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dl.uploadgram.me	176.9.247.226	true	false		high
patmushta.info	94.142.143.116	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
ipwhois.app	136.243.172.101	true	false		high
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	8.209.70.0	true	false		high
mta5.am0.yahoodns.net	98.136.96.91	true	false		high
c9d0e790b353537889bd47a364f5acff43c11f248.xyz	185.112.83.97	true	false		high
privacy-tools-for-you-780.com	8.209.70.0	true	false		high
microsoft-com.mail.protection.outlook.com	52.101.24.0	true	false		high
goo.su	172.67.139.105	true	false		high
transfer.sh	144.76.136.153	true	false		high
api.telegram.org	149.154.167.220	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high
api.ip.sb	unknown	unknown	false		high
yahoo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://81.163.30.181/l2.exe	true	• Avira URL Cloud: malware	unknown
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://81.163.30.181/l3.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.142.143.116	patmushta.info	Russian Federation		35196	IHOR-ASRU	false
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
172.67.139.105	goo.su	United States		13335	CLOUDFLARENETUS	false
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
8.209.70.0	host-data-coin-11.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
52.101.24.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
81.163.30.181	unknown	Russian Federation		58303	IR-RASANAPISHTAZIR	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553366
Start date:	14.01.2022
Start time:	19:07:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GNXG5XLBEH.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:	48
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@58/62@102/15
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 38.1% (good quality ratio 25.6%) • Quality average: 51.8% • Quality standard deviation: 41.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:08:35	API Interceptor	3x Sleep call for process: svchost.exe modified
19:09:09	Task Scheduler	Run new task: Firefox Default Browser Agent B475E6AC46161B97 path: C:\Users\user\AppData\Roaming\ttfssdi
19:09:26	API Interceptor	1x Sleep call for process: 6BA5.exe modified
19:09:45	API Interceptor	1x Sleep call for process: WerFault.exe modified
19:10:08	API Interceptor	1x Sleep call for process: explorer.exe modified
19:10:47	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
19:10:47	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run RegHost C:\Users\user\AppData\Roaming\Microsoft\RegHost.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2486023385576548
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4V:BJiRdwfu2SRU4V
MD5:	32D17CCD2B6339DF019EBB675E860FAF
SHA1:	9797760F17F157597E26E0060638986E6653A7F9
SHA-256:	4FA5B39006989138CDF98AE11DD5855CF9909200A2AC8666B1CB6BB45B949A0F
SHA-512:	B922ACC6838D46E0D3E7D4895C6451828A122450CC7BC6FC98880FA25807A3B7A486F57970E77AAB2E513BA80B12ECCC753FEA9020C81093DE4BF0954D4A702
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x57ece8f3, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25069143755463874
Encrypted:	false
SSDEEP:	384:s+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:zSB2nSB2RSjlK/+mLesOj1J2
MD5:	F7E6A2DE3097C7FFE9639C74B6A26D82
SHA1:	D158073CE723A78BDBC831702D34FAA27FEA317A
SHA-256:	6C65A26815CE80E9E63CA682743B45BB40FE45C91DE0C225865CE390D2C16B7B
SHA-512:	DC20BD49475F3778501D018B892C1D9F7C3F01CD5A1FF5B289D1C4B264011C536747BEFD743B61868B670B800956F2C6D7A18301F4520A422E8E8F0CD672D3B1
Malicious:	false
Reputation:	unknown
Preview:	W..... .....e.f.3...w.....&.....w..#....z..h.(.....3...w.....B.....@..... ....3...w..... .....}.#....z.....o#....z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07710005765895223
Encrypted:	false
SSDEEP:	3:faG1EvGU3TJl/bJdAtiVvmf4/All3VkttlmlnI:FQGiTJt4bf4A3
MD5:	4C83DD7FB6BC1F021316190F961B5B91
SHA1:	1B42B2D8F7EC7E5CB77888C6057447D07C427B03
SHA-256:	9E9A916A5E9AA99FACADC3DB55432377A47B40608C3DFD87819FCCA77FFBB86B
SHA-512:	EE335F572DD2D1B46AD21437F987263683EA96489A3F2F0D548761FC4EDC13FA1ED933455E7459F28AE54C56E2B4452CEF08A01AB1CB16611CF2106132D47E75
Malicious:	false
Reputation:	unknown
Preview:	.Qk.....3...w..#....z.....w.....w.....w....:O.....w.....o#....z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_5BBC.exe_362029c6c23990d576b7266aec72f8f83ce9e419_c52cd5fe_0e289cc1\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_5BBC.exe_362029c6c23990d576b7266aec72f8f83ce9e419_c52cd5fe_0e289cc1\Report.wer	
Entropy (8bit):	0.8116740932612948
Encrypted:	false
SSDEEP:	96:J3Fs18LHzErOQoJ7R3V6tpXIQcQec6tycEfcw3++HbHg/8BRTf3o8Fa9iVfOyWYV:Ja4Hzf8HQ0lzjIq/u7sXS274ItH
MD5:	424949616D212EF0F10948818A1A9A93
SHA1:	5A7114CD9918ACCCDE826C09676AC83B761A6756
SHA-256:	15964ACF293606ACCA72747608CB3B0E5A1C1DDD56F25D416D51331E4C8F1530
SHA-512:	071C070AA2CF180648F3FC89CBE6D660D45C99BAE79ADF8AE40160BC10BD3779EDC5AE45D76C3D2B5E962B62607D64BC7BBC5C3158D964295636DEB706A48 16
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.8.9.7.6.5.6.5.4.7.3.8.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.8.9.7.8.3.6.0.7.8.1.2.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.a.7.2.5.e.b.b.-.a.d.a.d.-.4.c.1.2.-.8.e.4.7.-.7.f.2.6.2.e.0.6.e.c.9.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.0.2.4.f.8.0.4.-.4.b.6.c.-.4.d.d.b.-.a.a.d.3.-.b.0.f.b.0.1.9.d.6.8.0.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.5.B.B.C...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.c.c.-.0.0.0.1.-.0.0.1.6.-.9.d.5.2.-.a.d.4.6.b.d.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.1.a.b.d.2.2.a.2.e.e.a.9.2.b.8.a.7.f.d.5.0.e.2.3.1.4.5.a.3.2.7.0.0.0.0.2.9.0.1.!.0.0.0.0.5.9.9.5.a.e.9.d.0.2.4.7.0.3.6.c.c.6.d.3.e.a.7.4.1.e.7.5.0.4.c.9.1.3.f.1.f.b.7.6.!.5.B.B.C...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.1././.1.2.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F4.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.69625050451798
Encrypted:	false
SSDEEP:	96:9GiZYWdtNxdSYAYHWOwPHcUYEZ3zt0iHFaoowSpmdJaOKGMvlIVlW1C3:9jZDcXLdySJaOKGMv6V81C3
MD5:	72F230E559D353F527212903830DCBB6
SHA1:	A46C90A7E6FF357384B1ADDC560178F5453B2CD8
SHA-256:	47F8457ED2B41853D2EFCEC7FB02DE8E0C19F5F89FE17CB67FD151109DE185E4
SHA-512:	68501EFCBDBD6560DCC2868A088413BD3FAF7E692102EEDF5814416AEB942499813CD202D3284CD2867B98CAFF40F3EE4CA97CA2C7EAA0D1314178514A0F6D 1
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD849.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jan 15 03:09:27 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.117103937458852
Encrypted:	false
SSDEEP:	192:5ZqT4MxcyQbNOeh0c9kk8JzTpYL4Sjtu30PIG3Z8IF:oQ0e83tiLx4EPLF
MD5:	496E92D721F8E10B39B44D0F4CA6D89D
SHA1:	AE388E1DC8882F735980D0460D10BFFC69AF9B79
SHA-256:	91FC0F6EA2F1BCBF168B57787F820DB2F41B77E3D0469B364F413E72E8937C7B
SHA-512:	0BD89C72EC7066EE6AD1F53AD6B2873E3616A5D5A520E3FB812AA332D301FBE47B5076CBE517C0BADF23F35F7960830D421CCA5F8578E20CFBB820DE84B317 F
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....:.a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....:.a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE171.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.7011350482745184
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE171.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNi6md6d6YIWSULgmfPRSDxCpDx89bdZsf1Dfm:RrlsNi56d6Y5SULgmfPRSzdyf1C
MD5:	968F3AF271FD4CE28C40F73590BCA036
SHA1:	77A499C5AD4A009DD85C5689FECEAD99CDF9DB95
SHA-256:	D989F0538F980FD768B617972D05FAE1B361E1F8C4EB4E4212F8DB71A7CF9B73
SHA-512:	385783DD10F08CF73203617B20A4964195E3323221474291499DCCAA2960488D27052FBD175516181A884C732C0DC6B92E4CEF49B8587082863C4C4E0F17DFB6
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE6F1.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.478780568175464
Encrypted:	false
SSDEEP:	48:cvIwSD8zsmJgtWI9h9WSC8BC8fm8M4Jd8qFx+q8vI89gERhdd:uITf8WMSN5JTKTgERhdd
MD5:	5A603AD54A5E06BACD7B138A39BE046E
SHA1:	58B7254947CAEF8F8808B08E9B8CB31618D7C9B0
SHA-256:	7DF81C368A2989544FC6977AE0242FEA067BA507BAD0F659106E2E0ECA6CA2E3
SHA-512:	09CC48B52225DC6267B4F73756C56C0EDDBD217532B2752F4F8D739D0366641C5ACF3CEC03CA3054B0B94C2283130687B3F4CD48463DCD25EFC8EEC9065EEED
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1342820" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF935.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	55166
Entropy (8bit):	3.063403298010223
Encrypted:	false
SSDEEP:	1536:MbHydL/jw6tEEQlhbZilVfBl8xfddAc8Vk:MbHydL/jw6tEEQlhbZilVfBmxfddAc8a
MD5:	588FF1C6A720F668343C3545EC86C5EE
SHA1:	DB8FFA83F59917EE1955379382ABD5C177ECEF25
SHA-256:	AB38D23F75AFDF2F6913F4E07F668C7CA4C4BC2CF5FC620802DD956E4D5D71A5
SHA-512:	C0C9AC910856431A969793280DAD81C9D0A80C42F8D32AFA48DCDAD8800513A27731807DD0E7332EF3830AA3F64D3238D4C15932BC3B3BE2CE743C4AC42F6C
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8058.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\8058.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8058.exe.log	
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\0fcf02de-4ec7-4c4a-9f75-b190c4b2731b.c7c3e4c9-bbf8-40be-800f-a09c9aae178d.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1218
Entropy (8bit):	3.589442580791056
Encrypted:	false
SSDEEP:	24:LLVR2mRipcTpWzgx71+8zsafc+Oc2CpXpPkX+vUViiBg5X3gebiL:LLD2mRiS6gvNzrfeIXpPkX+v8iiBg5Xq
MD5:	ED6375356DBE3105FB3C6C285BB7BB61
SHA1:	5B44C771F10C06AB6630EA9415D22B0ABF5072D9
SHA-256:	B910022E06D2F1FEB8D961628DBA6EF12A63A492182EEBEE6C33077E6035BD0B
SHA-512:	6525445A1750C62123EC52C830F22F93D79ABA02468C9A5E07ED49AE829EC4A1F1AE3B228DB239B867279134BF5C6FE3C97A3E44B2B64C3AFC62969D774D039
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.j.Z.?.v.e.r.=.e.e.7.1...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .1.1.:.5.7.:.3.3. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .e.d.f.f.1.b.c.b.-.c.f.5.5.-.4.8.c.8.-.8.7.e.6.-.a.d.0.4.2.6.9.c.4.b.e.9...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.p.n.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.j.Z.?.v.e.r.=.e.e.7.1...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.5.5.2.0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.5.5.2.0...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.l.i.c.,. .

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\0fcf02de-4ec7-4c4a-9f75-b190c4b2731b.down_data	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	15520
Entropy (8bit):	1.896672757405903
Encrypted:	false
SSDEEP:	48:x/6mM+k29W8sEvN4e4rxN+Y9rN+p4BCZxw/A/GQBC1GbGLxxVs4Psc5vH7CSpNvn:xS6kEWRvxNXrNQZqR+0Xsc5jhpNV4O
MD5:	E3016B6D693EF6EB1BA9DA3078AE4730
SHA1:	5AD0C746BD7B0DF41EBE31A8884A77E1208E6B01
SHA-256:	D55321AE7A013B00941E36D12160D6596D616EBD68D2240866275C170BB822F9
SHA-512:	737858FCB07EC6FED1014B9F58248AF81E3F21ED69CCF528365D77438F3284FCE6B2E3DBBD2EBBC318224F4E0C466453B558D3BD56359E66D4418C14DEA51A(
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....w=.....pHYs.....:.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2017 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2017-05-17T14:41:35-07:00</xmp:CreateDate>. <xmp:ModifyDate>2017-05-17T14:43:52-07:00</xmp:ModifyDate>. <xmp:M

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\21013e79-9794-49b7-ae5b-fc5c992bd6bc.a214058d-4932-49cc-ab40-d730f65403f6.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.605918884002608
Encrypted:	false
SSDEEP:	24:LLVR2mRiw0oUWzgx71++Bisafc+Oc2CpXpjjX+vUViwzB+vFX3+vqbbL0D:LLD2mRiabgvJirfeIXpjjX+v8iqBCX3S
MD5:	195D829E09800C81AE13EBEF1D5FCB05
SHA1:	DDBC8B89C88BA51ABCB9C3E91E08EE956C2E40B8
SHA-256:	AF908F5DE5D73626FEF4AEACE77887D9025A763E2B99B3AEBF05F56CDF5304C7

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\21013e79-9794-49b7-ae5b-fc5c992bd6bc.a214058d-4932-49cc-ab40-d730f65403f6.down_meta	
SHA-512:	5C62BB28712F1BCA6AF00515DBB3BEB0081F52987C03F622CCC44595C30A5CE8BC935A398D0C2DFA8A9694F4C55BC5E07818CB1F9581EC020DC4BDD3357B34 3
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.V.B.5.?.v.e.r.=.d.d.3.a...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.u.e.,. .1.1. .J.a.n. .2.0.2.2. .2.0.:.5.2.:.0.7. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .7.6.2.f.8.9.7.1.-.d.6.d.b.-.4.c.6.4.-.8.0.6.5.-.9.d.4.f.0.2.b.9.8.6.7.b...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.V.B.5.?.v.e.r.=.d.d.3.a...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .7.5.5.4.3.1...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .7.5.5.4.3.1...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\21013e79-9794-49b7-ae5b-fc5c992bd6bc.up_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	278
Entropy (8bit):	3.40206142697723
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQwRmRL3:ZxMghwLtHSM1Sb9mSMXAvwRml
MD5:	AEFA3D8CE597A555C0D1CC74126F7FA3
SHA1:	BE33A552E7BDC93A5749190A28EC843C9E6ED768
SHA-256:	6FD155BD2B31AFFEF15C8CE887B50ECBC912C0DD9C4113E2B76B6CDECCD0F6DA
SHA-512:	A9594A9589B147F8451E3241B2497E195DA9F582FB264BF0BF9E84B3CFD7BB6934F97507891744D78114B197757485C7147F6AFF21F25E07F25D986AA59D3B09
Malicious:	false
Reputation:	unknown
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.V.B.5.?.v.e.r.=.d.d.3.a.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\27cc05ce-f6ae-4e8c-aa08-af3f678f3684.7e4aef61-82dc-4c05-85c3-81f1b0303abe.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.5787279232030773
Encrypted:	false
SSDEEP:	24:LLVR2mRiwQfO1Wzgx71+f+fYMYsafc+Oc2CpXpjjX+vUViwQjBWX3BbN+zP6D:LLD2mRiHWOgvELbrfeIXpjjX+v8iHjBq
MD5:	8267193EA712F064D8D137F0ED94624D
SHA1:	44176BFD36C7E0E23106020D1E266C3ECDDD74DF
SHA-256:	589148B40E1EFEF193CA4EB5F35D1DC591FCB22898346A7CA8655A3E70633FCB
SHA-512:	7BBF2908CDEC58D9A8EE1949CBC3636F7B8C69E30EFBDF27B2D434BCEDC6F6C2E894D6B69C2E62A1D4957B776D6658D68EDE88D7979A30FC8438D71E999F9 E5
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.Y.e.S.?.v.e.r.=.0.9.d.6...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .F.r.i.,. .1.4. .J.a.n. .2.0.2.2. .1.3.:.0.9.:.4.7. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .0.8.1.5.2.c.d.8.-.c.d.a.3.-.4.1.0.e.-.8.e.7.c.-.d.a.c.2.c.1.6.a.0.c.8.8...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.Y.e.S.?.v.e.r.=.0.9.d.6...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .6.4.9.4.2.8...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .6.4.9.4.2.8...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\27cc05ce-f6ae-4e8c-aa08-af3f678f3684.down_data	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1080x1920, frames 3
Category:	dropped
Size (bytes):	649428
Entropy (8bit):	7.7771944987396555
Encrypted:	false
SSDEEP:	12288:/ELaBE1ZTI1vJqS1WgOmA7l8uyksA+IHt3xQio2GqFrg+CoMSIsLvMJ7xOoHZ:SyrqSHOr/eBINa0GqFrg+x4sWUsZ
MD5:	23F1E3C2429113D51CE85214A3EAA63C
SHA1:	A4E2DA580347C6039F9145C3B8CAA960AB50762B
SHA-256:	4C831289763620D63766F8C5E97CA92AB7AF0EEA912147C733FF447B1E476656
SHA-512:	840EEDE18168026B2E48CE951A4F796D43FDA8E2C1E12F36D25AF6ED4C041E8F3B26B5D3A824AD41E22FF9B24A31EF9A79D6A8014AE6F3A32EC8D28217391D(A

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\27cc05ce-f6ae-4e8c-aa08-af3f678f3684.down_data

Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C.....C.....8..".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...T..-..y.....0..j...H.t..t_.]V.%.. ?.!.G.....o....O&.;.}.<.W.....\|....y.G&.....X.\|34.i.s...{.g..e.....O.....yj..}..H.??.....U..S.^.....(....G.o..2\|.....Q..o<m.....<....\l;.H$..H.....WY....}.$..wd.^.....%?z..9)....=.e(.j...s z..qk.1.wWv..:I'.k..K.....c.-.....e.^.}.>;./.u.TK..#.....Q.mJu.8.v..$o.U.F.....Z.n..j.-...k$q.....7.m,.....8..R

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\28f286d4-7ba8-4d17-bd00-f85bb8c939a2.cc9fc646-c2fc-4fa6-88b0-56f3d96acf5a.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.5969448589373916
Encrypted:	false
SSDEEP:	24:LLVR2mRiDTXWzgx71+A8tzsafc+Oc2CpXpjjX+vUViXBGX3xbHckwU:LLD2mRiHwgvL8ZrfeIXpjjX+v8iXBGXJ
MD5:	E88A4678CD98FF4C33ABE52268A7C0F1
SHA1:	0ACC06763288CBD46231C1359D8C515A8F9E5DBF
SHA-256:	BDBA791D2D197B661BA522F55DE509508C61FB7A3ADB24C187CF9F51E56C6E86
SHA-512:	5A99D466C70AC3D5F0276E05EDF359450D3625FF6951226ADB2DDE453FB3BB06FABA7F97F4F4A1DA3738225BFC82313F864C9A8D8272A4380D90D4534882ECB
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.u.h.o.?.v.e.r.=.a.d.3.8...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .2.3.:.2.1.:.5.3. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .4.0.d.b.9.f.5.a.-.0.5.5.5.-.4.3.6.a.-.b.6.3.5.-.c.c.b.9.6.e.b.b.8.e.9.5...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.u.h.o.?.v.e.r.=.a.d.3.8...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.7.2.7.9.8.7...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.7.2.7.9.8.7...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\28f286d4-7ba8-4d17-bd00-f85bb8c939a2.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Windows), datetime=2020:08:25 09:19:56]
Category:	dropped
Size (bytes):	1727987
Entropy (8bit):	7.00466959635563
Encrypted:	false
SSDEEP:	24576:04jNiVr4qua18zGlkrZEJEKBcM/pra/R0DGoGaGZUWcId0nR2pN6oyD3KVRIHZFm:04jNiVr4qWG5PS5p8oyWzcbX9KPt
MD5:	16F8C62F063EB2B648E854B2DC08959A
SHA1:	166743B3BCC6B7D50C507D2522E8F3C644D720A9
SHA-256:	FB91AA134CD79665B6133C8943A052BBF660F21FC42FDD0FAFC78213DD3850B6
SHA-512:	801930F6ED038B9E489D4A900DE52116989FF2CD938B42C8FB690E3CD431756777DC65DA5B0821D4FC55A95538388D0EDD32B51E9C81CA198F75F0BB55A7A1B
Malicious:	false
Reputation:	unknown
Preview:	......Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 21.1 (Windows).2020:08:25 09:19:56.....8..... .....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d..... .....Z..".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...HEc.....%?.*2.L..LC .*.9..RhD....5b... $.3'F.N.FeJ#L.....>.:..1....0....R..q}....-.1.....T.....m.... ..h(..5..... "4....x....'..".X:...

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4fca2ad7-819f-4ce7-871e-d7f95abce2d8.701c9b8b-e624-449d-a7f7-5920d87b9fa6.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.596377708245441
Encrypted:	false
SSDEEP:	24:LLVR2mRiJTyWzgx71+XxPWJsafc+Oc2CpXpjjX+vUVi9BKkX3KPbDkwU:LLD2mRiNZgvIOJrfeIXpjjX+v8i9BKkX
MD5:	0FE0FF6CA45026CD1EBF503AC1ACEBFB
SHA1:	EF50B263F19557055B5532596B2D25AD258675A9
SHA-256:	EBAA06E959ED054EC3F00769234D5D05D09996EF388448147655EEBA2488483F
SHA-512:	4FA7BF1964C753E5E21CB8610186FDA56210CE8F83733389FC2E8133D2AE694E97BE508026437168EE5480E38EC1A293AB82B5A62D2FD22E192C2EB5F3C1E05E
Malicious:	false

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4fca2ad7-819f-4ce7-871e-d7f95abce2d8.701c9b8b-e624-449d-a7f7-5920d87b9fa6.down_meta

Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.k.k.?.v.e.r.=.8.c.6.2...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .1.7.:.1.1.:.1.0. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .4.e.0.a.9.3.4.6.-.0.9.9.0.-.4.3.c.9.-.8.3.2.3.-.2.1.8.3.5.2.0.d.5.6.b.3...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.k.k.?.v.e.r.=.8.c.6.2...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4fca2ad7-819f-4ce7-871e-d7f95abce2d8.up_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.40203749325483
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQi9nBo:ZxMghwLtHSM1Sb9mSMXAvO
MD5:	35DBDA98AE9B6FC0283A5A4C9C4AAC23
SHA1:	D3DD940A127CFAE4DBC453D02027D7DB06D17ADB
SHA-256:	3284A5D8408366FE712154660CA3C5723327F1F8B1E5E2573941670F2DD403EC
SHA-512:	BF0901B36FC704DCF76AE93483D6DF36919B5DB3F0F92ECD083D7A44416926906F948A1BF3B16033EE375F27B634B5B81ED52DD55B4ABDE93FC0613BB74AEE6 2
Malicious:	false
Reputation:	unknown
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.k.k.?.v.e.r.=.8.c.6.2.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\5c717cc5-fa43-4679-9bd0-506e2460bd23.d8889b23-4a02-470f-833a-b67283ec1ed8.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.5913432744209213
Encrypted:	false
SSDEEP:	24:LLVR2mRivWzgx71+BqCTsafc+Oc2CpXpjjX+vUViZZBz5RX3z5Wbb/TeL:LLD2mRiYgv+PTrfeIXpjjX+v8i3Bz5R9
MD5:	493F4DB619E362FC37095C0C075926CF
SHA1:	69543AA935B7B1B1E76D9CAA1126608C2478956C
SHA-256:	712BBF489C3EE89C2414725C89293818922B75D5B6E84B4759DE66D57439FBA3
SHA-512:	7C7173FEDF919C56EF02A12707F19A15C532C4AB14D215A426C2319D1DBC7ECB9435D5623DC434B527F3DA964709BF6D6411014AFD518C4472B981F1208DD47
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.9.e.R.?.v.e.r.=.b.7.f.9...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.u.e.,. .1.1. .J.a.n. .2.0.2.2. .2.1.:.0.0.:.0.8. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .f.6.2.e.3.8.8.7.-.f.f.b.c.-.4.d.9.3.-.8.c.f.8.-.a.9.a.a.7.a.e.8.4.6.3.b...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.9.e.R.?.v.e.r.=.b.7.f.9...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.8.3.7.1.1.3...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.8.3.7.1.1.3...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\5c717cc5-fa43-4679-9bd0-506e2460bd23.up_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.426779962179868
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQiLAoMc:ZxMghwLtHSM1Sb9mSMXAv00
MD5:	CF061E37763127705F0C30EE3B8AB460
SHA1:	569CE40921461B1DDBFAC8B87D2E41590275CB05
SHA-256:	5E635F4078440F931BFDF334D1F2EFF8B291BCD73680FF84FE0020BC06C5A944
SHA-512:	28D7B7A8CF655B78218562B8430E8461B5C1CBD072B0FBCB60E4F595B74DE7ADDB6A8F18E04EE0C0E216FA16794ED8574D1768B1360AB4EF45CC282CC761E7 3
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\5c717cc5-fa43-4679-9bd0-506e2460bd23.up_meta	
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.9.e.R.?.v.e.r.=.b.7.f.9.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\6f37363b-c375-4b45-91f9-ec727d246644.c7c3e4c9-bbf8-40be-800f-a09c9aae178d.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1218
Entropy (8bit):	3.589442580791056
Encrypted:	false
SSDEEP:	24:LLVR2mRipcTpWzgx71+8zsafc+Oc2CpXpPkX+vUViiBg5X3gebiL:LLD2mRiS6gvNzrfeIXpPkX+v8iiBg5Xq
MD5:	ED6375356DBE3105FB3C6C285BB7BB61
SHA1:	5B44C771F10C06AB6630EA9415D22B0ABF5072D9
SHA-256:	B910022E06D2F1FEB8D961628DBA6EF12A63A492182EEBEE6C33077E6035BD0B
SHA-512:	6525445A1750C62123EC52C830F22F93D79ABA02468C9A5E07ED49AE829EC4A1F1AE3B228DB239B867279134BF5C6FE3C97A3E44B2B64C3AFC62969D774D039
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.j.Z.?.v.e.r.=.e.e.7.1...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .1.1.:.5.7.:.3.3. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .e.d.f.f.1.b.c.b.-.c.f.5.5.-.4.8.c.8.-.8.7.e.6.-.a.d.0.4.2.6.9.c.4.b.e.9...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.p.n.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.j.Z.?.v.e.r.=.e.e.7.1...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.5.5.2.0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.5.5.2.0...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.l.i.c.,. .

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\6f37363b-c375-4b45-91f9-ec727d246644.up_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.4307777993094337
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQi9nOxzX:ZxMghwLtHSM1Sb9mSMXAvN
MD5:	4ADC4A45A014F77488BFC079F95EB4D0
SHA1:	4B9467083C60E6D721E714FBC7B1940421B758CB
SHA-256:	917FDDAA8EBC6C91DB178BAF7353B9BD01EA1C5DCE9DE8AA555647277C3E021F
SHA-512:	5C958A1C5C610F00DD5B8543699A98E325A7E9674770975D8091BFBCE58EA59811DF813E2CD7F79E09E7738F1A3F535B4B038FE11D7B8406F80E700523FAABD9
Malicious:	false
Reputation:	unknown
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.j.Z.?.v.e.r.=.e.e.7.1.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\7e716a44-d46f-42ba-819e-1ad870190297.cc9fc646-c2fc-4fa6-88b0-56f3d96acf5a.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.5969448589373916
Encrypted:	false
SSDEEP:	24:LLVR2mRiDTXWzgx71+A8tzsafc+Oc2CpXpjjX+vUViXBGX3xbHckwU:LLD2mRiHwgvL8ZrfeIXpjjX+v8iXBGXJ
MD5:	E88A4678CD98FF4C33ABE52268A7C0F1
SHA1:	0ACC06763288CBD46231C1359D8C515A8F9E5DBF
SHA-256:	BDBA791D2D197B661BA522F55DE509508C61FB7A3ADB24C187CF9F51E56C6E86
SHA-512:	5A99D466C70AC3D5F0276E05EDF359450D3625FF6951226ADB2DDE453FB3BB06FABA7F97F4F4A1DA3738225BFC82313F864C9A8D8272A4380D90D4534882ECB
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.u.h.o.?.v.e.r.=.a.d.3.8...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .2.3.:.2.1.:.5.3. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .4.0.d.b.9.f.5.a.-.0.5.5.5.-.4.3.6.a.-.b.6.3.5.-.c.c.b.9.6.e.b.b.8.e.9.5...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.u.h.o.?.v.e.r.=.a.d.3.8...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.7.2.7.9.8.7...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.7.2.7.9.8.7...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\7e716a44-d46f-42ba-819e-1ad870190297.up_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.4204444333325688
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQizLr/:ZxMghwLtHSM1Sb9mSMXAvOf
MD5:	69EC42767BCC5CEE5A189FC425B84465
SHA1:	CE4B848763A15E9379BAD715BE394DB4F381E95F
SHA-256:	099126C5D7E0375F4648D823761E763941ED67B55169B9C6BFECB06ED74F1856
SHA-512:	5DF588622ACB60A8B79EE729A6D818EDA9EEAC8EFB4A0ED413E2CF179F68D16E9DAFAA1DDCD1D7D3A96936E32837CAF7FBC932E61411CAB2A73AEBC753906EEF
Malicious:	false
Reputation:	unknown
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:././.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.u.h.o.?.v.e.r.=.a.d.3.8.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8d55ce73-4b6e-4fc2-8c77-af49ec66c092.7e4aef61-82dc-4c05-85c3-81f1b0303abe.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.5787279232030773
Encrypted:	false
SSDEEP:	24:LLVR2mRiwQfO1Wzgx71+f+fYMYsafc+Oc2CpXpjjX+vUViwQjBWX3BbN+zP6D:LLD2mRiHWOgvELbrfeIXpjjX+v8iHjBq
MD5:	8267193EA712F064D8D137F0ED94624D
SHA1:	44176BFD36C7E0E23106020D1E266C3ECDDD74DF
SHA-256:	589148B40E1EFEF193CA4EB5F35D1DC591FCB22898346A7CA8655A3E70633FCB
SHA-512:	7BBF2908CDEC58D9A8EE1949CBC3636F7B8C69E30EFBDF27B2D434BCEDC6F6C2E894D6B69C2E62A1D4957B776D6658D68EDE88D7979A30FC8438D71E999F9E5
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.Y.e.S.?.v.e.r.=.0.9.d.6...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .F.r.i.,. .1.4. .J.a.n. .2.0.2.2. .1.3.:.0.9.:.4.7. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .0.8.1.5.2.c.d.8.-.c.d.a.3.-.4.1.0.e.-.8.e.7.c.-.d.a.c.2.c.1.6.a.0.c.8.8...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.Y.e.S.?.v.e.r.=.0.9.d.6...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .6.4.9.4.2.8...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .6.4.9.4.2.8...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8d55ce73-4b6e-4fc2-8c77-af49ec66c092.up_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	278
Entropy (8bit):	3.3958192057775554
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQwRm4AUo:ZxMghwLtHSM1Sb9mSMXAvwRm4AU
MD5:	8FF007CE8512BF0CB7AF77033E0AC28E
SHA1:	8F5BC2546847165502F11236D056EF83E97A4305
SHA-256:	EF2F70B62E80BF46BFD71A89762993EAB3006186B1CD8CB9E9255E8897CF266C
SHA-512:	872FD514C0096CF6A36426C37AA1E946A20AC78CDE7FB1D4E1E45A8C2D5059617F33FAEB4FEC7DB2BEA56CEDDA8CB8DEC5687225D20262D1903BDDF15D71AE31
Malicious:	false
Reputation:	unknown
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.Y.e.S.?.v.e.r.=.0.9.d.6.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\bdc8be70-232d-44db-b8b8-fc3a9a8df62c.d8889b23-4a02-470f-833a-b67283ec1ed8.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\bdc8be70-232d-44db-b8b8-fc3a9a8df62c.d8889b23-4a02-470f-833a-b67283ec1ed8.down_meta	
Entropy (8bit):	3.5913432744209213
Encrypted:	false
SSDEEP:	24:LLVR2mRivWzgx71+BqCTsafc+Oc2CpXpjjX+vUViZZBz5RX3z5Wbb/TeL:LLD2mRiYgv+PTrfeIXpjjX+v8i3Bz5R9
MD5:	493F4DB619E362FC37095C0C075926CF
SHA1:	69543AA935B7B1B1E76D9CAA1126608C2478956C
SHA-256:	712BBF489C3EE89C2414725C89293818922B75D5B6E84B4759DE66D57439FBA3
SHA-512:	7C7173FEDF919C56EF02A12707F19A15C532C4AB14D215A426C2319D1DBC7ECB9435D5623DC434B527F3DA964709BF6D6411014AFD518C4472B981F1208DD47
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.9.e.R.?.v.e.r.=.b.7.f.9...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.u.e.,. .1.1. .J.a.n. .2.0.2.2. .2.1.:.0.0.:.0.8. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .f.6.2.e.3.8.8.7.-.f.f.b.c.-.4.d.9.3.-.8.c.f.8.-.a.9.a.a.7.a.e.8.4.6.3.b...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.Q.9.e.R.?.v.e.r.=.b.7.f.9...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.8.3.7.1.1.3...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.8.3.7.1.1.3...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\bdc8be70-232d-44db-b8b8-fc3a9a8df62c.down_data	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Windows), datetime=2020:08:25 09:18:51]
Category:	dropped
Size (bytes):	1837113
Entropy (8bit):	7.102008955383616
Encrypted:	false
SSDEEP:	24576:ZdC81bz+Y6eH6kUZlsEyfcq/irE/R0JGSUtvBafF3VVYEMntQRiOWXL47u694s3e:ZdC81bzpH/t0V9MiRnaL+ua3xBNU
MD5:	799C3428C8E6A5556DD21C00AABEF97B
SHA1:	D0130AB57E5ACE2CA39E2F49F3E822D82E9BBDCC
SHA-256:	9978B1B37A71F1E041B11123A1451E93A2AAB6BBCEBC7DE01BA0B8BF22C74B11
SHA-512:	B7A78F6175BA2F15C72C936CA30570A7D56B2BABEB3C031C202B81E85D2D661FEEF2B665A9263CAC417BC75D73344205F28C6C859DE84BC97B3421F2DBE97EF
Malicious:	false
Reputation:	unknown
Preview:	......Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 21.1 (Windows).2020:08:25 09:18:51.....8.....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d.....Z....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?....`....W.0....r..:...Z~.Pd.k5..Sk..X..x..`u..<)..q...7...G...g....4..x.T.G.0...z.l.o*....."6.+A.m..Ef.=.&L..v.7..G..jU....jzurt..P.l..5Z.G..G..i;..o..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\d9ba0342-18ab-4279-adeb-d351ea245ae5.down_data	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Windows), datetime=2021:11:11 06:55:38]
Category:	dropped
Size (bytes):	1654488
Entropy (8bit):	6.926504673655095
Encrypted:	false
SSDEEP:	24576:1k44jNiVr4qVhre8lekiZaSEKBcf/prV/RRJGoGaEqKEHisGpp7quKRDR7ripxi6:H4jNiVr4qXlZvKV9pp7qPRDNripY6
MD5:	3C36C820F3E016E8A3A63C34BA7BEF07
SHA1:	AF2A7EBB7A6D6C1815190C24EF732B2089115331
SHA-256:	F62AFA107BBFE2FEAEF84AB87277D31DFE1AAABF61400F241FDD50C45AB19D7F
SHA-512:	1074A8603B932052ED17825E83403D5F4EC3CD8CC7DB94BC4F262146DDA054640CBFB126FD728AB35C8B2B20285BC71CFE20BB3DEB3BDF8CC4B2877595B940C6
Malicious:	false
Reputation:	unknown
Preview:	......Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 21.1 (Windows).2021:11:11 06:55:38.....8.....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d.....Z..".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..(..].1.....}S.... ..4mp#...w..[..`.[.P.=..g.w.U{.....{..?..<..I..`..:._..d.T.k.q.m...;..1.....@..A1..5w.kZCk...*`....~.*...$9.{..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\d9ba0342-18ab-4279-adeb-d351ea245ae5.eb16e995-ca84-40f4-ab30-b44222e03118.down_meta	
Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\d9ba0342-18ab-4279-adeb-d351ea245ae5.eb16e995-ca84-40f4-ab30-b44222e03118.down_meta

Size (bytes):	1228
Entropy (8bit):	3.5947028556775
Encrypted:	false
SSDEEP:	24:LLVR2mRiqThWzgx71+0RWElsafc+Oc2CpXpjjX+vUViWBKsDhX3KsDmbpkwU:LLD2mRiGCgvHMElrfeIXpjjX+v8iWBKo
MD5:	FD409FA92FBEA2FD7073CDD1A343D129
SHA1:	176E1C047344F309731B6E3733624C09ED0E392D
SHA-256:	844648EF68EFF5EE414A1C551D9262412CBA813B75D17559FE886C480A548ECA
SHA-512:	57FDBABD69D84D9379D59824B3BDB65C9871B6176B8F4E83E7EA96D4BE38EEAAEDB03EFE97DDC6B0FA3C89866D345362DAA94C394DF05E896AFFA0DB03E7A7EF
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:././/.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.0.U.C.?.v.e.r.=.2.f.4.4...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .1.0.:.0.4.:.1.6. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .1.8.a.0.a.0.2.3.-.f.c.b.3.-.4.c.6.1.-.8.d.f.7.-.7.f.0.8.a.a.4.1.e.3.7.2...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:././/.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.0.U.C.?.v.e.r.=.2.f.4.4...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\e0fc5cf9-8432-419c-98fa-5245d76af360.a214058d-4932-49cc-ab40-d730f65403f6.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.605918884002608
Encrypted:	false
SSDEEP:	24:LLVR2mRiw0oUWzgx71++Bisafc+Oc2CpXpjjX+vUViwzB+vFX3+vqbbL0D:LLD2mRiabgvJirfeIXpjjX+v8iqBCX3S
MD5:	195D829E09800C81AE13EBEF1D5FCB05
SHA1:	DDBC8B89C88BA51ABCB9C3E91E08EE956C2E40B8
SHA-256:	AF908F5DE5D73626FEF4AEACE77887D9025A763E2B99B3AEBF05F56CDF5304C7
SHA-512:	5C62BB28712F1BCA6AF00515DBB3BEB0081F52987C03F622CCC44595C30A5CE8BC935A398D0C2DFA8A9694F4C55BC5E07818CB1F9581EC020DC4BDD3357B343
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:././/.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.V.B.5.?.v.e.r.=.d.d.3.a...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.u.e.,. .1.1. .J.a.n. .2.0.2.2. .2.0.:.5.2.:.0.7. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .7.6.2.f.8.9.7.1.-.d.6.d.b.-.4.c.6.4.-.8.0.6.5.-.9.d.4.f.0.2.b.9.8.6.7.b...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:././/.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.C.V.B.5.?.v.e.r.=.d.d.3.a...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .7.5.5.4.3.1...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .7.5.5.4.3.1...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\e0fc5cf9-8432-419c-98fa-5245d76af360.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	755431
Entropy (8bit):	7.889494455004551
Encrypted:	false
SSDEEP:	12288:skGgYlPnhhvcDi/Pg5Bn3Vv0eucNiMc+cQpawhhIfB7iTzWqovkjset8scoXmizl:skGgC6iAnFvw6iMA+hIp7Ado8tpv
MD5:	FFE1E08E186355FBDAA8C57461BAA6DA
SHA1:	3FBA91092AE606FEB46FE84225C4016CEB5E0872
SHA-256:	D62A3279E0AD100138EF5A397B53029AF95E42BE9BF9FEC30D9A7A246DC75111
SHA-512:	DB703B8C3F3E3AE8B340F415291FF7C8A22CFFD72F23642C3F2EB115B6CF14EB3C398C0E5E13DFB421A0FCA697A7CE0A56C7CC45C1DE22F032FD332BDD03FC8
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C.....C.....8...".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....R9.E$.,.Y...z..{..'.....V...Yj....m....w...[z}.....K....n..'..._.IV....9..C..<3d..V..m..ZnV..-.w...v?...}.....u.$..r....{j..==k....]b.sE..o..#8..v..s+Tg-z-J.C.}hC.....m..bk.....OE..Z.....z....Q..K.(..>e...kb..5]>8:.V+...Oc]S.....cZ.j.v...O3G=..w,..v.n8.\....%.....k..z....d.my%.r.o,....l...5[.]X.k.....8..7.....!.U...W.PV.N.K..>...k{.m..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\ee43e9f0-56a7-4da5-a52e-7978cee7ce3e.eb16e995-ca84-40f4-ab30-b44222e03118.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\ee43e9f0-56a7-4da5-a52e-7978cee7ce3e.eb16e995-ca84-40f4-ab30-b44222e03118.down_meta

Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.5947028556775
Encrypted:	false
SSDEEP:	24:LLVR2mRiqThWzgx71+0RWElsafc+Oc2CpXpjjX+vUViWBKsDhX3KsDmbpkwU:LLD2mRiGCgvHMElrfeIXpjjX+v8iWBKo
MD5:	FD409FA92FBEA2FD7073CDD1A343D129
SHA1:	176E1C047344F309731B6E3733624C09ED0E392D
SHA-256:	844648EF68EFF5EE414A1C551D9262412CBA813B75D17559FE886C480A548ECA
SHA-512:	57FDBABD69D84D9379D59824B3BDB65C9871B6176B8F4E83E7EA96D4BE38EEAAEDB03EFE97DDC6B0FA3C89866D345362DAA94C394DF05E896AFFA0DB03E7A7EF
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.0.U.C.?.v.e.r.=.2.f.4.4...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .1.0.:.0.4.:.1.6. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .1.8.a.0.a.0.2.3.-.f.c.b.3.-.4.c.6.1.-.8.d.f.7.-.7.f.0.8.a.a.4.1.e.3.7.2...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.0.U.C.?.v.e.r.=.2.f.4.4...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\ee43e9f0-56a7-4da5-a52e-7978cee7ce3e.up_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.411328286431714
Encrypted:	false
SSDEEP:	6:ZyncUkamOwhg2YMYtHSMLhU7lBSliHGSMX6YXKMwEQi9PzM:ZxMghwLtHSM1Sb9mSMXAv
MD5:	F89B0A182CEC59870B296ADB7C2FC692
SHA1:	C9301A976859229017D581106CABF70BE78E9726
SHA-256:	03C5CB5701A4D9E152464A849CA4573C9009C7D6F878E6456A482756210FC37B
SHA-512:	D4923FA307B710FC1B87B47A40394ECB85084F0E064D296BCE477EEA9EA36A8918103498D7FAC813F8C8554330CCBB09E856CEFB830E6449787F8260D4A26F2E
Malicious:	false
Reputation:	unknown
Preview:	F.4.2.0.C.4.E.A.-.4.2.6.1.-.4.B.6.6.-.8.B.9.C.-.E.A.A.8.C.C.C.9.6.A.D.E...G.E.T...h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.0.U.C.?.v.e.r.=.2.f.4.4.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\f3c574c2-74c3-4fcb-a00b-1b0c64e37f0d.701c9b8b-e624-449d-a7f7-5920d87b9fa6.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1228
Entropy (8bit):	3.596377708245441
Encrypted:	false
SSDEEP:	24:LLVR2mRiJTyWzgx71+XxPWJsafc+Oc2CpXpjjX+vUVi9BKkX3KPbDkwU:LLD2mRiNZgvIOJrfeIXpjjX+v8i9BKkX
MD5:	0FE0FF6CA45026CD1EBF503AC1ACEBFB
SHA1:	EF50B263F19557055B5532596B2D25AD258675A9
SHA-256:	EBAA06E959ED054EC3F00769234D5D05D09996EF388448147655EEBA2488483F
SHA-512:	4FA7BF1964C753E5E21CB8610186FDA56210CE8F83733389FC2E8133D2AE694E97BE508026437168EE5480E38EC1A293AB82B5A62D2FD22E192C2EB5F3C1E05E
Malicious:	false
Reputation:	unknown
Preview:	h.t.t.p.s.:./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.k.k.?.v.e.r.=.8.c.6.2...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .T.h.u.,. .1.3. .J.a.n. .2.0.2.2. .1.7.:.1.1.:.1.0. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .4.e.0.a.9.3.4.6.-.0.9.9.0.-.4.3.c.9.-.8.3.2.3.-.2.1.8.3.5.2.0.d.5.6.b.3...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .d.e.n.y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.P.8.k.k.?.v.e.r.=.8.c.6.2...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\f3c574c2-74c3-4fcb-a00b-1b0c64e37f0d.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Windows), datetime=2021:11:11 06:54:34]
Category:	dropped
Size (bytes):	1829994

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\f3c574c2-74c3-4fcb-a00b-1b0c64e37f0d.down_data	
Entropy (8bit):	7.092403290156545
Encrypted:	false
SSDEEP:	24576:LdC81bzA4GeD+kaZRfEyfcA/ir2/R0JGSUmfyttS6dSTeuErzQP/Lg40bw2Rf02b:LdC81bz/Dq39STvErQ/05d0k
MD5:	4FB1CD4A9C7B4165BF8CD730F367600C
SHA1:	1FD8481802A3512CC65105B600C9339784A31E10
SHA-256:	E60B827FEE4A3A7FF6033C3F244AE04D5A51D7E581936BE750F2EABE4F72E2A0
SHA-512:	C3D101D94A75EFE81C7E8AB1F45654271A67048A6439C2C202589038519D24B62A98F77EA267AE320ED2FC9AFBB7D6C4AE4B079C19AA05E4F7D7BA7A87C79E6 1
Malicious:	false
Reputation:	unknown
Preview:	.....Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 21.1 (Windows).2021:11:11 06:54:34.....8.. .....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d..... .....Z...."..... ?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...n.fx..w.V..^N[..k .u....T.y._M.=..$..k.G..gV...i. .4..j.)..k..a~.~.K.2....:..-wc..[....(....X....&y.<...pu..C@..>.J.....k.8.....@..xdx...:.V..X

C:\Users\user\AppData\Local\Temp\13C.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7336391
Entropy (8bit):	**7.993025428513385**
Encrypted:	**true**
SSDEEP:	196608:76+hvICteEroXxqENE+sKsXXgvkz+AlnhMCRKsAN2aL:DInEroXjsKkXgsCMhkrNF
MD5:	CBE604877A46CEEBA112802BC17FFEF8
SHA1:	E85AB4CCBE491348C39F751162FFF71A90643ECA
SHA-256:	32703A3D88B3E9B8FE1A64FD1CBCC0925FC2C74BCBDEFBBD6944CBFAD0029FEC
SHA-512:	86F3946B813FB457D95B6635FA308DA1BF5F2C0FBD5BDCA75F7776D1A01A2D3C67A8A9E268DCC145FF575D70FBE84BE9BEB112A0D2269B955795C74468C005 8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'X.8c9.kc9.kc9.kwR.jh9.kwR.jd9.kwR.j.9.k.V#kg9.k1L.jE9.k1L.jr9 .k1L.jj9.kwR.jh9.kc9.k.9.k.L.jp9.k.L.jb9.kRichc9.k.....PE..d...Q..a.....".....6...T.....@.....p...`.....[..x..... .....H... 9.....@9..8.....P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data.....p.....T.....@....pdata..... .....`.....@..@_RDATA.....~.....@..@.rsrc.....@..@.reloc..H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\1523.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3576320
Entropy (8bit):	**7.9976863291960605**
Encrypted:	**true**
SSDEEP:	49152:Y+RSFqeQKgdJee+ntOkgd+TuRCg+687ZEYNFvKfDIcK8nAONaGGh:Yb8eQKg+tOV0T0z875NFKfDPK8nASA
MD5:	5800952B83AECEFC3AA06CCB5B29A4C2
SHA1:	DB51DDBDF8B5B1ABECD6CFAB36514985F357F7A8
SHA-256:	B8BED0211974F32DB2C385350FB62954F0B0F335BC592B51144027956524D674
SHA-512:	2A490708A2C5B742CEB14DE6E2180C4CB606FCCEB5F17DE69249CF532EDC37B984686B534A88AE861CC38471C5892785C26DA68C4F662959542458C583E77E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....!7. .....|.N. .... M..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....x+...P.....@.....1.....@....rsrc..... M.....L0.....@....28gybOo.....N.....1.....@....ada ta.....pS.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\2205.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654

C:\Users\user\AppData\Local\Temp\2205.exe	
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I....v....h.....E....x....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\2D8F.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	557664
Entropy (8bit):	7.687250283474463
Encrypted:	false
SSDEEP:	12288:fWxcQhhhhhn8bieAtJlllLtrHWnjkQrK8iBHZkshvesxViA9Og+:fWZhhhhhUATlLtrUbK8oZphveoMA9
MD5:	6ADB5470086099B9169109333FADAB86
SHA1:	87EB7A01E9E54E0A308F8D5EDFD3AF6EBA4DC619
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3EDCD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$...*..... ...`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...",..

C:\Users\user\AppData\Local\Temp\4955.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7336385
Entropy (8bit):	**7.993036026488077**
Encrypted:	**true**
SSDEEP:	196608:l++hvICteEroXxqENE+sKsXXgvkwuUxNhMC/CKN7kL:BInEroXjsKkXgs/EhWKNY
MD5:	AE6510D9815C44A818F722ECAE6844B8
SHA1:	2A34B5110F5C3C2424AE9685F57261E2546BD963
SHA-256:	C3CAD582268B165711E2F2B1834891C7BCB5E57A7EFB1E709E3DF19D011AD656
SHA-512:	8CAA9E661403D5D86F69E7C35E45CDF927EF9EC0C6045ED2CA5AF2EAAF26B4F99291EADAF2F0C8C00A31B05B228C6DF0C4BD205A7B3EC70E263313A08FFEF4F8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'X.8c9.kc9.kc9.kwR.jh9.kwR.jd9.kwR.j.9.k.V#kg9.k1L.jE9.k1L.jr9.k1L.jj9.kwR.jh9.kc9.k.9.k.L.jp9.k.L.jb9.kRichc9.k.....PE..d.....a.....".....6...T.....@.....%.p..`.....[..x.....H... 9.....@9..8.....P.....text....5.....6..... .`.rdata.....P.....:.....@..@.data.....p.....T.....@....pdata.....`.....@..@_RDATA.....~.....@..@.rsrc.....@..@.reloc..H.....@..B.....

C:\Users\user\AppData\Local\Temp\54D0.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3596288

C:\Users\user\AppData\Local\Temp\54D0.exe

Entropy (8bit):	**7.997492170986202**
Encrypted:	**true**
SSDEEP:	49152:x+8QEA1GN2zhieKqcTe0f3nWNHiZWf5dxQNPY7wUE9E8gnH43lvn/3juAVUk3Imp:xZ3KKqcTMNIWBnYAlRo7uOUk3ll4UMS
MD5:	8897C1354CB525DE5F4DE514D6FE836D
SHA1:	2F92D4CCA4D7576603A442BBACB87450F41CFE6E
SHA-256:	407C68405D373D2C8EF66B004B293BE25D571348E8922D02D7B79EB20A5138DB
SHA-512:	A46C6F7BAF298C34607701353E136120153521326A77C787F62F8BF439BB7DEC188A757271B4C8E47E650E86272159FD5D072A1530195D60900FEB8C481F671D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....6. .....|.N. ....0M..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....?....P.....@.....1..p.....@....rsrc.....0M.....0.....@....2pZFPAB.....N.....02..... ..@....adata.....S.....6.....@.....

C:\Users\user\AppData\Local\Temp\5BBC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8lA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i. hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@..... .....e..P.....2..... Y..@..... .0.....text..... ..`.rdata..D?...0...@..."..... @..@.data...X....p...$...b.....@....rsrc.....@..@..... .....

C:\Users\user\AppData\Local\Temp\6471.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3590144
Entropy (8bit):	**7.997643531968**
Encrypted:	**true**
SSDEEP:	49152:3+N1VszZfKeEM30gwJHRUy0hsgpJx7SbEmW/DNYwtinYQYwDvvEipRiGqmkNajh1:381EKrHVRA2A/+NWxYZYYDvvNji7o
MD5:	DA5C869D0ADE431230679390B5D183BF
SHA1:	A0A3EC54CDC7762F78BF1DD2C5594F9A6AF2CBC3
SHA-256:	98CE1395284401CDB5EBF5BDBCB02DDE9C404BEB668B7FF985794AE0408A5805
SHA-512:	47EA2FF52B50F1E4CB27957451D6C50F2D90B861A4BAF9A96718749368D76491CF9B1D39AA23E059A2A589DC48BD1EF0C529AE201EAD635806CA89A276C8208
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....p S.....#87.....|.N. .....M..... .....@.....0.....@..... .....@...z.....@..... ...0.....@.....P.....@.....1..`.....@....rsrc.....M.....0.....@....kujN2o2.....N.....2..... ..@....adata.....`S.....6.....@.....

C:\Users\user\AppData\Local\Temp\6B9B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	322048

C:\Users\user\AppData\Local\Temp\6B9B.exe	
Entropy (8bit):	6.699290650106884
Encrypted:	false
SSDEEP:	6144:MQ2h5D3tUU9l9zaP2kuPC7dIvnxcDzQMCXfEXu:MQsJpzRtq7GvxcYMC8
MD5:	039CCF44EF7B55AEB4D22D211D17774E
SHA1:	5C6E0E0F14F56F8F9C1D990474D9799C595572C1
SHA-256:	9EE489B4B2FEC770F57CCC6D2EAB9CE29678E3D4CA8A9D6467634B76C30B850A
SHA-512:	881CA9044920D2C108E3719000C9D881B58BBC5294B96E910B89B27D103D0C56B9F0DCD846FCE0F5160CDD02BF30E3A04DD31D6AE7E3DCDA87B73F3E46540FA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L....4.`.....@.....P.....(.....@.....L.....text..... ..`.data.....@....tuv.....@....bezax.....@....lelepar.....@....rsrc...(.....@..@.reloc..ZF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\6BA5.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	324608
Entropy (8bit):	6.709124384088194
Encrypted:	false
SSDEEP:	6144:lx+/UbfEz9xL/a5EQlXyBhQ3hTTJhYjVcsT:lxsUbczr/NKCB+hTTYjuQ
MD5:	7E58C9178CBD9D56DB805F034EC795CB
SHA1:	4859C89EED51EAEDAC1BAFBD52BFB5E9382BFDC3
SHA-256:	2798CE7846DE002A01D784C809499EB20BF108F2D93119AAD082098AC0CB03CC
SHA-512:	8D4A8C162332095BF5AD4CB1A712D0C0389FCCD91758450A2ABAF79A238977F61A653EE3FD44AF3571D6A6588763C0AAC331474F64571CE7D5FD99614D4C238
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L....p._.....@.....id.....P.....(.....@.....L.....text...~..... ..`.data.....@....geravic.....@....pude.....@....vup.....@....rsrc...(.....$.....@..@.reloc..dF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\6E36.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.021094695416705
Encrypted:	false
SSDEEP:	384:1P27QR0ir3uqVQ1Tf+1rkZlgEdLcHIH+2f9sFIILCbj4KQWylH28iYfx:1PYQR0i4krj58LIL0zy2
MD5:	9DA91D9E3AD909FB8EBA4D3D74344982
SHA1:	D5B6872D062043478CBA1002A815A013952D3837
SHA-256:	0417281135837E3CCC11F35B2D17A6A3672B011E85C18884F54F6FEABA7B8069
SHA-512:	29D672F0BB8AEE885F008F7B7EBED499E7C5D8738B9373BF169896BE85C271FAAB5BD9792C176C7CDCB1C39606F07041E1E54E8F893D1D91F49509DF927AA8A0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\6E36.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!.....0..J.....rh... .....@.. .....1...@..... h..O.....Tg..8..... ....H.....text....H... ...J..... ..`.rsrc.....L.....@..@.reloc.....N.....@..B.....Th.....H.....C..."....e..p.....^..}.....(.....(....*..*..0.....(...%.-...(....s.....s..... ....o..... ....o.....(....r...po..... ....s.....o.....[o....o.....o ....[o....o!.....o"......o#....s$.....io%.....o&.....,..o'.....o(.....,..o'.....,..o'.....+...*..(.....".....0.....o).....(*.....s+....+..*...0.....s,.... ....(-.....(.....r%..po/.

C:\Users\user\AppData\Local\Temp\74DE.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\74DE.exe

Size (bytes):	1332224
Entropy (8bit):	6.299565191919942
Encrypted:	false
SSDEEP:	24576:ynJUxJwfdmVnIMJftatB5BgaOfvSpNMtbJTJlF6+L3bMObTCRqCeC1O441JD7cTM:yJMP7av7b9Gf40UCL
MD5:	E6776A105FE3B67E63EC9DCDF4AFCB63
SHA1:	DDBA6C56361F4C4556FD3FABFCECC40DA59F71A8
SHA-256:	511130568349F9ADAFB26B5CB2614E5E3BF46CA807F0F650F3413F916EE0D32B
SHA-512:	A8DB24C28D3C7637CD3E3DFBCF1152E66798EF0AE53D7E919820AB754D1681B5371D6C3C2A8D3CD32CB34D6AB8F1F94F20FB1B9577861D13CF9ECCE06E9FEA6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..J.....h... .....@.. ..... .@.....g..S..... ....H.....text....H... ...J..... ..`.rsrc.....L.....@..@.reloc..... .....R.....@..B.....g.....H.....P...h{.....)C.....ta.....g.....y....(.D..*.s!>...T...**....(i...*f....(j...rA..p(....(k...*f....ol...(m...ol...on...*.s.C...y ...*f....ol...r.".p(....on...*f....o....r.".p(....on...*f....o....rY#.p(....(k...*.....o....r.#.p(....r...p(....r...p(....(....on...*f....o....r>$.p(....(k...*f....o....r.$.p(....(k...*f....o....r.%.p(....(k...*f....o... .ru%.p(....(k...*.~....:#...r.%.p(.....#...(....o....s.....~....*.~....*.~

C:\Users\user\AppData\Local\Temp\77CC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	321024
Entropy (8bit):	6.6866910329414475
Encrypted:	false
SSDEEP:	6144:pNL0PSBctyx4QHvdwUQGanoDqGY8oQ/0ADAhNS6m:pNAPSlX0GrWD870AMNS
MD5:	D8DF1D21042865E2220B0D688BAE6DC4
SHA1:	ADD58C361D687FEB8A6E44CC0992342F6F426B57
SHA-256:	C17E700DE39B64348D46DA0AC5F69F8279479289A9626BEB63C5ABDB7BCEF1F2
SHA-512:	42B2BF7381BD0AD57002BB0AF51A2C7B9436D4E4090063CC9EFDF864EEB374B65C9424EBCB7489F4536AF5467A77DAEB73308C4679AC82BC8111BEA472E8E68F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W.,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...Im}`..... .....@.....@.....D...P.....(.....@..... .....L.....text..... ..`.data.....@....hex.....@....suba.....@....vez.....@....rsrc... (.....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\8058.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....I.. ...`....@.. ..... ..@.....`I..K....`..... ..... ..H.....text....).. ...*..... ..`.rsrc.....`.....@....reloc..... .....0.....@..B.....I.....H.....?.....hX..}.....(....*..0.....(d...8....*.~....u...s....z&8.....8.....*.....*....(d...(....*...j*..... ..*.....*.....*.....*....(....*.~(....(^...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\D9EC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\D9EC.exe	
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\evjgtzc.exe	
Process:	C:\Users\user\AppData\Local\Temp\77CC.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14218752
Entropy (8bit):	3.786406643567547
Encrypted:	false
SSDEEP:	6144:NNL0PSBctyx4QHvdwUQGanoDqGY8oQ/0ADAhNS6m:NNAPSlX0GrWD870AMNS
MD5:	BBB91EAF2FB4CC1AA911FF4D555EC36D
SHA1:	98DC3BAF9081291CDF915D67B9D654117465A279
SHA-256:	EFA995DDEA80E0C9D2DD1A6D6E1BA5319D76984153D72A5FFDEFBC141C863B2B
SHA-512:	B5403EB01038BC6801BDB7AF565DCBD9F78EA91DD6BDD17A2EFDE18AF0B33F450A19C2A635D8F57DAF89BA182343DD556E24E978D6FF0B1A99BFB74EB2480A31
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...Im}`..... .....@.....@.....D...P.....(.....@..... .....L.....text..... ..`.data.....@....hex.....@....suba.....@....vez.....@....rsrc... (.....@..@.reloc..ZF.....X.....@..B..... .....

C:\Users\user\AppData\Roaming\ttfssdi	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	321536
Entropy (8bit):	6.696489645572037
Encrypted:	false
SSDEEP:	6144:AJfyOCHHmx9MGofauzMYFm6ggAc3DJbkLGrl6:A9onmx4ffPw6kc3FkLm
MD5:	6F48E0E76C5DFB3FC3AA45311FA6D0EF
SHA1:	981A29377351493CE6BCE4D3AEDEEC9034DEE056
SHA-256:	277AC2C203E37DCF3B71748E7DE0610BA4BF87DDBB7A19CBE7E6BE4CCE5ED175
SHA-512:	394F5C1E1E83EEA7A838270EDD90AE644B4A4F8F0009AC9F382400EA10960F04A4DF4EC8E10CD75ABA7FD9F3424C951BDC6015742899EC77AC666C05F09692D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...wi._.....@.....@.....).....d...P.....0.....@..... .....L.....text..... ..`.data.....@....vaxego.....@....gig.....@....hojotew.....@....rsrc.. .0.....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Roaming\ttfssdi:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\ttfssdi:Zone.Identifier	
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220115_030846_681.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3141361646616425
Encrypted:	false
SSDEEP:	96:BtCKIoCT2o+5K5+u9L/YAFC6SI2lfvkHM4QOT2zjFzoxNMCbdJRW:BELI6Tw02RtwQC3w
MD5:	927B70246B82E8AD324C06020435451F
SHA1:	41DAC7278D27522B4316A24AE60C2E78190018D1
SHA-256:	D6329A8ED63E4E96A0D31CE00D13086835E2A4621699A93F5A4F81C6C7A1D480
SHA-512:	55C145816A8F4E92E3C79E30F6BC7A6D6BEABC1305F9B07B079586F2EF1E96CC7F026CD8E0FF48F27A9C410E9FE4DCDE7786AE20DC4AD46F38E6DBC789F1D 22
Malicious:	false
Reputation:	unknown
Preview:	....!.....p.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1...../_8..... ....h..6.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.2.0.1.1.5._.0.3.0.8.4.6._.6.8.1...e.t.l.....P.P.....p..... .....

C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14218752
Entropy (8bit):	3.786406643567547
Encrypted:	false
SSDEEP:	6144:NNL0PSBctyx4QHvdwUQGanoDqGY8oQ/0ADAhNS6m:NNAPSlX0GrWD870AMNS
MD5:	BBB91EAF2FB4CC1AA911FF4D555EC36D
SHA1:	98DC3BAF9081291CDF915D67B9D654117465A279
SHA-256:	EFA995DDEA80E0C9D2DD1A6D6E1BA5319D76984153D72A5FFDEFBC141C863B2B
SHA-512:	B5403EB01038BC6801BDB7AF565DCBD9F78EA91DD6BDD17A2EFDE18AF0B33F450A19C2A635D8F57DAF89BA182343DD556E24E978D6FF0B1A99BFB74EB2480 A31
Malicious:	**true**
Reputation:	unknown

C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe (copy)	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L...!m}`..... .....@.....@.....D...P.....(.....@.....L.....text..... ..`.data.....@....hex.....@....suba.....@....vez.....@....rsrc...(.....@..@.reloc..ZF.....X.....@..B.....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.265179812909518
Encrypted:	false
SSDEEP:	12288:Ax+BOdPDqHjKi7fAOti2ulQ1Aap48xZk8tj8v7W8TKogE410qbDhDkbx:C+BOdPDqHjKi7fA0Egwx
MD5:	6AACC767C385FCA2EE1130CB536A2E41
SHA1:	6E32F8C0D1C95973831D0579FA644632A2C05DDB
SHA-256:	AC3162E77CDB85ABB007BB8EF33CC578204C157F406EE022299668116FEE247A
SHA-512:	F589967137ADE4ADA5E51ABA689EE22101ACCF9217DA2EBB7E83230BC88DCCDE15835A2C6570442CF7B44D60B5794AE2B5AEE976E1BCD6425FD7E029A810F5A0
Malicious:	false
Reputation:	unknown
Preview:	regfQ...Q...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmf..K.....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.7831703751847625
Encrypted:	false
SSDEEP:	384:/stDR5tZrdbdXp5/Qp8NXQnxOf2ofPmxwp+5GjZmGCIDTTVi5N5WeqESODe:UtXrjXpupLgf2oWxwpiWmGCWTVGN5nSO
MD5:	379E1E75362BB6743CCED68E1B4ACF52
SHA1:	D108BCB832E6863B71BEA1B7F6CBD98CD75BF935
SHA-256:	0B7EFBF7B662B46C164CD8D018BE3E2D8DC23BC07B4F98EBC5237B93BEF24511
SHA-512:	530F87B8BC13EC0FE7D96B677B6BDF405AC3FEE7A83C6A7AA646EA5A6D0B5905AFE63E139D26042A03A3D55DD17BB9C14740077D243A8A4A742533E9CB25EED4
Malicious:	false
Reputation:	unknown
Preview:	regfP...P...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmf..K.....

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBllydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8
SHA-512:	48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090F
Malicious:	false
Reputation:	unknown

\Device\ConDrv	
Preview:	..A specified value is not valid.....Usage: add rule name=<string>.. dir=in|out.. action=allow|block|bypass.. [program=<program path>].. [service=<service short name>|any].. [description=<string>].. [enable=yes|no (default=yes)].. [profile=public|private|domain|any[,...]].. [localip=any|<IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [localport=0-65535|<port range>[,...]|RPC|RPC-EPMap|IPHTTPS|any (default=any)].. [remoteport=0-65535|<port range>[,...]|any (default=any)].. [protocol=0-255|icmpv4|icmpv6|icmpv4:type,code|icmpv6:type,code|.. tcp|udp|any (default=any)].. [interfacetype=wireless|lan|ras|any].. [rmtcomputergrp=<SDDL string>].. [rmtusrgrp=<SDDL string>].. [edge=yes|deferapp|deferuser|no (default=no)].. [security=authenticate|authenc|authdynenc|authnoencap|

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.696489645572037
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	GNXG5XLBEH.exe
File size:	321536
MD5:	6f48e0e76c5dfb3fc3aa45311fa6d0ef
SHA1:	981a29377351493ce6bce4d3aedeec9034dee056
SHA256:	277ac2c203e37dcf3b71748e7de0610ba4bf87ddbb7a19cbe7e6be4cce5ed175
SHA512:	394f5c1e1e83eea7a838270edd90ae644b4a4f8f0009ac9f382400ea10960f04a4df4ec8e10cd75aba7fd9f3424c951bdc6015742899ec77ac666c05f09692d4
SSDEEP:	6144:AJfyOCHHmx9MGofauzMYFm6ggAc3DJbkLGrl6:A9onmx4ffPw6kc3FkLm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,...~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L...wi._.....

File Icon

Icon Hash:	c8d0d8e0f8e0f4e8

Static PE Info

General

Entrypoint:	0x41b840
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F906977 [Wed Oct 21 17:01:43 2020 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:	6801e04a0c2ca60ac2497c0d8723846b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e91e	0x3ea00	False	0.583777756986	data	6.97280495233	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.340983072917	data	3.46813100102	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.vaxego	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gig	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.hojotew	0x14f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x8730	0x8800	False	0.594985064338	data	5.82818673804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x465a	0x4800	False	0.344021267361	data	3.68094584687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
Assamese	India	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 19:09:10.061032057 CET	192.168.2.5	8.8.8.8	0xddd3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:10.540186882 CET	192.168.2.5	8.8.8.8	0x8cb0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.001127005 CET	192.168.2.5	8.8.8.8	0xb88a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.482151031 CET	192.168.2.5	8.8.8.8	0x9f8a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.671001911 CET	192.168.2.5	8.8.8.8	0xac73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.842314005 CET	192.168.2.5	8.8.8.8	0x8f08	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 19:09:13.487374067 CET	192.168.2.5	8.8.8.8	0x9857	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:13.655011892 CET	192.168.2.5	8.8.8.8	0xc3e6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:14.117935896 CET	192.168.2.5	8.8.8.8	0x5f4f	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:15.862174034 CET	192.168.2.5	8.8.8.8	0xb8b3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:16.343225002 CET	192.168.2.5	8.8.8.8	0x82e5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:16.538634062 CET	192.168.2.5	8.8.8.8	0xdc51	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:17.318478107 CET	192.168.2.5	8.8.8.8	0x4068	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:17.542150974 CET	192.168.2.5	8.8.8.8	0xfeed	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.053544998 CET	192.168.2.5	8.8.8.8	0x7a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.225140095 CET	192.168.2.5	8.8.8.8	0x6c1c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.414207935 CET	192.168.2.5	8.8.8.8	0xa496	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.574366093 CET	192.168.2.5	8.8.8.8	0xa674	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.755300045 CET	192.168.2.5	8.8.8.8	0x2ae1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.930671930 CET	192.168.2.5	8.8.8.8	0x45ad	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:22.103765011 CET	192.168.2.5	8.8.8.8	0x58fe	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:22.276225090 CET	192.168.2.5	8.8.8.8	0xc071	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:24.539366007 CET	192.168.2.5	8.8.8.8	0x9c96	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:24.708920956 CET	192.168.2.5	8.8.8.8	0x80f1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:24.883527040 CET	192.168.2.5	8.8.8.8	0xa1aa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:25.057566881 CET	192.168.2.5	8.8.8.8	0x44df	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.415585995 CET	192.168.2.5	8.8.8.8	0x6ce0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.608776093 CET	192.168.2.5	8.8.8.8	0xff0f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.781918049 CET	192.168.2.5	8.8.8.8	0x85c6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.971153021 CET	192.168.2.5	8.8.8.8	0xacf	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:29.799472094 CET	192.168.2.5	8.8.8.8	0xbf32	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:30.237000942 CET	192.168.2.5	8.8.8.8	0x6a35	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:30.404517889 CET	192.168.2.5	8.8.8.8	0x71eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.368099928 CET	192.168.2.5	8.8.8.8	0xf76c	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:46.057374954 CET	192.168.2.5	8.8.8.8	0x7543	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:51.701255083 CET	192.168.2.5	8.8.8.8	0xa402	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:51.869379044 CET	192.168.2.5	8.8.8.8	0xd245	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:52.061209917 CET	192.168.2.5	8.8.8.8	0xff90	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:52.685651064 CET	192.168.2.5	8.8.8.8	0x682f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:52.867140055 CET	192.168.2.5	8.8.8.8	0x6e11	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.037122011 CET	192.168.2.5	8.8.8.8	0xde79	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.203223944 CET	192.168.2.5	8.8.8.8	0xf614	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 19:09:53.369959116 CET	192.168.2.5	8.8.8.8	0xc24d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.533875942 CET	192.168.2.5	8.8.8.8	0xd299	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.705943108 CET	192.168.2.5	8.8.8.8	0xcff8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.905255079 CET	192.168.2.5	8.8.8.8	0x48d4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:54.187428951 CET	192.168.2.5	8.8.8.8	0x498f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:54.374730110 CET	192.168.2.5	8.8.8.8	0xc996	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:54.642282963 CET	192.168.2.5	8.8.8.8	0x8151	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.267733097 CET	192.168.2.5	8.8.8.8	0x5361	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.433132887 CET	192.168.2.5	8.8.8.8	0xc314	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.609422922 CET	192.168.2.5	8.8.8.8	0xf7c5	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.989248037 CET	192.168.2.5	8.8.8.8	0x4d2a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.160315990 CET	192.168.2.5	8.8.8.8	0xe30a	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.346404076 CET	192.168.2.5	8.8.8.8	0x8b73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.572753906 CET	192.168.2.5	8.8.8.8	0x42a6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.744287968 CET	192.168.2.5	8.8.8.8	0x5eb0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.939517021 CET	192.168.2.5	8.8.8.8	0x32e9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:59.110661030 CET	192.168.2.5	8.8.8.8	0xabae	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.348560095 CET	192.168.2.5	8.8.8.8	0x8611	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.543709993 CET	192.168.2.5	8.8.8.8	0x80e8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.731966019 CET	192.168.2.5	8.8.8.8	0xbba2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.919981003 CET	192.168.2.5	8.8.8.8	0x53bb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:08.140322924 CET	192.168.2.5	8.8.8.8	0x9f55	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:12.538479090 CET	192.168.2.5	8.8.8.8	0xf62c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:12.788062096 CET	192.168.2.5	8.8.8.8	0xe3c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:12.958772898 CET	192.168.2.5	8.8.8.8	0xf6dd	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:15.889401913 CET	192.168.2.5	8.8.8.8	0xd2d7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:16.059786081 CET	192.168.2.5	8.8.8.8	0xafa8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:16.257030964 CET	192.168.2.5	8.8.8.8	0xa528	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:17.758302927 CET	192.168.2.5	8.8.8.8	0x96fe	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:17.944961071 CET	192.168.2.5	8.8.8.8	0xe098	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:25.004935026 CET	192.168.2.5	8.8.8.8	0x8ab5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:25.170507908 CET	192.168.2.5	8.8.8.8	0x4602	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:25.353204966 CET	192.168.2.5	8.8.8.8	0x72b3	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:26.418530941 CET	192.168.2.5	8.8.8.8	0x8ec9	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:27.932214975 CET	192.168.2.5	8.8.8.8	0x970	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.099606991 CET	192.168.2.5	8.8.8.8	0xdb9e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.560112953 CET	192.168.2.5	8.8.8.8	0x7f32	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 19:10:28.724280119 CET	192.168.2.5	8.8.8.8	0x198c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.901891947 CET	192.168.2.5	8.8.8.8	0xa4fc	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:31.461930037 CET	192.168.2.5	8.8.8.8	0x387	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:32.138627052 CET	192.168.2.5	8.8.8.8	0xf4ee	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:32.386116982 CET	192.168.2.5	8.8.8.8	0x3a28	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:33.787772894 CET	192.168.2.5	8.8.8.8	0xe497	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:34.013952971 CET	192.168.2.5	8.8.8.8	0x6864	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:34.291979074 CET	192.168.2.5	8.8.8.8	0x5f07	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:35.669361115 CET	192.168.2.5	8.8.8.8	0xbe71	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:35.835163116 CET	192.168.2.5	8.8.8.8	0x130e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:36.012844086 CET	192.168.2.5	8.8.8.8	0x7e50	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.088051081 CET	192.168.2.5	8.8.8.8	0x490e	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.963994026 CET	192.168.2.5	8.8.8.8	0x6a1e	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:44.740060091 CET	192.168.2.5	8.8.8.8	0x55cc	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:44.765990973 CET	192.168.2.5	8.8.8.8	0x247b	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:44.972399950 CET	192.168.2.5	8.8.8.8	0xce19	Standard query (0)	ipwhois.app	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.654849052 CET	192.168.2.5	8.8.8.8	0xb7cd	Standard query (0)	c9d0e790b353537889bd47a364f5acff43c11f248.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.838181019 CET	192.168.2.5	8.8.8.8	0xbeca	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:47.321703911 CET	192.168.2.5	8.8.8.8	0x2e44	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:48.172898054 CET	192.168.2.5	8.8.8.8	0xa86a	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:57.879049063 CET	192.168.2.5	8.8.8.8	0x71c1	Standard query (0)	dl.uploadgram.me	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.204118013 CET	192.168.2.5	8.8.8.8	0xc8fa	Standard query (0)	yahoo.com	MX (Mail exchange)	IN (0x0001)
Jan 14, 2022 19:11:01.225033045 CET	192.168.2.5	8.8.8.8	0xd0a2	Standard query (0)	mta5.am0.yahoodns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:09:10.384404898 CET	8.8.8.8	192.168.2.5	0xddd3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:10.825388908 CET	8.8.8.8	192.168.2.5	0x8cb0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.314507008 CET	8.8.8.8	192.168.2.5	0xb88a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.499597073 CET	8.8.8.8	192.168.2.5	0x9f8a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:11.688426971 CET	8.8.8.8	192.168.2.5	0xac73	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:12.127974987 CET	8.8.8.8	192.168.2.5	0x8f08	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:13.506998062 CET	8.8.8.8	192.168.2.5	0x9857	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:09:13.966306925 CET	8.8.8.8	192.168.2.5	0xc3e6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:14.136221886 CET	8.8.8.8	192.168.2.5	0x5f4f	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:16.192797899 CET	8.8.8.8	192.168.2.5	0xb8b3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:16.360732079 CET	8.8.8.8	192.168.2.5	0x82e5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:16.852404118 CET	8.8.8.8	192.168.2.5	0xdc51	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:17.337629080 CET	8.8.8.8	192.168.2.5	0x4068	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:17.837946892 CET	8.8.8.8	192.168.2.5	0xfeed	No error (0)	privacy-tools-for-you-780.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.073492050 CET	8.8.8.8	192.168.2.5	0x7a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.244182110 CET	8.8.8.8	192.168.2.5	0x6c1c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.517277002 CET	8.8.8.8	192.168.2.5	0xa496	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.593890905 CET	8.8.8.8	192.168.2.5	0xa674	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.774349928 CET	8.8.8.8	192.168.2.5	0x2ae1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:21.949736118 CET	8.8.8.8	192.168.2.5	0x45ad	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:22.123107910 CET	8.8.8.8	192.168.2.5	0x58fe	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:22.587418079 CET	8.8.8.8	192.168.2.5	0xc071	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:24.557038069 CET	8.8.8.8	192.168.2.5	0x9c96	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:24.728074074 CET	8.8.8.8	192.168.2.5	0x80f1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:24.903656006 CET	8.8.8.8	192.168.2.5	0xa1aa	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:25.076198101 CET	8.8.8.8	192.168.2.5	0x44df	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.434825897 CET	8.8.8.8	192.168.2.5	0x6ce0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.628560066 CET	8.8.8.8	192.168.2.5	0xff0f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.801300049 CET	8.8.8.8	192.168.2.5	0x85c6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.991117954 CET	8.8.8.8	192.168.2.5	0xacf	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.991117954 CET	8.8.8.8	192.168.2.5	0xacf	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.991117954 CET	8.8.8.8	192.168.2.5	0xacf	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:27.991117954 CET	8.8.8.8	192.168.2.5	0xacf	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:09:27.991117954 CET	8.8.8.8	192.168.2.5	0xacf	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:30.085545063 CET	8.8.8.8	192.168.2.5	0xbf32	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:30.256505013 CET	8.8.8.8	192.168.2.5	0x6a35	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:30.421962976 CET	8.8.8.8	192.168.2.5	0x71eb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.396714926 CET	8.8.8.8	192.168.2.5	0xf76c	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.396714926 CET	8.8.8.8	192.168.2.5	0xf76c	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.396714926 CET	8.8.8.8	192.168.2.5	0xf76c	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.396714926 CET	8.8.8.8	192.168.2.5	0xf76c	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.396714926 CET	8.8.8.8	192.168.2.5	0xf76c	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:43.396714926 CET	8.8.8.8	192.168.2.5	0xf76c	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:46.160974026 CET	8.8.8.8	192.168.2.5	0x7543	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:51.718183994 CET	8.8.8.8	192.168.2.5	0xa402	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:51.889224052 CET	8.8.8.8	192.168.2.5	0xd245	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:52.358066082 CET	8.8.8.8	192.168.2.5	0xff90	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:52.703072071 CET	8.8.8.8	192.168.2.5	0x682f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:52.886606932 CET	8.8.8.8	192.168.2.5	0x6e11	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.056230068 CET	8.8.8.8	192.168.2.5	0xde79	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.222333908 CET	8.8.8.8	192.168.2.5	0xf614	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.389302015 CET	8.8.8.8	192.168.2.5	0xc24d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.551351070 CET	8.8.8.8	192.168.2.5	0xd299	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.725091934 CET	8.8.8.8	192.168.2.5	0xcff8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:53.922821999 CET	8.8.8.8	192.168.2.5	0x48d4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:54.206341982 CET	8.8.8.8	192.168.2.5	0x498f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:54.392158031 CET	8.8.8.8	192.168.2.5	0xc996	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:09:54.660291910 CET	8.8.8.8	192.168.2.5	0x8151	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.285299063 CET	8.8.8.8	192.168.2.5	0x5361	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.452198982 CET	8.8.8.8	192.168.2.5	0xc314	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.630558014 CET	8.8.8.8	192.168.2.5	0xf7c5	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:57.630558014 CET	8.8.8.8	192.168.2.5	0xf7c5	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.006366014 CET	8.8.8.8	192.168.2.5	0x4d2a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.180192947 CET	8.8.8.8	192.168.2.5	0xe30a	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.365708113 CET	8.8.8.8	192.168.2.5	0x8b73	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.593264103 CET	8.8.8.8	192.168.2.5	0x42a6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.764146090 CET	8.8.8.8	192.168.2.5	0x5eb0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:58.960181952 CET	8.8.8.8	192.168.2.5	0x32e9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:09:59.130079031 CET	8.8.8.8	192.168.2.5	0xabae	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.366018057 CET	8.8.8.8	192.168.2.5	0x8611	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.561201096 CET	8.8.8.8	192.168.2.5	0x80e8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.751497030 CET	8.8.8.8	192.168.2.5	0xbba2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:07.938688040 CET	8.8.8.8	192.168.2.5	0x53bb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:08.159094095 CET	8.8.8.8	192.168.2.5	0x9f55	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:12.556054115 CET	8.8.8.8	192.168.2.5	0xf62c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:12.807543993 CET	8.8.8.8	192.168.2.5	0xe3c9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:12.975985050 CET	8.8.8.8	192.168.2.5	0xf6dd	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:15.908402920 CET	8.8.8.8	192.168.2.5	0xd2d7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:16.078675985 CET	8.8.8.8	192.168.2.5	0xafa8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:16.582515955 CET	8.8.8.8	192.168.2.5	0xa528	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:17.777923107 CET	8.8.8.8	192.168.2.5	0x96fe	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:18.231518984 CET	8.8.8.8	192.168.2.5	0xe098	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:25.023981094 CET	8.8.8.8	192.168.2.5	0x8ab5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:10:25.189588070 CET	8.8.8.8	192.168.2.5	0x4602	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:25.382838011 CET	8.8.8.8	192.168.2.5	0x72b3	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:26.740726948 CET	8.8.8.8	192.168.2.5	0x8ec9	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:27.951181889 CET	8.8.8.8	192.168.2.5	0x970	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.408941984 CET	8.8.8.8	192.168.2.5	0xdb9e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.579654932 CET	8.8.8.8	192.168.2.5	0x7f32	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.743089914 CET	8.8.8.8	192.168.2.5	0x198c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:28.921109915 CET	8.8.8.8	192.168.2.5	0xa4fc	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:31.481004000 CET	8.8.8.8	192.168.2.5	0x387	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:32.155909061 CET	8.8.8.8	192.168.2.5	0xf4ee	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:32.403192043 CET	8.8.8.8	192.168.2.5	0x3a28	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:33.806910038 CET	8.8.8.8	192.168.2.5	0xe497	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:34.033373117 CET	8.8.8.8	192.168.2.5	0x6864	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:34.311547041 CET	8.8.8.8	192.168.2.5	0x5f07	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:35.688616037 CET	8.8.8.8	192.168.2.5	0xbe71	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:35.854535103 CET	8.8.8.8	192.168.2.5	0x130e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:36.034266949 CET	8.8.8.8	192.168.2.5	0x7e50	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.106853962 CET	8.8.8.8	192.168.2.5	0x490e	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.106853962 CET	8.8.8.8	192.168.2.5	0x490e	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.106853962 CET	8.8.8.8	192.168.2.5	0x490e	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.106853962 CET	8.8.8.8	192.168.2.5	0x490e	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.106853962 CET	8.8.8.8	192.168.2.5	0x490e	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.106853962 CET	8.8.8.8	192.168.2.5	0x490e	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.987297058 CET	8.8.8.8	192.168.2.5	0x6a1e	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:10:41.987297058 CET	8.8.8.8	192.168.2.5	0x6a1e	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.987297058 CET	8.8.8.8	192.168.2.5	0x6a1e	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.987297058 CET	8.8.8.8	192.168.2.5	0x6a1e	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:41.987297058 CET	8.8.8.8	192.168.2.5	0x6a1e	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:44.763099909 CET	8.8.8.8	192.168.2.5	0x55cc	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 19:10:44.788398981 CET	8.8.8.8	192.168.2.5	0x247b	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 19:10:44.996448040 CET	8.8.8.8	192.168.2.5	0xce19	No error (0)	ipwhois.app		136.243.172.101	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.672281027 CET	8.8.8.8	192.168.2.5	0xb7cd	No error (0)	c9d0e790b353537889bd47a364f5acff43c11f248.xyz		185.112.83.97	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.861773014 CET	8.8.8.8	192.168.2.5	0xbeca	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.861773014 CET	8.8.8.8	192.168.2.5	0xbeca	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.861773014 CET	8.8.8.8	192.168.2.5	0xbeca	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.861773014 CET	8.8.8.8	192.168.2.5	0xbeca	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:45.861773014 CET	8.8.8.8	192.168.2.5	0xbeca	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:47.343697071 CET	8.8.8.8	192.168.2.5	0x2e44	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:48.189995050 CET	8.8.8.8	192.168.2.5	0xa86a	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 14, 2022 19:10:57.902101040 CET	8.8.8.8	192.168.2.5	0x71c1	No error (0)	dl.uploadgram.me		176.9.247.226	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.223313093 CET	8.8.8.8	192.168.2.5	0xc8fa	No error (0)	yahoo.com			MX (Mail exchange)	IN (0x0001)
Jan 14, 2022 19:11:01.223313093 CET	8.8.8.8	192.168.2.5	0xc8fa	No error (0)	yahoo.com			MX (Mail exchange)	IN (0x0001)
Jan 14, 2022 19:11:01.223313093 CET	8.8.8.8	192.168.2.5	0xc8fa	No error (0)	yahoo.com			MX (Mail exchange)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		98.136.96.91	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		67.195.204.73	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		67.195.228.110	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		98.136.96.74	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		98.136.96.75	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		67.195.204.72	A (IP address)	IN (0x0001)
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		98.136.96.76	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 19:11:01.242662907 CET	8.8.8.8	192.168.2.5	0xd0a2	No error (0)	mta5.am0.yahoodns.net		67.195.228.106	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sasldotps.net
  - host-data-coin-11.com
- hvxghwlm.org
- gvuhy.com
- xcewx.net
- fuylvs.net
- ejshmyhdg.net
- fxdrjy.net
- pmdsi.net
- data-host-coin-8.com
- jvggxpunvp.net
- utujjcpga.com
- anaxqk.org
- aeoceljuvu.org
- privacy-tools-for-you-780.com
- tavpv.org
- ylklohfb.net
- unicupload.top
- snjxprkrs.net
- ognsyxbqt.net
- mqsidiop.net
- ffjbt.com
- xhmgc.org
- dlrkn.org
- hqphi.org
- hrbkqnyvuq.org
- 185.7.214.171:8080
- oanyhf.net

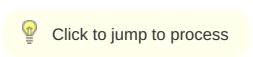
- ebkix.org
- kglcf.net
- ralhhxo.com
- ucqxo.com
- rvrxkhapq.org
- tmefv.org
- ublgjca.net
- uauswjxvxi.com
- ihlanbec.com
- ocvhk.net
- bunksfs.com
- bhqyvtr.org
- vvcoavsyoi.org
- mgspnorl.com
- jlttjsjsn.net
- lwmkqmxs.net
- wodlytuu.org
- opwshtlv.com
- iofaey.org
- ndvhcbnqxy.net
- slwqa.org
- mudbgksxf.com
- ltpsu.com
- lkdybspw.org
- tumar.com
- dxlbaxnq.com
- 81.163.30.181
- vmrsokyf.net
- kuhyti.org
- jhryuyevsi.com

- tsjnpmoxk.net
- dhgvgbi.net
- sthgmss.net
- lqucepm.org
- drivqge.com
- srpcpdlmu.net
- sbdfkwshp.net
- getygnekfa.net
- svqaek.com
- vcddpnrql.org
- lchxcgbqi.org
- ksxvhtvig.net
- nxrloqgt.org
- aeymga.org
- duekablkqo.com
- foilygkb.org
- babqykwmy.org
- ygspe.com
- sytacviqe.org

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: GNXG5XLBEH.exe PID: 3224 Parent PID: 5108

General

Start time:	19:08:25
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\GNXG5XLBEH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GNXG5XLBEH.exe"
Imagebase:	0x400000
File size:	321536 bytes
MD5 hash:	6F48E0E76C5DFB3FC3AA45311FA6D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: GNXG5XLBEH.exe PID: 6268 Parent PID: 3224

General

Start time:	19:08:26
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\GNXG5XLBEH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GNXG5XLBEH.exe"
Imagebase:	0x400000
File size:	321536 bytes
MD5 hash:	6F48E0E76C5DFB3FC3AA45311FA6D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.303363186.0000000000470000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.303673269.0000000002091000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3472 Parent PID: 6268

General

Start time:	19:08:33
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000000.288599943.000000000030E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6632 Parent PID: 556

General

Start time:	19:08:35
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 6912 Parent PID: 556

General

Start time:	19:08:43
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 6952 Parent PID: 556

General

Start time:	19:08:45
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7024 Parent PID: 556

General

Start time:	19:08:46
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7088 Parent PID: 556

General

Start time:	19:08:46
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 7156 Parent PID: 556

General

Start time:	19:08:47
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff64ff60000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5604 Parent PID: 556

General

Start time:	19:08:47
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6424 Parent PID: 556

General

Start time:	19:08:57
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: ttfssdi PID: 4512 Parent PID: 904

General

Start time:	19:09:09
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\ttfssdi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ttfssdi
Imagebase:	0x400000
File size:	321536 bytes
MD5 hash:	6F48E0E76C5DFB3FC3AA45311FA6D0EF
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: ttfssdi PID: 1284 Parent PID: 4512

General

Start time:	19:09:11
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\ttfssdi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ttfssdi
Imagebase:	0x400000
File size:	321536 bytes
MD5 hash:	6F48E0E76C5DFB3FC3AA45311FA6D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.354285300.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.354370443.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6600 Parent PID: 556

General

Start time:	19:09:14
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: 5BBC.exe PID: 6604 Parent PID: 3472

General

Start time:	19:09:14
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\5BBC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\5BBC.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs

Analysis Process: svchost.exe PID: 1064 Parent PID: 556

General

Start time:	19:09:18
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: 6B9B.exe PID: 6156 Parent PID: 3472

General

Start time:	19:09:19
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\6B9B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6B9B.exe
Imagebase:	0x400000
File size:	322048 bytes
MD5 hash:	039CCF44EF7B55AEB4D22D211D17774E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: WerFault.exe PID: 6204 Parent PID: 1064

General

Start time:	19:09:19
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6604 -ip 6604
Imagebase:	0x140000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 6B9B.exe PID: 6568 Parent PID: 6156

General

Start time:	19:09:21
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\6B9B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6B9B.exe
Imagebase:	0x400000
File size:	322048 bytes
MD5 hash:	039CCF44EF7B55AEB4D22D211D17774E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001A.00000002.375596550.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001A.00000002.375811349.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 3896 Parent PID: 6604

General

Start time:	19:09:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6604 -s 520
Imagebase:	0x140000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: 6BA5.exe PID: 1412 Parent PID: 3472

General

Start time:	19:09:23
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\6BA5.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6BA5.exe
Imagebase:	0x400000
File size:	324608 bytes
MD5 hash:	7E58C9178CBD9D56DB805F034EC795CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001C.00000002.368715638.0000000000869000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000001C.00000002.368715638.0000000000869000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: BackgroundTransferHost.exe PID: 240 Parent PID: 792

General

Start time:	19:09:23
Start date:	14/01/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff7505d0000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: 77CC.exe PID: 5196 Parent PID: 3472

General

Start time:	19:09:26
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\77CC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\77CC.exe
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	D8DF1D21042865E2220B0D688BAE6DC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001E.00000002.396801518.0000000002170000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001E.00000002.395583768.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001E.00000003.371626952.0000000002190000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 8058.exe PID: 5500 Parent PID: 3472

General

Start time:	19:09:28
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8058.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8058.exe
Imagebase:	0xd00000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
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: 0000001F.00000002.423233100.0000000004011000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: cmd.exe PID: 5716 Parent PID: 5196

General

Start time:	19:09:31
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\ceaplexz\
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5720 Parent PID: 5716

General

Start time:	19:09:32
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6480 Parent PID: 5196

General

Start time:	19:09:32
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\evjgtzc.exe" C:\Windows\SysWOW64\ceaplexz\
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6436 Parent PID: 6480

General

Start time:	19:09:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5984 Parent PID: 5196

General

Start time:	19:09:33
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create ceaplexz binPath= "C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe /d\"C:\Users\user\AppData\Local\Temp\77CC.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x8c0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5992 Parent PID: 5984

General

Start time:	19:09:34
Start date:	14/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 2076 Parent PID: 5196

General

Start time:	19:09:34
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description ceaplexz "wifi internet conection
Imagebase:	0x8c0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6116 Parent PID: 2076

General

Start time:	19:09:36
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 484 Parent PID: 5196

General

Start time:	19:09:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start ceaplexz
Imagebase:	0x8c0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5188 Parent PID: 484

General

Start time:	19:09:38
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 4864 Parent PID: 5196

General

Start time:	19:09:39
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x11f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: evjgtzc.exe PID: 4876 Parent PID: 556

General

Start time:	19:09:39
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ceaplexz\evjgtzc.exe /d"C:\Users\user\AppData\Local\Temp\77CC.exe"
Imagebase:	0x400000
File size:	14218752 bytes
MD5 hash:	BBB91EAF2FB4CC1AA911FF4D555EC36D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002B.00000003.399149809.0000000000620000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002B.00000002.401571286.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002B.00000002.402320315.0000000000660000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002B.00000002.402219986.0000000000600000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 5268 Parent PID: 4864

General

Start time:	19:09:39
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4020 Parent PID: 4876

General

Start time:	19:09:41
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xed0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002D.00000002.552204136.0000000002EE0000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis