ID: 553404
Sample Name:
ECD2MpEBSf.exe
Cookbook: default.jbs
Time: 20:27:34
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

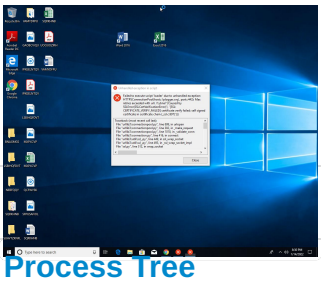
Windows Analysis Report ECD2MpEBSf.exe

Overview

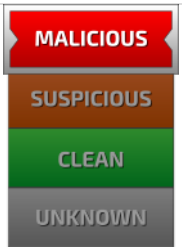
General Information

Sample Name:	ECD2MpEBSf.exe
Analysis ID:	553404
MD5:	31f0d01ee1fd687..
SHA1:	a45a34a020ad13..
SHA256:	8facf32116a5f68…
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



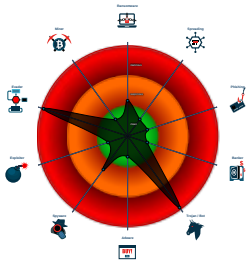
Raccoon RedLine SmokeLoader Tofsee Vidar

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…
- Yara detected Raccoon Stealer
- 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…

Classification



Process Tree

- **System is w10x64**
- ECD2MpEBSf.exe (PID: 7104 cmdline: "C:\Users\user\Desktop\ECD2MpEBSf.exe" MD5: 31F0D01EE1FD6876668692791657D97E)
  - ECD2MpEBSf.exe (PID: 7132 cmdline: "C:\Users\user\Desktop\ECD2MpEBSf.exe" MD5: 31F0D01EE1FD6876668692791657D97E)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - BB8A.exe (PID: 6816 cmdline: C:\Users\user\AppData\Local\Temp\BB8A.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 6968 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6816 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - CCB2.exe (PID: 6844 cmdline: C:\Users\user\AppData\Local\Temp\CCB2.exe MD5: 043B44289E31BD54357F9A5C21833259)
      - D936.exe (PID: 7124 cmdline: C:\Users\user\AppData\Local\Temp\D936.exe MD5: 9517CA2BC20EC061024C1209970CCD2E)
        - cmd.exe (PID: 6412 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\qeprvgom\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5468 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\krmdinzg.exe" C:\Windows\SysWOW64\qeprvgom\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 4608 cmdline: C:\Windows\System32\sc.exe" create qeprvgom binPath= "C:\Windows\SysWOW64\qeprvgom\krmdinzg.exe /d\"C:\Users\user\AppData\Local\Temp\D936.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6464 cmdline: C:\Windows\System32\sc.exe" description qeprvgom "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 1716 cmdline: "C:\Windows\System32\sc.exe" start qeprvgom MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 64 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 6744 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: 3716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 3D34.exe (PID: 6404 cmdline: C:\Users\user\AppData\Local\Temp\3D34.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 3D34.exe (PID: 2832 cmdline: C:\Users\user\AppData\Local\Temp\3D34.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 3D34.exe (PID: 472 cmdline: C:\Users\user\AppData\Local\Temp\3D34.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - A332.exe (PID: 6580 cmdline: C:\Users\user\AppData\Local\Temp\A332.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - CADF.exe (PID: 5628 cmdline: C:\Users\user\AppData\Local\Temp\CADF.exe MD5: CBE604877A46CEEBA112802BC17FFEF8)
        - CADF.exe (PID: 5504 cmdline: C:\Users\user\AppData\Local\Temp\CADF.exe MD5: CBE604877A46CEEBA112802BC17FFEF8)
      - D502.exe (PID: 2248 cmdline: C:\Users\user\AppData\Local\Temp\D502.exe MD5: 1B1E4286625BB189A526E910F2031C7B)
      - E3A9.exe (PID: 5272 cmdline: C:\Users\user\AppData\Local\Temp\E3A9.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
        - AppLaunch.exe (PID: 5620 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - FB58.exe (PID: 5136 cmdline: C:\Users\user\AppData\Local\Temp\FB58.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
- svchost.exe (PID: 6408 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3512 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- jgdhbua (PID: 6700 cmdline: C:\Users\user\AppData\Roaming\jgdhbua MD5: 31F0D01EE1FD6876668692791657D97E)
  - jgdhbua (PID: 6784 cmdline: C:\Users\user\AppData\Roaming\jgdhbua MD5: 31F0D01EE1FD6876668692791657D97E)
- svchost.exe (PID: 6680 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6964 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6876 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6816 -ip 6816 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6064 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- krmdinzg.exe (PID: 6888 cmdline: C:\Windows\SysWOW64\qeprvgom\krmdinzg.exe /d"C:\Users\user\AppData\Local\Temp\D936.exe" MD5: C8DE2E3F0DF5D9E1C126828B1444DBEA)
  - svchost.exe (PID: 3000 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- jgdhbua (PID: 5664 cmdline: C:\Users\user\AppData\Roaming\jgdhbua MD5: 31F0D01EE1FD6876668692791657D97E)
  - jgdhbua (PID: 6308 cmdline: C:\Users\user\AppData\Roaming\jgdhbua MD5: 31F0D01EE1FD6876668692791657D97E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\A4DE.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
00000001.00000002.721727855.00000000006A1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000005.00000000.708255964.00000000044C1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000020.00000002.800983655.00000000006C0000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000020.00000003.798724710.00000000007C0000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000026.00000000.825922987.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.ECD2MpEBSf.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
17.3.D936.exe.22d0000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
18.2.3D34.exe.430f910.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
18.2.3D34.exe.444ba90.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
32.2.krmdinzg.exe.400000.0.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 20 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:

Yara detected Raccoon Stealer

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

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)

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

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)

Tries to detect virtualization through RDTSC time measurements

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
- Modifies the windows firewall

Stealing of Sensitive Information:

- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- Yara detected Raccoon Stealer
- Yara detected Vidar stealer
- Yara detected Tofsee

Remote Access Functionality:

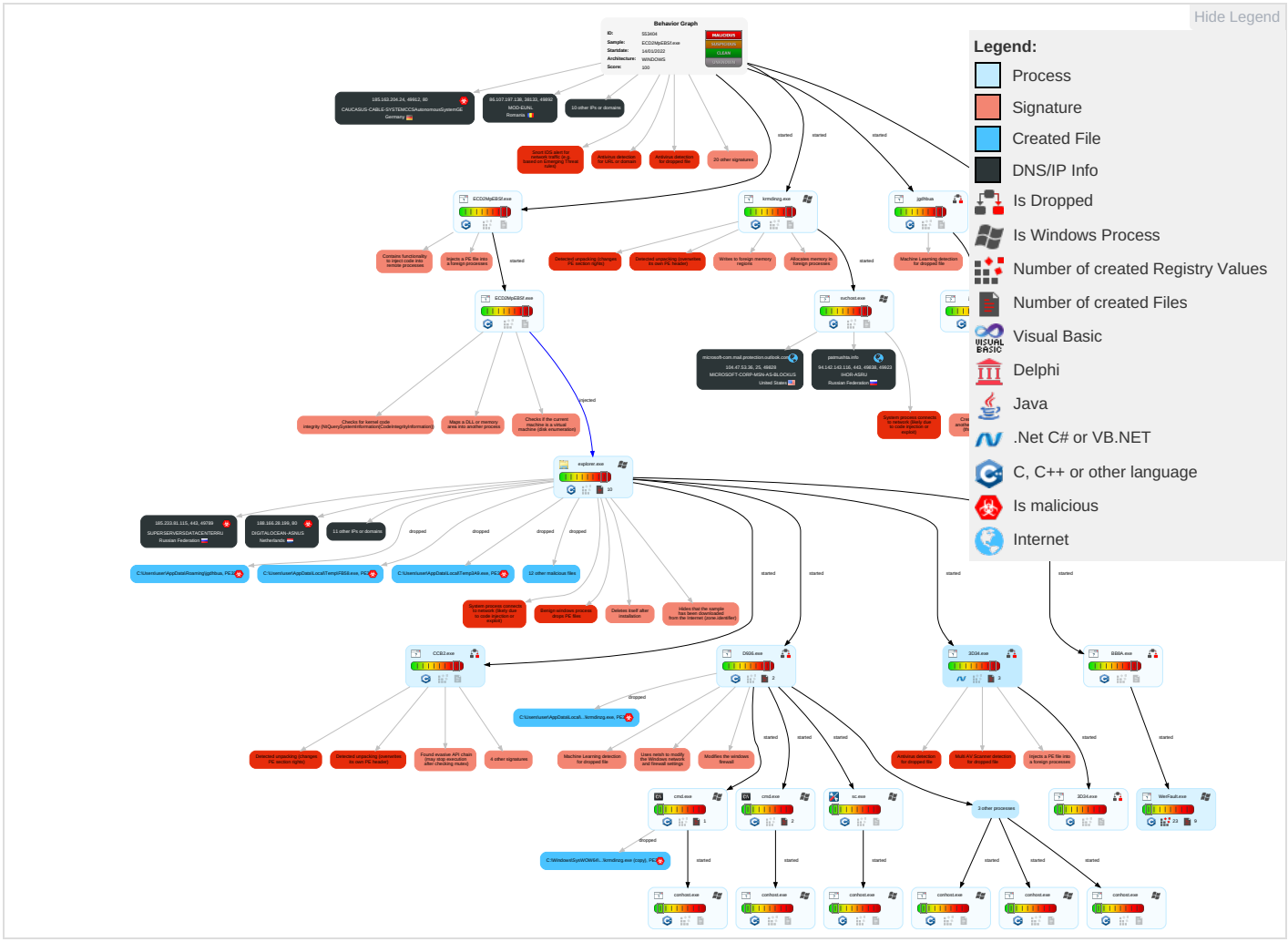
- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- Yara detected Raccoon Stealer
- Yara detected Vidar stealer
- Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts 1	Native API 5 3 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Exploitation for Client Execution 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Command and Scripting Interpreter 3	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	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	Service Execution 3	Logon Script (Mac)	Windows Service 1 4	Software Packing 4 3	NTDS	System Information Discovery 3 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Process Injection 7 1 3	Timestomp 1	LSA Secrets	Security Software Discovery 6 5 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Virtualization/Sandbox Evasion 2 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 3 1	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Proto
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
ECD2MpEBSf.exe	36%	Virustotal		Browse
ECD2MpEBSf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\888A.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\CADF.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\3D34.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\6C37.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D936.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\krmdinzg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jgdhbua	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CCB2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A332.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3D34.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A4DE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FB58.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E3A9.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D502.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BB8A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9889.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3D34.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3D34.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\6C37.exe	50%	ReversingLabs	Win32.Infostealer.Generic	
C:\Users\user\AppData\Local\Temp\A332.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\A332.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\A4DE.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
C:\Users\user\AppData\Local\Temp\BB8A.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\BB8A.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\FB58.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FB58.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.ECD2MpEBSf.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
11.0.jgdhbua.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.BB8A.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.3.D936.exe.22d0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.ECD2MpEBSf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.jgdhbua.6f15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.3D34.exe.ec0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.0.BB8A.exe.2080e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.D936.exe.22b0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.2.CCB2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.krmdinzg.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.0.ECD2MpEBSf.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.3D34.exe.ec0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.ECD2MpEBSf.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
1.2.ECD2MpEBSf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.BB8A.exe.2080e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.svchost.exe.e70000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
37.0.3D34.exe.150000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.3.BB8A.exe.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.ECD2MpEBSf.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
15.3.CCB2.exe.7b0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
32.3.krmdinzg.exe.7c0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.ECD2MpEBSf.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.0.jgdhbua.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.ECD2MpEBSf.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
12.0.BB8A.exe.2080e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.3D34.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.2.BB8A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.0.3D34.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.ECD2MpEBSf.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.1.jgdhbua.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.krmdinzg.exe.6c0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
32.2.krmdinzg.exe.7c0000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
0.2.ECD2MpEBSf.exe.5715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.BB8A.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.0.3D34.exe.150000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
17.2.D936.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
18.2.3D34.exe.ec0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
18.0.3D34.exe.ec0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
11.2.jgdhbua.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.0.3D34.exe.150000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
18.0.3D34.exe.ec0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
11.0.jgdhbua.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.CCB2.exe.680e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://185.163.204.24/	0%	Avira URL Cloud	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://81.163.30.181/l2.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://185.163.204.24//l/f/RGwRWn4BZ2GIX1a3oIgO/7e7a36a98c7545dda4f314e30bbcbe9a8ba64652	0%	Avira URL Cloud	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://74.201.28.62/book/KB5009812.png	0%	Avira URL Cloud	safe	
http://185.163.204.24//l/f/RGwRWn4BZ2GIX1a3oIgO/6bf5d5b41363c3e6b44705458de7ee6f935456db	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://185.163.204.22/capibar	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://74.201.28.62/book/KB5009812.exe	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://81.163.30.181/l3.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	8.209.70.0	true	false		high
github.com	140.82.121.4	true	false		high
patmushta.info	94.142.143.116	true	false		high
raw.githubusercontent.com	185.199.108.133	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.135.233	true	false		high
microsoft-com.mail.protection.outlook.com	104.47.53.36	true	false		high
iplogger.org	148.251.234.83	true	false		high
goo.su	172.67.139.105	true	false		high
transfer.sh	144.76.136.153	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://185.163.204.24/	true	• Avira URL Cloud: safe	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/l2.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://185.163.204.24//l/f/RGwRWn4BZ2GIX1a3oIgO/7e7a36a98c7545dda4f314e30bbcbe9a8ba64652	true	• Avira URL Cloud: safe	unknown
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://74.201.28.62/book/KB5009812.png	true	• Avira URL Cloud: safe	unknown
http://185.163.204.24//l/f/RGwRWn4BZ2GIX1a3oIgO/6bf5d5b41363c3e6b44705458de7ee6f935456db	true	• Avira URL Cloud: safe	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://185.163.204.22/capibar	true	• Avira URL Cloud: malware	unknown
http://74.201.28.62/book/KB5009812.exe	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.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
185.163.45.70	unknown	Moldova Republic of		39798	MIVOCLOUDMD	false
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
74.201.28.62	unknown	United States		35913	DEDIPATH-LLCUS	true
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
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
104.47.53.36	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
148.251.234.83	iplogger.org	Germany		24940	HETZNER-ASDE	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
185.163.204.22	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false
185.163.204.24	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553404
Start date:	14.01.2022
Start time:	20:27:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ECD2MpEBSf.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.evad.winEXE@58/27@91/19
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20.6% (good quality ratio 16%) • Quality average: 63% • Quality standard deviation: 39.5%
HCA Information:	• Successful, ratio: 60% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:29:09	Task Scheduler	Run new task: Firefox Default Browser Agent D3FD9BFE35A9B440 path: C:\Users\user\AppData\Roaming\jgd hbua
20:29:20	API Interceptor	1x Sleep call for process: CCB2.exe modified
20:29:30	API Interceptor	8x Sleep call for process: svchost.exe modified
20:29:34	API Interceptor	1x Sleep call for process: WerFault.exe modified
20:30:03	API Interceptor	1x Sleep call for process: D502.exe modified
20:30:05	API Interceptor	6x Sleep call for process: A332.exe modified

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\Windows\WER\ReportQueue\AppCrash_BB8A.exe_be9cde9f8afa847dd729874ac7bf4b4f63becc5_1db953ea_1aa14f53\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8138648214423995
Encrypted:	false
SSDEEP:	96:EMFoXBw0L4UB8OQoJ7R3V6tpXIQcQec6tycEfcw3W+HbHg/8BRTf3o8Fa9iVfOy4:NiXB4UF8HQ0lrjlq/u7sOS274ItL
MD5:	35C09D408A6C338FC99B4D619F09234D
SHA1:	B557CC04365F06A74899D2F89A372B92FBB1385F
SHA-256:	CBE31A4DBB4EE6246323C74A4D8636EB77A11BF8A6BFE3842D16AF7B39046AC6
SHA-512:	23E8BB9EC9DB20EDB7C3F061B36208031697495FA4F1FA1164E464EB6011EC43ADD2BDDF616182DE93E436D977E4F0ADCD8ABC7DA6A297C10E57133DFF7A5CB7
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.=.1.3.2.8.6.6.6.2.1.6.3.4.4.6.0.5.1.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.6.2.1.7.2.6.0.2.2.6.4.8.....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.=.2.6.7.7.6.f.3.1.-.3.9.c.1.-.4.4.4.8.-.a.6.5.d.-.1.5.b.c.e.0.d.7.7.d.d.6.....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.=.9.2.7.9.5.a.6.1.-.b.2.1.1.-.4.7.d.a.-.8.1.1.a.-.f.b.9.d.d.9.f.7.2.2.b.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.=.B.B.8.A...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.a.a.0.-.0.0.0.1.-.0.0.1.b.-.1.f.6.e.-.b.b.0.2.7.d.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.e.8.8.d.1.e.9.a.d.e.e.6.3.e.f.3.0.e.9.c.4.2.3.1.7.4.c.7.6.e.c.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.!.B.B.8.A...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\WER6175.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52702
Entropy (8bit):	3.051899513483229
Encrypted:	false
SSDEEP:	1536:DMHZ0DVisN/xdUMvGpto675v1yc+Jqh//W:DMHZ0DVisN/xdUMvGpto675v1yc+Jy/u
MD5:	2DEB23693D4D6D1F0B30650211014B40
SHA1:	72E6E6CE2182B1A1C1AF4A0A3CEB2DF043DD8191
SHA-256:	A481D7F7B26B38CCF3929C4927AD03DA25B187C1C7DE77B62CB298A78A11E31E
SHA-512:	B0FB53ECD8DD88A06B32E2FBFE112E4CC7FB15595C30F2D59A9E5B7A7F2F35755B82C5DDBB7CD9C7AF227E80D44149B15251CAD6E1DCB42FFB9D172FE2CB5B85
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6175.tmp.csv	
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:\ProgramData\Microsoft\Windows\WER\Temp\WER65FA.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6957049550715424
Encrypted:	false
SSDEEP:	96:9GiZYWEcslyQrYLYQFW0HlYEZAut6izqFXew3OnLMia+U0/q2uIC03:9jZDExs4FeLba+U0/q25C03
MD5:	07F06FDC5DEA39B6918FC620424D43B0
SHA1:	AFA91D954F8DB12AEC97F6FF59F6746442D2A7E8
SHA-256:	EC9A9FD75480B2FACDDAB5125C6E85115E1BF11E991AFD983FBE00112B774021
SHA-512:	2D1100B7E3CF54785103B166187A243D718A93467C1909D8D20BD59450D637ACE16A1F913A100557775AC318D3D9CA6B984A44862902AD6346DABB9640CFC449
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\WERAE40.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 19:29:24 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36708
Entropy (8bit):	2.1273152419502526
Encrypted:	false
SSDEEP:	192:+tJjOn9V/XOeh0kIKTZv5A6KX58TGX9VcNuCuTX4J+EnD3:EebZvyJufJhD3
MD5:	B8C8DEEC4450644C4227E014A2F987EF
SHA1:	66326B9DCCAEC52DBF078174D55669422F63F8F4
SHA-256:	7961AB36D2264DDD76223C005CF57840E173C220670F6850DAD3CD4D2F6041D8
SHA-512:	51098772159BCEFF9B35993AC7E7AA43B751DE986CEBBF61CBD80C5271827DF9ACDD78CCB06BE89F1B2000C630EA3B69EB1771BE8DC72D3BD0520BD6DAAD1DE
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....a.....$...z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERB4E9.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):	8392
Entropy (8bit):	3.702812242647528
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZq6q6YrRSUdNgmfGRSV+pDD89bw9sfNQm:RrlsNik6q6Y9SUHgmfGRS9w2fv
MD5:	C3E4A8A325B469EFC2F80337215A25E0
SHA1:	7D9597D4BA2C8F1AA5F9698D9AC14E33276F309A
SHA-256:	323F3D032F6993091B78A9A6710F627860E006AB94D4C6CBDD1E633309E27221
SHA-512:	56310025638F81BEA8509B8B3EA414E79F18F3EC41E9C026B941A463A59AB0C025876B1F4412371DD75922931C4EF1B8C4793EF4D51FE04E70A7946606C0EEF6
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E9.tmp.WERInternalMetadata.xml	
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.>.6.8.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB9CC.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):	4.477856827118253
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI9BtWSC8Bu8fm8M4Jd8qF0qv+q8vx8SbTFHOed:ulTfl+cSN9JHvK3bhHOed
MD5:	F002D88880F6E1E2E1F1BDE33239C82B
SHA1:	5AA9856DE403B3B4FCE7154CD49B26FF9BE665FB
SHA-256:	78885C4292C966EED96C82261A11912DBD801F44BA2283A7BE01E016751A5452
SHA-512:	A64ADF5872BA2DBA40F80F1498000F96F2D310A9A582C84B1F3D01F1311372B69309BAAF0583111AE35880569203172D79EABFD4448C5AA253303084BC0FC4B5
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="1342360" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3D34.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\3D34.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
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\Temp\3D34.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% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\3D34.exe

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\6C37.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\888A.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\9889.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

C:\Users\user\AppData\Local\Temp\9889.exe

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\A332.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
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
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....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..''?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\A4DE.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:	29D672F0BB8AEE885F008F7B7EBED499E7C5D8738B9373BF169896BE85C271FAAB5BD9792C176C7CDCB1C39606F07041E1E54E8F893D1D91F49509DF927AA8A 0
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\A4DE.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!.....0..J.....rh... .....@.. .....1... .@..... h..O.....Tg..8..... ....H.....text....H... ...J..... ..`.rsrc.....L.....@..@.relo c.....N.....@..B.....Th.....H.....C..''.....e..p.....^..}.....(.....(.....*..*..0.....(...%.-...(.....s.....s..... ....o..... ....o.....(....r...p o..... ....s.....o.....[o....o.....o ....[o....o!.....o''.....o#....s$.....io%.....o&.....,...o'.....o(.....,.o'.....,.o'.....+...*..(.....''.....0.....o).....(*.....s +....+..*...0.....s,.... ....(-.....(.....r%..po/.

C:\Users\user\AppData\Local\Temp\BB8A.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/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0 ECB

C:\Users\user\AppData\Local\Temp\BB8A.exe

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\CADF.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:	86F3946B813FB457D95B6635FA308DA1BF5F2C0FBD5BDCA75F7776D1A01A2D3C67A8A9E268DCC145FF575D70FBE84BE9BEB112A0D2269B955795C74468C0059 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\CCB2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	324608
Entropy (8bit):	6.705560699768563
Encrypted:	false
SSDEEP:	6144:8cXfhxLWOCPRZa9XQ9XuxYADj5QTM44lq46Ue:8cXfhxKPZyK+x3NQN4l3Je
MD5:	043B44289E31BD54357F9A5C21833259
SHA1:	C042C1D364887BBF71B070C8DD6C66C08A818834
SHA-256:	8DC59F6481C6FE183ADAC2B720FFA276CC9F52D83521200B1A85BB5FF8E4046A
SHA-512:	AC7098ED6CC6922577D0C87F4E3BA6EF32973C1641C98B3C675EFBBC548A63346DE87A0026ADB850144B120604BB7B9982A69E1AA2859D0E0A3A0CCE0857375
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L...o.}`.....P.....@.....[.....t...P.....(.....@.....L.....text..... ..`.data.....@....zic.....@....wuvuhus.....@....jufot.....@....rsrc...(.....$.....@..@.reloc..dF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\D502.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	54272
Entropy (8bit):	4.125149292696976
Encrypted:	false
SSDEEP:	192:s7yxMfjf6NrLqKZ6mXS9LzL1pvULIRPqY2F3991ZuBhyY8PGCz9QwAOSZCGQyBbf:KyufjSLq86mXS9LzLdqY2LHZ4cZA
MD5:	1B1E4286625BB189A526E910F2031C7B
SHA1:	650C0550F12C65D9841D10AB589FF39261018957
SHA-256:	C9D7CB68DEC80469C3C03B0E90C7AF1972462CA7779424DB3BFD9D44AEBAA624
SHA-512:	68F2366606B658FDDB2B5E9BAE2E6931FB455A230F8A4813EACB38A3D7853B9640F46FE9EE6FFD9862A509558B66C30A3494CB7231C3EF7CD784950771273155

C:\Users\user\AppData\Local\Temp\D502.exe

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....vL....."...0.....5... ...@....@.. ....@.....4..O....@..\.....4..... ....H.....text..... ....`.rsrc...\....@.....@..@.rel oc.....@..B.....4.....H.....#..`.....3.....0..:.....(.....(....(.....s.....o.....(.....(....(.....+..*".(....*..0..... ...(....r...p.....%.." ...(.....(.....%. N..."....o....&. ....(.....&.....&...(....r...pr5..pr9..p(.....%..'...(.....(....s.....%.r;..p.o....t.....+..*.....B..Q.....0..7.....(.....,.....i(.....(.....o....&s .....(... .o!...o"....s#.....o$.....+...(%.....o&...o'.....((..

C:\Users\user\AppData\Local\Temp\D936.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.685128709167328
Encrypted:	false
SSDEEP:	6144:BVMH4gQJqHQsl0yMo5DLaniwlnKh8MKxjDSmoETpqy:BVMY+lGiLlqKhexjpoEH
MD5:	9517CA2BC20EC061024C1209970CCD2E
SHA1:	5A3886349DEB4B7E6BA272304779C0C050BCDDCB
SHA-256:	07750C17A95131F145A3CD2418E0BBF031963537C7F2A1BCB4AEAB1D63EC8510
SHA-512:	51E289B0AC2F7D3083666B7707C415BE5EFC18CB8F4592288ADF768BF3990A6150A99F8B46FA283F74DE6D9556C9886303DA3E5D6A6B60E6BE0E086B2B230044
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...Q..._.....@.....P.....(.....@..... ....L.....text..... ..`.data.....@....lih.....@....cazelob.....@....pox.....@....rsrc... (.....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\E3A9.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\FB58.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
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\FB58.exe

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....$..................g.....q.l....v....h......E....x.....f.....c...Rich..................PE..L....[._. ....2.......0.......0....@..........................P\|......q.....................................Xf..(....p.. ....1.............................@Y..@............0..............................text.......... .. ..`.rdata.."?...0...@...$.............@..@.data...8....p.......d.............@....rsrc... .n..p.....................@..@..

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

Process:	C:\Users\user\AppData\Local\Temp\D936.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10624000
Entropy (8bit):	3.8323533062805604
Encrypted:	false
SSDEEP:	12288:GVMY+lGiLlqKhexjpoEHQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ3:SIl0I4jq
MD5:	C8DE2E3F0DF5D9E1C126828B1444DBEA
SHA1:	568F6EDAFCFAA907DC199443324666D4F7BA6BFB
SHA-256:	B62D0D45AB934497D91566E94D2FA277A6726CEC40DD4D50CFEC6F898E43A538
SHA-512:	20BED97AB819B162DE12BCF7942B254339E5F263478781B272AF943DB03691EA8EC3F130AE97F72C0289DA0BA320929BEDFC900CAA4EDAB4B76FEB066194901 4
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...Q.._...@...P.......(..@........... ....L............................text............................... ..`.data...............................@....lih...............................@....cazelob...........................@....pox...............................@....rsrc... (...........................@..@.reloc..ZF.........................@..B.. ....

C:\Users\user\AppData\Roaming\jgdhbua

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.688597828759442
Encrypted:	false
SSDEEP:	6144:zVMKim/rLWU5lbsbe8USFaX6EUNoO3Ez5B+D240obIIZfGd:zVMkfCeiFNbmOUFB+T0oXud
MD5:	31F0D01EE1FD6876668692791657D97E
SHA1:	A45A34A020AD13C9373BD14C45268004F505E1E1
SHA-256:	8FACF32116A5F68467C71032D3A207ABAA20FBCC56FCAB6A3DB650B4D30AD115
SHA-512:	7E737CFE1DB59AEF0BADA3184C059720EBB5744ADD725246E5A600E6CC1A3B6D0AA6B19EC6B90F5C1C1C0253D96B7A8C390594A9E0D14E35F45C9DBD10899 7A
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.......(...............................................................@........... ....L............................text...~............................ ..`.data...............................@....kipex..............................@....him...............................@....hakir.............................@....rsrc... (...........................@..@.reloc..ZF.......H..................@..B.. ....

C:\Users\user\AppData\Roaming\jgdhbua:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**

C:\Users\user\AppData\Roaming\jgdhbua:Zone.Identifier	
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\SysWOW64\qeprvgom\krmdinzg.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10624000
Entropy (8bit):	3.8323533062805604
Encrypted:	false
SSDEEP:	12288:GVMY+lGiLlqKhexjpoEHQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ3:SIl0I4jq
MD5:	C8DE2E3F0DF5D9E1C126828B1444DBEA
SHA1:	568F6EDAFCFAA907DC199443324666D4F7BA6BFB
SHA-256:	B62D0D45AB934497D91566E94D2FA277A6726CEC40DD4D50CFEC6F898E43A538
SHA-512:	20BED97AB819B162DE12BCF7942B254339E5F263478781B272AF943DB03691EA8EC3F130AE97F72C0289DA0BA320929BEDFC900CAA4EDAB4B76FEB066194901 4
Malicious:	**true**
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...Q.._..@...P.......(..@.......... ....L...........................text.............................. ..`.data..............................@....lih...............................@....cazelob...........................@....pox...............................@....rsrc... (..........................@..@.reloc..ZF.........................@..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):	4.237236426202636
Encrypted:	false
SSDEEP:	12288:FHIJeoqgeg5Fu/+BTQ9S1gTbMzZHogTtvN7r8XcfGa+2LXOU:lIJeoqgeg5I/+BjuM
MD5:	01943BF0494A56FD1AF5097441A3E2FC
SHA1:	4CF795A460778BD03A6A2749446779DDCDFCEC54
SHA-256:	862DA49FCA1E84DA44B0D9C45AD8508A03150FF8507F67620DB7AE11996AC6CB
SHA-512:	5779CCC50C91B4407A3E4DE37335B04E8D6DDC6276C5D75588E566975096EF057B444BD7AC22ACCD223AFF7FA79BB9FEF4475584DC3A76DD6C7DA54D33675D C
Malicious:	false
Reputation:	unknown
Preview:	regfH...H...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.rmtm....}... ....Y.Z.. ....

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):	20480
Entropy (8bit):	3.3450377575042998
Encrypted:	false
SSDEEP:	384:ybC5K5th4KgnVVeeDzei1NKZtjaT8GNwf3JC1M8l:i8KZg/eeDzesNYtjnGNwf2M8
MD5:	A2DE4322DAE6C2648B667D68B52FD8FF
SHA1:	B54F25C4DA3A3B828D3226F549164FDC540FF1B4
SHA-256:	F914769C1902117E0711746610EB7EE84F726B27CF539EC2B72214C58FD858EE
SHA-512:	3B53D772597F6654B54F9B8EC024DF9FAFD90BE702BB13FC3E1E95B257E165756388143DAD362F5CAA874DA6446180B6A42A287FBAC84D49FEE37628F3019259
Malicious:	false
Reputation:	unknown
Preview:	regfG...G...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.rmtm....}... ....Y.ZHvLE.N......G...........L..A..O."...~...................... ..hbin................p.\..,..........nk,.....}................................ ....&...{ad79c032-a2ea-f756-e377-7 2fb9332c3ae}......nk .....}....... ....Z......................Root........lf......Root....nk .....}................................ ....*...............DeviceCensus................... ...vk.................WritePermissionsCheck.......p...

\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
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):	6.688597828759442
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:	ECD2MpEBSf.exe
File size:	320512
MD5:	31f0d01ee1fd6876668692791657d97e
SHA1:	a45a34a020ad13c9373bd14c45268004f505e1e1
SHA256:	8facf32116a5f68467c71032d3a207abaa20fbcc56fcab6a3db650b4d30ad115
SHA512:	7e737cfe1db59aef0bada3184c059720ebb5744add72524 6e5a600e6cc1a3b6d0aa6b19ec6b90f5c1c1c0253d96b7 a8c390594a9e0d14e35f45c9dbd1089917a
SSDEEP:	6144:zVMKim/rLWU5lbsbe8USFaX6EUNoO3Ez5B+D2 40obIIZfGd:zVMkfCeiFNbmOUFB+T0oXud
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.....`.....

File Icon

Icon Hash:	c8d0d8e0f8e0f4e8

Static PE Info

General

Entrypoint:	0x41b4a0
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:	0x60A4EF0B [Wed May 19 10:57:15 2021 UTC]

General

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	0x3e57e	0x3e600	False	0.582117359719	data	6.96486152385	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.340657552083	data	3.47052178831	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.kipex	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.him	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.hakir	0x14f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x8728	0x8800	False	0.594812729779	data	5.84048651179	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x465a	0x4800	False	0.347710503472	data	3.69715033583	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 20:29:09.717817068 CET	192.168.2.4	8.8.8.8	0xc52	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.181456089 CET	192.168.2.4	8.8.8.8	0x50b7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.642838955 CET	192.168.2.4	8.8.8.8	0xc074	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.815781116 CET	192.168.2.4	8.8.8.8	0xdff0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.981431007 CET	192.168.2.4	8.8.8.8	0x1085	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:11.163989067 CET	192.168.2.4	8.8.8.8	0xa4aa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:12.559750080 CET	192.168.2.4	8.8.8.8	0xa259	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:13.018269062 CET	192.168.2.4	8.8.8.8	0x778e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:13.470618010 CET	192.168.2.4	8.8.8.8	0x833b	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:15.160757065 CET	192.168.2.4	8.8.8.8	0x3a22	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:15.331547976 CET	192.168.2.4	8.8.8.8	0xd7c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:15.498477936 CET	192.168.2.4	8.8.8.8	0x4bcf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.069087982 CET	192.168.2.4	8.8.8.8	0xa142	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.254492044 CET	192.168.2.4	8.8.8.8	0x4c77	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.430603027 CET	192.168.2.4	8.8.8.8	0x81eb	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.583122015 CET	192.168.2.4	8.8.8.8	0xc787	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.754019022 CET	192.168.2.4	8.8.8.8	0x40fb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.923821926 CET	192.168.2.4	8.8.8.8	0xca44	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:17.383294106 CET	192.168.2.4	8.8.8.8	0x863	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:17.549067974 CET	192.168.2.4	8.8.8.8	0x9726	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:19.420042992 CET	192.168.2.4	8.8.8.8	0x96a6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:19.596793890 CET	192.168.2.4	8.8.8.8	0xe326	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:19.781554937 CET	192.168.2.4	8.8.8.8	0x1a4e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:20.140119076 CET	192.168.2.4	8.8.8.8	0x4a7f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.354924917 CET	192.168.2.4	8.8.8.8	0x10bc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.519073963 CET	192.168.2.4	8.8.8.8	0xaddd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.720685959 CET	192.168.2.4	8.8.8.8	0x5f8e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.898070097 CET	192.168.2.4	8.8.8.8	0x1acd	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:25.476651907 CET	192.168.2.4	8.8.8.8	0xf661	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:25.665709019 CET	192.168.2.4	8.8.8.8	0x14c4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:25.838196993 CET	192.168.2.4	8.8.8.8	0xe7cb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:35.077847004 CET	192.168.2.4	8.8.8.8	0x9952	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:37.770320892 CET	192.168.2.4	8.8.8.8	0x3059	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:47.191591024 CET	192.168.2.4	8.8.8.8	0x55ea	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:47.362592936 CET	192.168.2.4	8.8.8.8	0x7678	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 20:29:47.820290089 CET	192.168.2.4	8.8.8.8	0xcf52	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.001112938 CET	192.168.2.4	8.8.8.8	0xbff0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.171740055 CET	192.168.2.4	8.8.8.8	0xa2f1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.384460926 CET	192.168.2.4	8.8.8.8	0x8df1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.576780081 CET	192.168.2.4	8.8.8.8	0x4328	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.759460926 CET	192.168.2.4	8.8.8.8	0xfe2b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.955866098 CET	192.168.2.4	8.8.8.8	0xd0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.140610933 CET	192.168.2.4	8.8.8.8	0x4039	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.306057930 CET	192.168.2.4	8.8.8.8	0xa0aa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.476068974 CET	192.168.2.4	8.8.8.8	0xc6d3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.657352924 CET	192.168.2.4	8.8.8.8	0x8431	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.830569029 CET	192.168.2.4	8.8.8.8	0x8d3d	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.056298018 CET	192.168.2.4	8.8.8.8	0xee16	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.218890905 CET	192.168.2.4	8.8.8.8	0xdf9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.380956888 CET	192.168.2.4	8.8.8.8	0xbc85	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.825635910 CET	192.168.2.4	8.8.8.8	0xc6ed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.002545118 CET	192.168.2.4	8.8.8.8	0xafa7	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.220135927 CET	192.168.2.4	8.8.8.8	0xce80	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.391541004 CET	192.168.2.4	8.8.8.8	0x66db	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.554003000 CET	192.168.2.4	8.8.8.8	0x75ac	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.713959932 CET	192.168.2.4	8.8.8.8	0x81b7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.879584074 CET	192.168.2.4	8.8.8.8	0x3011	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:02.214329958 CET	192.168.2.4	8.8.8.8	0x5c1a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:02.380536079 CET	192.168.2.4	8.8.8.8	0xee93	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.107853889 CET	192.168.2.4	8.8.8.8	0xa06f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.271703959 CET	192.168.2.4	8.8.8.8	0xce9b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.445702076 CET	192.168.2.4	8.8.8.8	0x87ab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.621660948 CET	192.168.2.4	8.8.8.8	0x4535	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:11.996265888 CET	192.168.2.4	8.8.8.8	0xcf0a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:12.182595968 CET	192.168.2.4	8.8.8.8	0xbcea	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:12.377898932 CET	192.168.2.4	8.8.8.8	0x475c	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:17.901901960 CET	192.168.2.4	8.8.8.8	0xe8c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:18.180469036 CET	192.168.2.4	8.8.8.8	0x2817	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:18.268348932 CET	192.168.2.4	8.8.8.8	0xfb9d	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:18.416841030 CET	192.168.2.4	8.8.8.8	0xe2eb	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:20.727615118 CET	192.168.2.4	8.8.8.8	0xf1ed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:20.905186892 CET	192.168.2.4	8.8.8.8	0x38f1	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 20:30:23.109894991 CET	192.168.2.4	8.8.8.8	0xcf31	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:27.657519102 CET	192.168.2.4	8.8.8.8	0x803b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:27.846710920 CET	192.168.2.4	8.8.8.8	0x4d74	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.016140938 CET	192.168.2.4	8.8.8.8	0xdb9b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.256848097 CET	192.168.2.4	8.8.8.8	0xfaf7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.459739923 CET	192.168.2.4	8.8.8.8	0x78e4	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.469984055 CET	192.168.2.4	8.8.8.8	0xcb6	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:31.864511967 CET	192.168.2.4	8.8.8.8	0xa7eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:32.156472921 CET	192.168.2.4	8.8.8.8	0xe5f1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:32.393162012 CET	192.168.2.4	8.8.8.8	0xcd5e	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:34.850267887 CET	192.168.2.4	8.8.8.8	0xef5d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.069546938 CET	192.168.2.4	8.8.8.8	0xe884	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.279342890 CET	192.168.2.4	8.8.8.8	0xd4ee	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.785237074 CET	192.168.2.4	8.8.8.8	0x7bd0	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:42.930880070 CET	192.168.2.4	8.8.8.8	0x2726	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:44.214027882 CET	192.168.2.4	8.8.8.8	0x3fe1	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:44.502847910 CET	192.168.2.4	8.8.8.8	0xc3	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:48.241736889 CET	192.168.2.4	8.8.8.8	0xee5a	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:31:08.601046085 CET	192.168.2.4	8.8.8.8	0x1b20	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:29:10.019198895 CET	8.8.8.8	192.168.2.4	0xc52	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.490426064 CET	8.8.8.8	192.168.2.4	0x50b7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.660072088 CET	8.8.8.8	192.168.2.4	0xc074	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:10.833611012 CET	8.8.8.8	192.168.2.4	0xdff0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:11.001287937 CET	8.8.8.8	192.168.2.4	0x1085	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:11.183374882 CET	8.8.8.8	192.168.2.4	0xa4aa	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:12.869715929 CET	8.8.8.8	192.168.2.4	0xa259	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:13.305824041 CET	8.8.8.8	192.168.2.4	0x778e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:13.490113020 CET	8.8.8.8	192.168.2.4	0x833b	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:15.180360079 CET	8.8.8.8	192.168.2.4	0x3a22	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 20:29:15.349201918 CET	8.8.8.8	192.168.2.4	0xd7c9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:15.812786102 CET	8.8.8.8	192.168.2.4	0x4bcf	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.087862968 CET	8.8.8.8	192.168.2.4	0xa142	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.274111032 CET	8.8.8.8	192.168.2.4	0x4c77	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.533947945 CET	8.8.8.8	192.168.2.4	0x81eb	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.602067947 CET	8.8.8.8	192.168.2.4	0xc787	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:16.773143053 CET	8.8.8.8	192.168.2.4	0x40fb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:17.236701965 CET	8.8.8.8	192.168.2.4	0xca44	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:17.402679920 CET	8.8.8.8	192.168.2.4	0x863	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:17.859249115 CET	8.8.8.8	192.168.2.4	0x9726	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:19.439167023 CET	8.8.8.8	192.168.2.4	0x96a6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:19.616394997 CET	8.8.8.8	192.168.2.4	0xe326	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:19.801878929 CET	8.8.8.8	192.168.2.4	0x1a4e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:20.159404039 CET	8.8.8.8	192.168.2.4	0x4a7f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.372855902 CET	8.8.8.8	192.168.2.4	0x10bc	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.540100098 CET	8.8.8.8	192.168.2.4	0xaddd	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.738399982 CET	8.8.8.8	192.168.2.4	0x5f8e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.921998978 CET	8.8.8.8	192.168.2.4	0x1acd	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.921998978 CET	8.8.8.8	192.168.2.4	0x1acd	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.921998978 CET	8.8.8.8	192.168.2.4	0x1acd	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.921998978 CET	8.8.8.8	192.168.2.4	0x1acd	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:23.921998978 CET	8.8.8.8	192.168.2.4	0x1acd	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:25.495446920 CET	8.8.8.8	192.168.2.4	0xf661	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:25.683790922 CET	8.8.8.8	192.168.2.4	0x14c4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:25.859040022 CET	8.8.8.8	192.168.2.4	0xe7cb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:35.107043982 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:29:35.107043982 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:35.107043982 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:35.107043982 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:35.107043982 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:35.107043982 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:37.789823055 CET	8.8.8.8	192.168.2.4	0x3059	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:47.210695982 CET	8.8.8.8	192.168.2.4	0x55ea	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:47.657924891 CET	8.8.8.8	192.168.2.4	0x7678	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:47.839870930 CET	8.8.8.8	192.168.2.4	0xcf52	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.020026922 CET	8.8.8.8	192.168.2.4	0xbff0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.191282988 CET	8.8.8.8	192.168.2.4	0xa2f1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.403235912 CET	8.8.8.8	192.168.2.4	0x8df1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.596955061 CET	8.8.8.8	192.168.2.4	0x4328	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.779263020 CET	8.8.8.8	192.168.2.4	0xfe2b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:48.975230932 CET	8.8.8.8	192.168.2.4	0xd0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.159852028 CET	8.8.8.8	192.168.2.4	0x4039	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.325958967 CET	8.8.8.8	192.168.2.4	0xa0aa	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.493980885 CET	8.8.8.8	192.168.2.4	0xc6d3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.676035881 CET	8.8.8.8	192.168.2.4	0x8431	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:49.849984884 CET	8.8.8.8	192.168.2.4	0x8d3d	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.075565100 CET	8.8.8.8	192.168.2.4	0xee16	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.237838984 CET	8.8.8.8	192.168.2.4	0xdf9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.404228926 CET	8.8.8.8	192.168.2.4	0xbc85	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:53.404228926 CET	8.8.8.8	192.168.2.4	0xbc85	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:29:53.844762087 CET	8.8.8.8	192.168.2.4	0xc6ed	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.020250082 CET	8.8.8.8	192.168.2.4	0xafa7	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.239521980 CET	8.8.8.8	192.168.2.4	0xce80	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.408709049 CET	8.8.8.8	192.168.2.4	0x66db	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.573277950 CET	8.8.8.8	192.168.2.4	0x75ac	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.733412027 CET	8.8.8.8	192.168.2.4	0x81b7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:29:54.896519899 CET	8.8.8.8	192.168.2.4	0x3011	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:02.233520031 CET	8.8.8.8	192.168.2.4	0x5c1a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:02.399200916 CET	8.8.8.8	192.168.2.4	0xee93	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.127019882 CET	8.8.8.8	192.168.2.4	0xa06f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.290981054 CET	8.8.8.8	192.168.2.4	0xce9b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.464379072 CET	8.8.8.8	192.168.2.4	0x87ab	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:04.640945911 CET	8.8.8.8	192.168.2.4	0x4535	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:12.016377926 CET	8.8.8.8	192.168.2.4	0xcf0a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:12.201699972 CET	8.8.8.8	192.168.2.4	0xbcea	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:12.395394087 CET	8.8.8.8	192.168.2.4	0x475c	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:17.920705080 CET	8.8.8.8	192.168.2.4	0xe8c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:18.199744940 CET	8.8.8.8	192.168.2.4	0x2817	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:18.287906885 CET	8.8.8.8	192.168.2.4	0xfb9d	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:18.434205055 CET	8.8.8.8	192.168.2.4	0xe2eb	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:20.746655941 CET	8.8.8.8	192.168.2.4	0xf1ed	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:20.923949003 CET	8.8.8.8	192.168.2.4	0x38f1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:23.129528046 CET	8.8.8.8	192.168.2.4	0xcf31	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:27.675003052 CET	8.8.8.8	192.168.2.4	0x803b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:27.865788937 CET	8.8.8.8	192.168.2.4	0x4d74	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.032931089 CET	8.8.8.8	192.168.2.4	0xdb9b	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 20:30:28.275589943 CET	8.8.8.8	192.168.2.4	0xfaf7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.478533983 CET	8.8.8.8	192.168.2.4	0x78e4	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:28.489126921 CET	8.8.8.8	192.168.2.4	0xcb6	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:31.883305073 CET	8.8.8.8	192.168.2.4	0xa7eb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:32.173628092 CET	8.8.8.8	192.168.2.4	0xe5f1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:32.412640095 CET	8.8.8.8	192.168.2.4	0xcd5e	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:34.867557049 CET	8.8.8.8	192.168.2.4	0xef5d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.089627981 CET	8.8.8.8	192.168.2.4	0xe884	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.296699047 CET	8.8.8.8	192.168.2.4	0xd4ee	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.804399967 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.804399967 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.804399967 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.804399967 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.804399967 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:35.804399967 CET	8.8.8.8	192.168.2.4	0x7bd0	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:42.953994989 CET	8.8.8.8	192.168.2.4	0x2726	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:42.953994989 CET	8.8.8.8	192.168.2.4	0x2726	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:42.953994989 CET	8.8.8.8	192.168.2.4	0x2726	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:42.953994989 CET	8.8.8.8	192.168.2.4	0x2726	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:42.953994989 CET	8.8.8.8	192.168.2.4	0x2726	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:44.238307953 CET	8.8.8.8	192.168.2.4	0x3fe1	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:44.521907091 CET	8.8.8.8	192.168.2.4	0xc3	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:44.521907091 CET	8.8.8.8	192.168.2.4	0xc3	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:44.521907091 CET	8.8.8.8	192.168.2.4	0xc3	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:30:44.521907091 CET	8.8.8.8	192.168.2.4	0xc3	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Jan 14, 2022 20:30:48.260907888 CET	8.8.8.8	192.168.2.4	0xee5a	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:31:08.620507956 CET	8.8.8.8	192.168.2.4	0x1b20	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pieilmtu.com
  - host-data-coin-11.com
- nwilglig.org
- nfbqltka.com
- cvdhldsf.net
- qcjatd.com
- xrovmrlel.net
- cmgcwqatb.org
- owgvnnuoml.com
- data-host-coin-8.com
- opviax.net
- nunmqyect.net
- kyadmhioim.com
- rnsdjgkq.org
- sjgvu.com
- unicupload.top
- cqsurm.com
- gculkm.com
- ifvodd.net
- lvmiyiiy.com
- pegqugok.net
- uhiqru.org
- jbinuykf.net
- kybdaip.org
- 185.7.214.171:8080

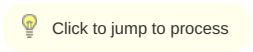
- doynnfulb.net
- nxysak.org
- jxgxnkpb.org
- mfkcxcj.org
- codldamrms.net
- niaqngu.org
- hmpbvq.org
- ktpvhvj.com
- ovfkbfuk.org
- cgqgnij.net
- pdjtd.com
- jcppp.com
- fnkfxr.net
- crnelkeerw.net
- lyxrabhsyj.net
- dvrkmsgph.org
- bdwjscwkyb.org
- laegissbnw.net
- pmulpwtk.net
- vgfuhgdk.com
- gjmsrnrg.net
- hffekwpew.org
- nrofkgudk.org
- ldeax.net
- mvdnpk.org
- uaeudvuct.net
- tfmwuwhaf.org
- 81.163.30.181
- bjmmoxjkh.com
- uekxwe.org

- 74.201.28.62
- ybthjouy.net
- qycehx.net
- udwhex.net
- 185.163.204.22
- 185.163.204.24
- hriqvkh.com
- rajclxd.org
- rkgofw.com
- cmhrt.com
- rdctx.net
- hqdkqcs.com
- cfyeur.com
- lwqbhm.net
- podwtxiqj.com
- kxheih.com
- ahptoxawd.com
- ruiwhjpxrd.net
- ukonhqmwew.net
- qmeixpxj.org

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ECD2MpEBSf.exe PID: 7104 Parent PID: 6048

General

Start time:	20:28:28
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\ECD2MpEBSf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ECD2MpEBSf.exe"
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	31F0D01EE1FD6876668692791657D97E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ECD2MpEBSf.exe PID: 7132 Parent PID: 7104

General

Start time:	20:28:29
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\ECD2MpEBSf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ECD2MpEBSf.exe"
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	31F0D01EE1FD6876668692791657D97E
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: 00000001.00000002.721727855.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.721690876.0000000000680000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 7132

General

Start time:	20:28:36
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 00000005.00000000.708255964.00000000044C1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6408 Parent PID: 568

General

Start time:	20:28:37
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:	0x7ff6eb840000
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: 3512 Parent PID: 568

General

Start time:	20:28:55
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:	0x7ff6eb840000
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: jgdhbua PID: 6700 Parent PID: 968

General

Start time:	20:29:10
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\jgdhbua
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jgdhbua
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	31F0D01EE1FD6876668692791657D97E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: svchost.exe PID: 6680 Parent PID: 568

General

Start time:	20:29:10
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:	0x7ff6eb840000
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: jgdhbua PID: 6784 Parent PID: 6700

General

Start time:	20:29:11
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\jgdhbua
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jgdhbua
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	31F0D01EE1FD6876668692791657D97E
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: 0000000B.00000002.776599972.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.776791205.00000000020A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: BB8A.exe PID: 6816 Parent PID: 3424

General

Start time:	20:29:12
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\BB8A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BB8A.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
Reputation:	moderate

Analysis Process: svchost.exe PID: 6964 Parent PID: 568

General

Start time:	20:29:15
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
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: WerFault.exe PID: 6876 Parent PID: 6964

General

Start time:	20:29:16
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6816 -ip 6816
Imagebase:	0x1010000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: CCB2.exe PID: 6844 Parent PID: 3424

General

Start time:	20:29:17
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\CCB2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CCB2.exe
Imagebase:	0x400000
File size:	324608 bytes

MD5 hash:	043B44289E31BD54357F9A5C21833259
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: 0000000F.00000002.775841578.00000000007F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000002.775841578.00000000007F9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: 6968 Parent PID: 6816

General

Start time:	20:29:17
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6816 -s 520
Imagebase:	0x1010000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: D936.exe PID: 7124 Parent PID: 3424

General

Start time:	20:29:21
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\D936.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D936.exe
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	9517CA2BC20EC061024C1209970CCD2E
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: 00000011.00000002.796450954.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000002.797091655.00000000022B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000003.779473426.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: 3D34.exe PID: 6404 Parent PID: 3424

General

Start time:	20:29:23
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3D34.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3D34.exe
Imagebase:	0xec0000
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: 00000012.00000002.833275323.00000000041F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000002.833464312.0000000004361000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 89%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 6412 Parent PID: 7124

General

Start time:	20:29:25
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\qeprvgom\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 4652 Parent PID: 6412

General

Start time:	20:29:25
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5468 Parent PID: 7124

General

Start time:	20:29:26
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\krmdinzg.exe" C:\Windows\SysWOW64\qeprvgom\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 4672 Parent PID: 5468

General

Start time:	20:29:26
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6064 Parent PID: 568

General

Start time:	20:29:27
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:	0x7ff6eb840000
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: sc.exe PID: 4608 Parent PID: 7124

General

Start time:	20:29:27
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create qeprvgom binPath= "C:\Windows\SysWOW64\qeprvgom\krmdinzg.exe /d\"C:\Users\user\AppData\Local\Temp\D936.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xb40000
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: 6424 Parent PID: 4608

General

Start time:	20:29:27
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6464 Parent PID: 7124

General

Start time:	20:29:28
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description qeprvgom "wifi internet conection
Imagebase:	0xb40000
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: 6604 Parent PID: 6464

General

Start time:	20:29:29
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 1716 Parent PID: 7124

General

Start time:	20:29:29
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start qeprvgom
Imagebase:	0xb40000
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: 64 Parent PID: 1716

General

Start time:	20:29:30
Start date:	14/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: krmdinzg.exe PID: 6888 Parent PID: 568

General

Start time:	20:29:30
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\qeprvgom\krmdinzg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\qeprvgom\krmdinzg.exe /d"C:\Users\user\AppData\Local\Temp\D936.exe"
Imagebase:	0x400000
File size:	10624000 bytes
MD5 hash:	C8DE2E3F0DF5D9E1C126828B1444DBEA
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: 00000020.00000002.800983655.00000000006C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000003.798724710.00000000007C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000002.800731759.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000002.801019606.00000000007C0000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: netsh.exe PID: 6744 Parent PID: 7124

General

Start time:	20:29:30
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:	0x7ff77ba70000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3716 Parent PID: 6744

General

Start time:	20:29:31

Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 3000 Parent PID: 6888

General

Start time:	20:29:32
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0x12f0000
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: 00000023.00000002.1024071704.0000000000E70000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 3D34.exe PID: 2832 Parent PID: 6404

General

Start time:	20:29:35
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3D34.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\3D34.exe
Imagebase:	0x150000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis