ID: 553412
Sample Name: OG9rNsihJ7.exe
Cookbook: default.jbs
Time: 21:03:19
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

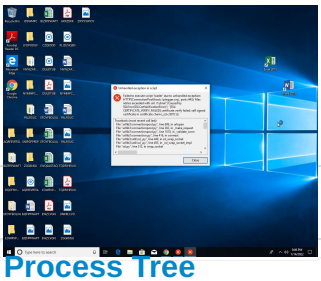
Windows Analysis Report OG9rNsihJ7.exe

Overview

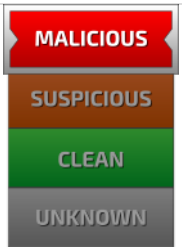
General Information

Sample Name:	OG9rNsihJ7.exe
Analysis ID:	553412
MD5:	5c7b4677105504..
SHA1:	5362af084622dc8.
SHA256:	0245c82558329c..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



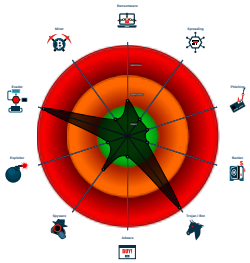
RedLine SmokeLoader Tofsee Vidar

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- OG9rNsihJ7.exe (PID: 4948 cmdline: "C:\Users\user\Desktop\OG9rNsihJ7.exe" MD5: 5C7B46771055043F59E0451A342B7ED1)
  - OG9rNsihJ7.exe (PID: 5424 cmdline: "C:\Users\user\Desktop\OG9rNsihJ7.exe" MD5: 5C7B46771055043F59E0451A342B7ED1)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - B1B2.exe (PID: 6924 cmdline: C:\Users\user\AppData\Local\Temp\B1B2.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 7156 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6924 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - BFBD.exe (PID: 6984 cmdline: C:\Users\user\AppData\Local\Temp\BFBD.exe MD5: 5C7B46771055043F59E0451A342B7ED1)
        - BFBD.exe (PID: 7140 cmdline: C:\Users\user\AppData\Local\Temp\BFBD.exe MD5: 5C7B46771055043F59E0451A342B7ED1)
        - svchost.exe (PID: 7140 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
      - 254E.exe (PID: 1268 cmdline: C:\Users\user\AppData\Local\Temp\254E.exe MD5: 41AB3EFA04441E560A279BD0F7C0503D)
      - 3136.exe (PID: 5060 cmdline: C:\Users\user\AppData\Local\Temp\3136.exe MD5: 023802260A0216012A5F00079406D967)
        - cmd.exe (PID: 5992 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\ffiawxs\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 1928 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\xqfkdfcl.exe" C:\Windows\SysWOW64\ffiawxs\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 3532 cmdline: C:\Windows\System32\sc.exe" create ffiawxs binPath= "C:\Windows\SysWOW64\ffiawxs\xqfkdfcl.exe /d\"C:\Users\user\AppData\Local\Temp\3136.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5500 cmdline: C:\Windows\System32\sc.exe" description ffiawxs "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 7068 cmdline: "C:\Windows\System32\sc.exe" start ffiawxs MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 3720 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: 4560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 3BC6.exe (PID: 6244 cmdline: C:\Users\user\AppData\Local\Temp\3BC6.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 3BC6.exe (PID: 7064 cmdline: C:\Users\user\AppData\Local\Temp\3BC6.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 3756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4840 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6092 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2600 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4568 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 2076 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1188 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6656 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- vfgiwcs (PID: 6824 cmdline: C:\Users\user\AppData\Roaming\vfgiwcs MD5: 5C7B46771055043F59E0451A342B7ED1)
  - vfgiwcs (PID: 6840 cmdline: C:\Users\user\AppData\Roaming\vfgiwcs MD5: 5C7B46771055043F59E0451A342B7ED1)
- svchost.exe (PID: 6976 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 7020 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6924 -ip 6924 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 7148 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- xqfkdfcl.exe (PID: 5432 cmdline: C:\Windows\SysWOW64\ffiawxs\xqfkdfcl.exe /d"C:\Users\user\AppData\Local\Temp\3136.exe" MD5: 5C50CF4AF77D12BF94B3FC09437C8B16)
  - svchost.exe (PID: 3440 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\8017.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
0000002D.00000000.408848131.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
0000001D.00000002.380383276.000000000400000.00000040.00020000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000018.00000002.366966979.00000000004B0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000001C.00000002.357825450.000000000083A000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000001C.00000002.357825450.000000000083A000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.1.vfgiwcs.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
30.2.3BC6.exe.3aaf910.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.1.OG9rNsihJ7.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
42.2.xqfkdfcl.exe.840000.2.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
19.2.vfgiwcs.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 24 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

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

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

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

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

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

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

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

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

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

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

Yara detected Tofsee

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

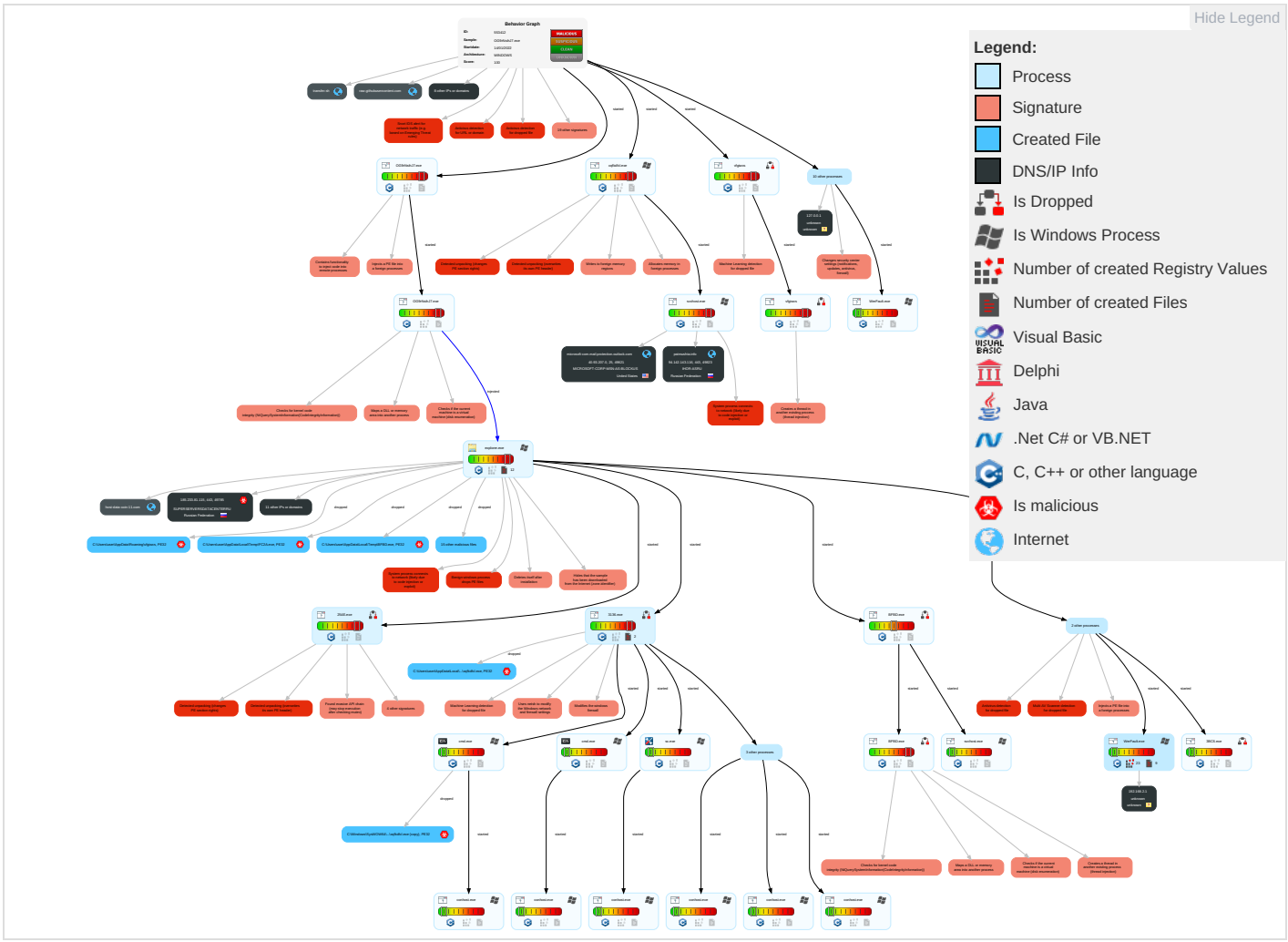
Yara detected Tofsee

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Protc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 4 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

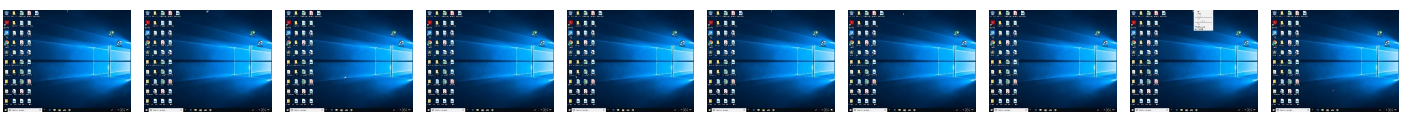
Behavior Graph

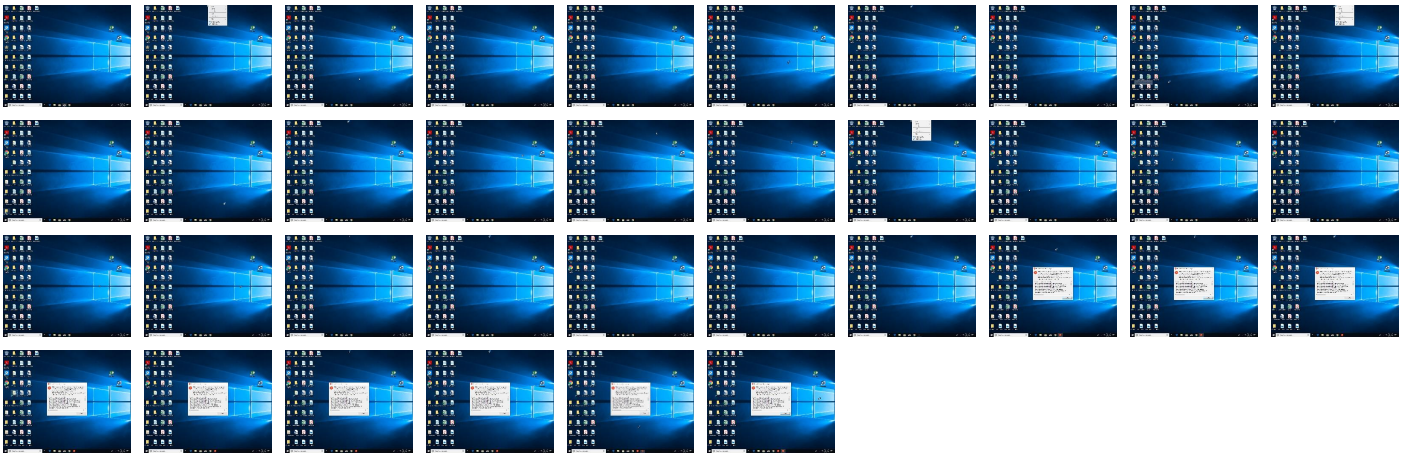


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OG9rNsihJ7.exe	49%	ReversingLabs	Win32.Trojan.Chapak	
OG9rNsihJ7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\3BC6.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\xqfkdfcl.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\2473.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\6AF7.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\3BC6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FC2A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\vfgiwcs	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9789.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\254E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\45AA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B1B2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8017.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2F32.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\54AF.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\xqfkdfcl.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BFBD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3136.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\88E2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7808.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3A7E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3BC6.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3BC6.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\45AA.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\45AA.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\54AF.exe	50%	ReversingLabs	Win32.Infostealer.Generic	
C:\Users\user\AppData\Local\Temp\8017.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
30.0.3BC6.exe.650000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
30.0.3BC6.exe.650000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.0.B1B2.exe.2080e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.0.3BC6.exe.3c0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.1.OG9rNsihJ7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.1.vfgiwcs.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.0.3BC6.exe.3c0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
28.2.254E.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.OG9rNsihJ7.exe.5f15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.3.254E.exe.7f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.2.vfgiwcs.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.xqfkdfcl.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
29.2.3136.exe.6c0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
30.2.3BC6.exe.650000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.vfgiwcs.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.3.3136.exe.7f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.0.B1B2.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.BFBD.exe.6c15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.0.3BC6.exe.3c0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.2.OG9rNsihJ7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.0.3BC6.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.0.B1B2.exe.2080e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.0.3BC6.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
1.0.OG9rNsihJ7.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.0.BFBD.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.OG9rNsihJ7.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.0.3BC6.exe.650000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.vfgiwcs.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.OG9rNsihJ7.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.0.3BC6.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
24.1.BFBD.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.B1B2.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
24.2.BFBD.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.0.BFBD.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.3.xqfkdfcl.exe.7f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.0.vfgiwcs.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
44.2.svchost.exe.7b0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
45.2.3BC6.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
45.0.3BC6.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
20.2.B1B2.exe.2080e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.254E.exe.6c0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
45.0.3BC6.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
29.2.3136.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
42.2.xqfkdfcl.exe.840000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
45.0.3BC6.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
18.2.vfgiwcs.6415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.0.BFBD.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.B1B2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.xqfkdfcl.exe.680e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.3.B1B2.exe.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.0.3BC6.exe.650000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://81.163.30.181/l2.exe	100%	Avira URL Cloud	malware	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
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://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://74.201.28.62/book/KB5009812.png	0%	Avira URL Cloud	safe	
http://schemas.microsoft.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://74.201.28.62/book/KB5009812.exe	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://81.163.30.181/l3.exe	100%	Avira URL Cloud	malware	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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
cdn.discordapp.com	162.159.133.233	true	false		high
ipwhois.app	136.243.172.101	true	false		high
unicupload.top	54.38.220.85	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-data-coin-11.com	8.209.70.0	true	false		high
c9d0e790b353537889bd47a364f5acff43c11f248.xyz	185.112.83.97	true	false		high
privacy-tools-for-you-780.com	8.209.70.0	true	false		high
microsoft-com.mail.protection.outlook.com	40.93.207.0	true	false		high
goo.su	172.67.139.105	true	false		high
transfer.sh	144.76.136.153	true	false		high
api.telegram.org	149.154.167.220	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high
api.ip.sb	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://81.163.30.181/l2.exe	true	• Avira URL Cloud: malware	unknown
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://74.201.28.62/book/KB5009812.png	true	• Avira URL Cloud: safe	unknown
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	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/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://81.163.30.181/l3.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.93.207.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	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
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
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
81.163.30.181	unknown	Russian Federation		58303	IR-RASANAPISHTAZIR	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553412
Start date:	14.01.2022
Start time:	21:03:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OG9rNsihJ7.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@60/37@100/15
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.5% (good quality ratio 16.1%) • Quality average: 52.1% • Quality standard deviation: 40.6%
HCA Information:	• Successful, ratio: 58% • 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
21:04:25	API Interceptor	10x Sleep call for process: svchost.exe modified
21:04:56	Task Scheduler	Run new task: Firefox Default Browser Agent B300E2CA9C9656AE path: C:\Users\user\AppData\Roaming\vfg iwcs
21:05:11	API Interceptor	1x Sleep call for process: 254E.exe modified
21:05:29	API Interceptor	1x Sleep call for process: WerFault.exe modified
21:05:55	API Interceptor	1x Sleep call for process: explorer.exe modified
21:06:32	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run RegHost C:\Users\user\AppData\Roaming\Microsoft\RegHost.exe
21:06:34	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
21:06:52	Task Scheduler	Run new task: services path: C:\Users\user\AppData\Roaming\Microsoft\services.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24860094463598098
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4P:BJiRdwfu2SRU4P
MD5:	C9689D25BCB7A6122C80D8D1248CD525
SHA1:	3626F8C656E1F3524CD70D2C237FBDC25AF8C26B
SHA-256:	A1B6750BEA5C766B4AC8A6D65695475180388153C3504BBBA66053A8BB3F9014
SHA-512:	1B132DCA5A85A0B510A84117A7F8CEEB2AD4591C24EFA651D6E39B2D94140F4D37E30DFBDC4A860D661E54188703ABD742AA3153ED9B6EEECEB0E16FA093D4F
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x962e81fb, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506309986392212
Encrypted:	false
SSDEEP:	384:M+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:TSB2nSB2RSjlK/+mLesOj1J2
MD5:	AEF5940564973C51F03B64B3BF5DAF42
SHA1:	B5A630CEDB208FCF5DE3E8C4EE6C1ECE9AC50644
SHA-256:	03AD212E8D9030DB0C6C1AE6B3C3560681FB1C5DC012CC75FECC751E81C39F6A
SHA-512:	B91EB9A7ACB63185D5304A2AEF6CEB973AD4F7C031BDB6BB51CECAF7A44AE1B44CC83DD2A9EA92051188AE0FA67FEF65D3B5C15F162EAFB5C400D0E6720FF44F
Malicious:	false
Reputation:	unknown
Preview:	....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... ....3...w..... .....k..t....z.....iQ.....z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07533799262335537
Encrypted:	false

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
SSDEEP:	3:rftl7Ev/2ff4lkl/bJdAtiX0/gqkf4l1all3VkttlmlnI:DXinkt4ztQ3
MD5:	2107023193542ECC0970CB79A0C9E236
SHA1:	F5D4FD1244E423620174644F19B9F4C484DCA0A5
SHA-256:	9B5F9895367FCB9497C1DA993C21C355AA6937BF3FD1FD719E08EAAF905BCDD4
SHA-512:	1DA7C4DB4F8D644D2EADBE475EC111B408697B2E974C5943C9A1AD4230C0C57451AC5B0CCEC2F97C1E4C93D15CC2C2D291ECA6BDC40AD7574CBFC75959A3929
Malicious:	false
Reputation:	unknown
Preview:	.1'.....3...w.....z.....w.....w.....w....:O....w.....iQ.....z.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_B1B2.exe_97263ecc359653bdc088fc4542e7f7e1a086af1b_57588827_1b13b61d\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):	0.8138460270665933
Encrypted:	false
SSDEEP:	96:zvFmoP1pgLnCDyaC9OQoJ7R3V6tpXIQcQec6tycEfcw3qhz+HbHg/8BRTf3o8Fa7:zvP1pKC+q8HQ0lLjIq/u7sZS274Itvu
MD5:	A718EF39D4118C87DFC94920D817BDB7
SHA1:	1C873AFB51135338D4F94B5A7F259BC0D7874793
SHA-256:	D295541AB8373183E475D1A7780D51C4C8AFEA49D4ECEA63F440B98656873954
SHA-512:	3AD8085642AB1655D958F37C3E0E0DCA86911047587D74A31B8A5E152AA3854BD8E41CC9074F4481444F0B170DD69CF1B184E7D0F26D414EA87F3CF9EC50AE8
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.=.1.3.2.8.6.6.9.6.7.1.1.6.5.9.9.5.2.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.9.6.7.2.8.0.1.9.3.7.0.3.....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.=.1.2.5.7.b.a.b.9.-.4.c.8.a.-.4.4.1.d.-.8.5.3.c.-.8.7.b.3.5.1.1.7.8.c.0.1.....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.=.3.8.c.c.4.2.1.3.-.8.3.c.d.-.4.4.a.a.-.b.4.9.1.-.5.a.a.9.6.6.d.8.2.f.4.0.....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.1.B.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.0.c.-.0.0.0.1.-.0.0.1.6.-.6.6.7.3.-.e.6.7.2.c.d.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.4.3.2.a.e.1.c.8.6.8.c.9.6.1.2.8.e.c.a.0.4.a.e.4.c.5.4.4.7.e.6.0.0.0.0.2.9.0.1.!.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.1.B.2...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\WER1914.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49372
Entropy (8bit):	3.067630685633625
Encrypted:	false
SSDEEP:	1536:SrHbYM8XsdtCvsOVnMZFRInPK/AyqP0b5Nt6:SrHbYM8XsdtCvsOVnMZFRIPK/AyqP0bg
MD5:	338F750C272EF10F787C1E43F7469E7C
SHA1:	6BAD6258FA53FAC05D2F096E899F246786E4A3F0
SHA-256:	4A99A6B112F2BC0F1B2EE04E5A0E555EBCC6685B1F3735577DBD42D6FBE86085
SHA-512:	E7D72CBE85F51D6D393F3EDCFD3518CCD7C5254A6DA052111D957B0644BBB75AB5FF978E9A7B9300D71FEDE41D288BB64931E8F906F5836464558E697812459
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E5.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6954899185007766
Encrypted:	false
SSDEEP:	96:9GiZYW+L4ZOtYzYIfRWLEH9UYEZJsJtMifFSySwmM7azdv30JiIU83:9jZD+fUlKscaazd/0JFU83
MD5:	7C2AA9B20C71B8DD577514C4DDBBD712
SHA1:	463B97C6A6F96546361BF21B6317E9293607FA2F

C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E5.tmp.txt	
SHA-256:	8C1BF6329AB684529639CC05DBF3B1780CF840DC68291086737CB14EAD142A10
SHA-512:	1093A857D78BD1CEC600A6B6DBD50166CB7CEC200129E3A88F877AE91B1A92F148B5946E8FEE0FC3E9DC6D388CE9F5639DDCD4B58EEF98AFB9F61DCE93C37903
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\WER472.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.700501604073412
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLe696YIhSUFEgmfIRSHCpDg89bo2HlsfIYm:RrlsNiS696YeSUGgmfIRSao/f+
MD5:	4B651050CA6DE05729DB037C8478C51F
SHA1:	0BF9C319562E7CC3201B2DED04AAD2231E896310
SHA-256:	AD3B556FE1FE1665E2FE34EC93BA192963A2E9CDA8BC79E0CA94B61A97D2B727
SHA-512:	28A03C0F8399AA0F8A121B51EAAA0E5CCC6530AA3015959673B489CD3847CC89105A6E82D766C1C6F6379B60D71A4EBB5C8700D651B0BC162181E9447FEF147
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB49.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):	4.473771438286213
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI9IOWSC8BJG8fm8M4JHl8qFBD4+q8vX8p5PnzmdU1d:uITfljvSNzDJH7EKu5PnCdU1d
MD5:	CF08C1DE42859C20B2D34A25654CB927
SHA1:	08723BDD9572112FF16270CC766085C89148915D
SHA-256:	C480A9FF150CBDE8804F51B4264A3213697E2614F04CE506BB11A2C34BE377FB
SHA-512:	5043BB5B3A08FFC31FFCACCF95D3641A88708C05C2AD3E5FC37B08E92CDBA171BA9EFBA39D8D78C3405FA8C15EC4B8471611663D5A27FE445418A923DC48A627
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="1342935" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA77.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51858
Entropy (8bit):	3.0616433192144115
Encrypted:	false
SSDEEP:	1536:jLHv5WmtKiTdiIMZN+fNz0Ehs9WKTebyqbp:jLHv5WmtKiTdiIMZN+fx0Ehs9WKTebyG
MD5:	74A2DA0D08295658AA1F0293F6EADF2E
SHA1:	0C6C053599986E8D921BEEA9FE16EF324FB39CC4
SHA-256:	00D32A923A24EDE8F79E33C2E661F32AD3D903EDBE6C4B2D24A9344840782DE7
SHA-512:	24C2574F4AC293E82DCFA458C2C671BCE4D3CC2FC8AF56554C8A772CA83F89F9C4A16083CAA2A40D6A6C3AEAAAA90B8209158D9FC50F4ED93864869042B40DF

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA77.tmp.csv	
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBEED.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695534489993445
Encrypted:	false
SSDEEP:	96:9GiZYWztLC0YZYHWlKbfHCUYEZlot0iXFjKVw5/4ZidaWXHBJrXIsJ3:9jZDVO7Y2JdaWXHBJr4sJ3
MD5:	25F7F1558464C00B4E4D702D387DA442
SHA1:	3240050B847D2BFCB21F9C7F866FA8488C98C37C
SHA-256:	AAA81A7419C4ED2C6E75EC2BE1C2DEBF54550E1F8B97352416130C7ED4290C9D
SHA-512:	F7F6CF719652058B24450EF387F149614AD950FDA2ADFD3418BDA3951B33A639461864E7E81292B87F327789101C2C25203D0D0C1F7A5499CE4303217AA2FA6C
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\WERFA10.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jan 15 05:05:13 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	42152
Entropy (8bit):	1.9990135190542404
Encrypted:	false
SSDEEP:	192:TcGeH/iNOeh0wVM6/7wJ8EpwLkSjtUHpKxTHtE1W:WHeLsxyLFEsdu1W
MD5:	51E48C78778D421A4C28C21DF4E8DEEF
SHA1:	E1B678DFFCAEB6074ED6C741457D3B6FFD198BB8
SHA-256:	F8B2510CC073E240F4FA3588B5D06DECB7C7FFEEDD9B09E3715D06A82EC5E098
SHA-512:	1BB92EF8DDF4137C261C73562E177FF1F5FBA83AE7720846C000777C36FE9C88C1082897051CB95E8BDF88A340CBA92BCE925164705BA687BC87CC204F98EF9
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....V.a.....4...v(.....T.....8.....T.....x.....d.....U.....B.....GenuineIntelW.....T.....U.a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3BC6.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\3BC6.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3BC6.exe.log	
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\2473.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\254E.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	324096
Entropy (8bit):	6.7085322399040335
Encrypted:	false
SSDEEP:	6144:7YHQmo4o6MLYuiQagdEmekrti+RUgf8pbdv:7oQLRPEQLFnrlRt8pJ
MD5:	41AB3EFA04441E560A279BD0F7C0503D
SHA1:	36498DB70D79BC77FD1D8C9543457BA467486D77
SHA-256:	5CE3B77E18533D7FC98C430034D5F384D81289FD28E3E9FF7DB248EB508F8002
SHA-512:	735CA627FFD1E4581854B3F8D1777AAD86A1BFBEE975C46F021EE1E2C19547EF84F498ADD85705B9B8BB24BCBE143AEDDEF31CBAB9D343D264AD2FF4C1888 2B
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.....@....wuxut.....@....tijayu.....@....zemoyi.....@....rsrc...(.....".....@..@.reloc..dF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\2F32.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
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\2F32.exe

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\3136.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	321536
Entropy (8bit):	6.690971316601855
Encrypted:	false
SSDEEP:	6144:7vrN0pZXR3Srrj51BawxgIKP184NSWd2hQAjh3C:zrN0vR36TBHLY1JSWMQAt
MD5:	023802260A0216012A5F00079406D967
SHA1:	AC1B2B166216DE3D15552BCD23BEC03536AFE1A7
SHA-256:	0B2E2469C995A8D8DAF14CD69EF8717590B538C8A5B432F8704079DB5CF03D04
SHA-512:	589294C84150CFAC2830D58BC7BCA665FF86574417792BF7C02905924058F745F4D55CB12F01FB5C894A1964D2EF1009031FA598D6288CE581F22B7D19B01283
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L.....}`.....@.....4...P.....(..... ...@..... ....L.....text..... ..`.data.....@....yocinoj.....@....lebe.....@....wuno.....@....rsrc... (.....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\3A7E.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\3BC6.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\3BC6.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\45AA.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\54AF.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:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3ED CD
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\6AF7.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:I++hvICteEroXxqENE+sKsXXgvkwuUxNhMC/CKN7kL:BInEroXjsKkXgs/EhWKNY
MD5:	AE6510D9815C44A818F722ECAE6844B8
SHA1:	2A34B5110F5C3C2424AE9685F57261E2546BD963
SHA-256:	C3CAD582268B165711E2F2B1834891C7BCB5E57A7EFB1E709E3DF19D011AD656
SHA-512:	8CAA9E661403D5D86F69E7C35E45CDF927EF9EC0C6045ED2CA5AF2EAAF26B4F99291EADAF2F0C8C00A31B05B228C6DF0C4BD205A7B3EC70E263313A08FFEF 4F8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%

C:\Users\user\AppData\Local\Temp\6AF7.exe

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\7808.exe

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

C:\Users\user\AppData\Local\Temp\8017.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\8017.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\88E2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1474560
Entropy (8bit):	6.247221725855881
Encrypted:	false
SSDEEP:	24576:EhiK5YeyX+krf/WDW7lhw/Re3/gXfoGmxXS+TaeSmOsS6SVHdYPQLnfnqG6JJzTm:v4jyX+krf/WDW7lhw/Re3/gXfoGmxXSt
MD5:	8C7457EEF295583195EF22683C133923
SHA1:	DD03B6C66BDAFDFC9DDFA468072D0D2C7AE97733
SHA-256:	E45E273ADB510E4D06F8D10B121740CDFABD862EA7D5617BCCE4BC9D81485939
SHA-512:	6437E6C0F4E36110B2614CFAE192AF5F18654D83478DBC4807DF42112A5E407150E9EEDF652E29E20EABFCD169657C40B64E660E344C392CB61D8C492FD07DC
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\88E2.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[(h.....0..v..... .....@.. ..... .@.....W..... ....H.....text....u... ...v..... ..`.rsrc.....x.....@..@.reloc..... .....~.....@..B.....H.....4...P.....+N...`..tg.....g.....y....(.O..*.s+I...b...**....(i...*f....(j...r...p(....(k...*f....ol...(m...ol...on...*.s.N... ....*f....ol...r.'.p(....on...*f....o....rc'.p(....on...*f....o....r.'.p(....(k...*.....o....r/(.p(....r/!.p(....rq!.p(....(....on...*f....o....r.(.p(....(k...*f....o....r.(.p(....(k...*f....o....r.).p(....(k...*f....o....r.).p(.... (k...*.~....:#...r;*.p(.....#...(....o....s.....~....*.~....*.~

C:\Users\user\AppData\Local\Temp\9789.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3602944
Entropy (8bit):	**7.997581797791447**
Encrypted:	**true**
SSDEEP:	98304:dUo6hIZwh7VTBNLQP/zCAtY5oujwp+sTEo2fSTUD1R:dUPhIZwhBzQD1GoufsbTUDT
MD5:	E13718B977E0A61DEFA3A5313E1FBED6
SHA1:	F70F1A541102F74517050D9731898592386196F4
SHA-256:	2B13A7CCA8C39A41F4E760F432948D1E16DC75444B28FFAD71042F5817926AAE
SHA-512:	2034240C486D46A8EC52C85892ACEEA2B9ABF6E5199AFD33FDB4AE6FE12FFA480006B0F93B5BF6CFB6AD9C1B5A58DFFDD26D05E4BAA7095948D7686ABFC040FC
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.....O7. .....|.O. ....pM..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....P.....@.....1...../.....@....rsrc.....pM.....0.....@....wZtCyLX.....O.....J2.....@....adata.....S.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\B1B2.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8lA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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\BFBD.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	321024
Entropy (8bit):	6.6910111765717115
Encrypted:	false
SSDEEP:	6144:1dNi2kGfRHG5p1JX9BnaPGMq3yvNITJwD3EsG1ALc:XNsGfIfnpBCvuJw4sG+
MD5:	5C7B46771055043F59E0451A342B7ED1
SHA1:	5362AF084622DC8EFC661C703D4C7C5DD6839BE1
SHA-256:	0245C82558329CFD8EF5EF901E4929075D4D873BA20D9704731758580CAED7BE
SHA-512:	F16FDD7212BC64F05EF67B41E29DD8966645B7FA0E7D78E8883503503A3589A090C54846500925F17B8DD1D133E1F5BB37BBDE16F3E5C50864847C17F7DF2C06
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Temp\BFBD.exe	
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....h_.....@.....1.....P.....(.....@..... ....L.....text..... ..`.data.....@....zafif.....@....naladin.....@....ger.....@....rsrc... (.....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\FC2A.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%
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\xqfkdfcl.exe	
Process:	C:\Users\user\AppData\Local\Temp\3136.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13666304
Entropy (8bit):	3.7861536709741657
Encrypted:	false
SSDEEP:	6144:4vrN0pZXR3Srrj51BawxgIKP184NSWd2hQAjh3C:KrN0vR36TBHLY1JSWMQAt
MD5:	5C50CF4AF77D12BF94B3FC09437C8B16
SHA1:	C3D531F3C72F96EFCB00F932E744859755E88E54
SHA-256:	43EF54A754F54F17F38D5D6AC207B1EF17953FD742A18124CCD2423E7E01B6F8
SHA-512:	592FA7679DE8F8673287088C175EA7EB4D035B589F71C060F0151BF37FA4B55C13A96B8B214F26538768C1F64B891A9E5B7DFBF7481274F327C8CBC31518B296
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L.....}`.....@.....4...P.....(..... ...@..... ....L.....text..... ..`.data.....@....yocinoj.....@....lebe.....@....wuno.....@....rsrc... (.....@..@.reloc..ZF.....@..B..... .....

C:\Users\user\AppData\Roaming\vfgiwcs	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	321024
Entropy (8bit):	6.6910111765717115
Encrypted:	false
SSDEEP:	6144:1dNi2kGfRHG5p1JX9BnaPGMq3yvNITJwD3EsG1ALc:XNsGfIfnpBCvuJw4sG+
MD5:	5C7B46771055043F59E0451A342B7ED1
SHA1:	5362AF084622DC8EFC661C703D4C7C5DD6839BE1
SHA-256:	0245C82558329CFD8EF5EF901E4929075D4D873BA20D9704731758580CAED7BE
SHA-512:	F16FDD7212BC64F05EF67B41E29DD8966645B7FA0E7D78E8883503503A3589A090C54846500925F17B8DD1D133E1F5BB37BBDE16F3E5C50864847C17F7DF2C06
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Roaming\vfgiwcs	
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.....h_.....@.....1.....P.....(.....@.....L.....text..... ..`.data.....@....zafif.....@....naladin.....@....ger.....@....rsrc...(.....@..@.reloc..ZF.....H.....@..B.....

C:\Users\user\AppData\Roaming\vfgiwcs: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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220115_050436_607.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.375971674018937
Encrypted:	false
SSDEEP:	96:VC5Hf/o+Wco5dyE9P/YsZACXxFI2lQGgkhnp4vezT2AjFzONMCidJRRj5N:M98Hpg2wuPCCP
MD5:	8306EA709D3745A390765D410EC31DAE
SHA1:	936DBE90F785ED33F45FC201D7BC814E11F5308F
SHA-256:	1A86E818169EEE39C19C4CF088EE777782FC15A652CF287228B748F4284CA90A
SHA-512:	59D2CBB5C9474B7E46D1A590DD67BFAB68A7CBBDA7B966EAF00A10A121E50F97C655088108B74EB357685E99E347243B4A8905A224423279B5E9710F8C145CC
Malicious:	false
Reputation:	unknown
Preview:	....!.....(.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1...../_8..... .....0.~d.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.:.\.W.i.n. d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o.s.v.c... 2.0.2.2.0.1.1.5._.0.5.0.4.3.6._.6.0.7...e.t.l.....P.P.....(.....

C:\Windows\SysWOW64\ffiawxs\xqfkdfcl.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13666304

C:\Windows\SysWOW64\ffiawxs\xqfkdfcl.exe (copy)	
Entropy (8bit):	3.7861536709741657
Encrypted:	false
SSDEEP:	6144:4vrN0pZXR3Srrj51BawxgIKP184NSWd2hQAjh3C:KrN0vR36TBHLY1JSWMQAt
MD5:	5C50CF4AF77D12BF94B3FC09437C8B16
SHA1:	C3D531F3C72F96EFCB00F932E744859755E88E54
SHA-256:	43EF54A754F54F17F38D5D6AC207B1EF17953FD742A18124CCD2423E7E01B6F8
SHA-512:	592FA7679DE8F8673287088C175EA7EB4D035B589F71C060F0151BF37FA4B55C13A96B8B214F26538768C1F64B891A9E5B7DFBF7481274F327C8CBC31518B296
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.....}`.....@.....4...P.....(..... ...@..... ....L.....text..... ..`.data.....@....yocinoj.....@....lebe.....@....wuno.....@....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):	4.262263551383356
Encrypted:	false
SSDEEP:	12288:73ZKSZjdY1Nuot+yrYLwOFZcgSiIb7uMCTi3xzM2gdGX+oNU6iD+EVEV:7ZKSZjdY1Nuot+ybcY9V
MD5:	BFF50EE8D271FF908B21241B2424A1E1
SHA1:	67996C2F184A7B329E2C68781E7E354EB781D2FA
SHA-256:	2881D8D250821B2B44ECA36D4FCAF909B998042A74FDBA62CEC164AFDCA8AE1E
SHA-512:	72EA7560877C003AA5AF36379C5453EB6A18C6F30C67039B98EF38E2D98E980DC0E1A0F32D6035E31E454E707CC194DB77052E1CF5F55C319295381DB7B600BE
Malicious:	false
Reputation:	unknown
Preview:	regfQ...Q...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmr.*x..... ....!%..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.7779067348278756
Encrypted:	false
SSDEEP:	384:AkQAO25/ZrdtdXp55Qp8cXQnxOf2onPmxwpa5GjZmGhODTTV85N5i9zwbCeT:PPBr5XpEpQgf2o+xwpGWmGh0TVoN5kzE
MD5:	953434AD47F5C2003B186C7B2E817D4F
SHA1:	8568DEEB4E58E4CA8B05A9A8F870BC26F185A58A
SHA-256:	ABB8237331BB32B29B72BC2DB4133432D9C4B42C16ACB4D87D26B3DC4DB08E37
SHA-512:	03F8F26709DA5A97B466E784B96CC67F86B1D875CDCFDD558010CDFF168C42534F726059AC2FAC036F2789A931B59FFE8B95FDE2A2D7E83116ECBB4461930EE
Malicious:	false
Reputation:	unknown
Preview:	regfP...P...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmr.*x..... ....!%HvLE.^.....P.....}vp8.EJ.W!I.).Q..... ..hbin.....p.\..,.....nk,.s.*x..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .s.*x..... .....P..... .....Z.....Root.....lf.....Root....nk .s.*x.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

\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/HToZV9It199hiALIlg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBllydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8

\Device\ConDrv	
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):	6.6910111765717115
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:	OG9rNsihJ7.exe
File size:	321024
MD5:	5c7b46771055043f59e0451a342b7ed1
SHA1:	5362af084622dc8efc661c703d4c7c5dd6839be1
SHA256:	0245c82558329cfd8ef5ef901e4929075d4d873ba20d9704731758580caed7be
SHA512:	f16fdd7212bc64f05ef67b41e29dd8966645b7fa0e7d78e8883503503a3589a090c54846500925f17b8dd1d133e1f5bb37bbde16f3e5c50864847c17f7df2c06
SSDEEP:	6144:1dNi2kGfRHG5p1JX9BnaPGMq3yvNITJwD3EsG1ALc:XNsGfIfnpBCvuJw4sG+
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.....h_.....

File Icon

Icon Hash:	c8d0d8e0f0e0e4e0

Static PE Info

General

Entrypoint:	0x41b5e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F68D411 [Mon Sep 21 16:25:53 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6801e04a0c2ca60ac2497c0d8723846b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e6be	0x3e800	False	0.58234375	data	6.96452184589	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.340494791667	data	3.46807929414	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.zafif	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.naladin	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ger	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	0.594841452206	data	5.84519780089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x465a	0x4800	False	0.346137152778	data	3.69349629733	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 21:04:55.877932072 CET	192.168.2.5	8.8.8.8	0x7494	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:56.323577881 CET	192.168.2.5	8.8.8.8	0x4933	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:56.493093014 CET	192.168.2.5	8.8.8.8	0xe41d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:56.927520037 CET	192.168.2.5	8.8.8.8	0xf2bd	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 21:04:57.367894888 CET	192.168.2.5	8.8.8.8	0x4af2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:57.536972046 CET	192.168.2.5	8.8.8.8	0x1f4c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:59.186599016 CET	192.168.2.5	8.8.8.8	0xd444	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:59.364273071 CET	192.168.2.5	8.8.8.8	0x992b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:59.856811047 CET	192.168.2.5	8.8.8.8	0x1977	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:02.046914101 CET	192.168.2.5	8.8.8.8	0x7b24	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:02.222532988 CET	192.168.2.5	8.8.8.8	0xf3bf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:02.713391066 CET	192.168.2.5	8.8.8.8	0x3fda	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:03.289355993 CET	192.168.2.5	8.8.8.8	0xb555	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:03.469676971 CET	192.168.2.5	8.8.8.8	0xea8f	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:05.988169909 CET	192.168.2.5	8.8.8.8	0x14b4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:06.242278099 CET	192.168.2.5	8.8.8.8	0xadd5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.186929941 CET	192.168.2.5	8.8.8.8	0x7f70	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.427100897 CET	192.168.2.5	8.8.8.8	0x3d00	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.655709982 CET	192.168.2.5	8.8.8.8	0x147d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.846596956 CET	192.168.2.5	8.8.8.8	0x31d8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:08.083580971 CET	192.168.2.5	8.8.8.8	0xb57c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:08.250816107 CET	192.168.2.5	8.8.8.8	0x9388	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.244743109 CET	192.168.2.5	8.8.8.8	0xf22f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.415355921 CET	192.168.2.5	8.8.8.8	0x2e3a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.582473040 CET	192.168.2.5	8.8.8.8	0x11d1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.776063919 CET	192.168.2.5	8.8.8.8	0xe372	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:13.304208040 CET	192.168.2.5	8.8.8.8	0x55	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:13.750782013 CET	192.168.2.5	8.8.8.8	0xf6a9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:13.945065975 CET	192.168.2.5	8.8.8.8	0x3e41	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:14.142004967 CET	192.168.2.5	8.8.8.8	0x7e8a	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:16.810718060 CET	192.168.2.5	8.8.8.8	0x780d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:16.979959965 CET	192.168.2.5	8.8.8.8	0x5162	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:17.161175013 CET	192.168.2.5	8.8.8.8	0xdbe6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.889240980 CET	192.168.2.5	8.8.8.8	0xc6ab	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:31.535420895 CET	192.168.2.5	8.8.8.8	0xd6fa	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:38.788865089 CET	192.168.2.5	8.8.8.8	0x5d88	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:38.973396063 CET	192.168.2.5	8.8.8.8	0xc0e2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:39.412410975 CET	192.168.2.5	8.8.8.8	0x35d4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:39.601656914 CET	192.168.2.5	8.8.8.8	0xda93	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.071396112 CET	192.168.2.5	8.8.8.8	0x6de5	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 21:05:40.235871077 CET	192.168.2.5	8.8.8.8	0x6600	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.415290117 CET	192.168.2.5	8.8.8.8	0xc569	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.594440937 CET	192.168.2.5	8.8.8.8	0xd440	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.760528088 CET	192.168.2.5	8.8.8.8	0xe780	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.929953098 CET	192.168.2.5	8.8.8.8	0xf572	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.097774982 CET	192.168.2.5	8.8.8.8	0x6af7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.270361900 CET	192.168.2.5	8.8.8.8	0x53f1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.448005915 CET	192.168.2.5	8.8.8.8	0xf55f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.652324915 CET	192.168.2.5	8.8.8.8	0x9aa7	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:44.983249903 CET	192.168.2.5	8.8.8.8	0x6528	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.159842968 CET	192.168.2.5	8.8.8.8	0x8d7c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.366871119 CET	192.168.2.5	8.8.8.8	0xaab3	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.883004904 CET	192.168.2.5	8.8.8.8	0xc70f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.052864075 CET	192.168.2.5	8.8.8.8	0x618a	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.254223108 CET	192.168.2.5	8.8.8.8	0x1909	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.441540003 CET	192.168.2.5	8.8.8.8	0xa099	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.627866030 CET	192.168.2.5	8.8.8.8	0x2c58	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.859006882 CET	192.168.2.5	8.8.8.8	0x4dac	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:47.035129070 CET	192.168.2.5	8.8.8.8	0xda7c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:54.463512897 CET	192.168.2.5	8.8.8.8	0x1e0c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:54.629339933 CET	192.168.2.5	8.8.8.8	0xc241	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.111166954 CET	192.168.2.5	8.8.8.8	0x927a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.279705048 CET	192.168.2.5	8.8.8.8	0xa1d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.445163965 CET	192.168.2.5	8.8.8.8	0x77e6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.622380018 CET	192.168.2.5	8.8.8.8	0xdc86	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:59.973757029 CET	192.168.2.5	8.8.8.8	0x109b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:00.155663013 CET	192.168.2.5	8.8.8.8	0xa8a6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:00.540651083 CET	192.168.2.5	8.8.8.8	0xa441	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:03.809344053 CET	192.168.2.5	8.8.8.8	0x1cf8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:04.012093067 CET	192.168.2.5	8.8.8.8	0xab6b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:04.175112009 CET	192.168.2.5	8.8.8.8	0xc3c1	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:05.754617929 CET	192.168.2.5	8.8.8.8	0xcdcd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:05.994390011 CET	192.168.2.5	8.8.8.8	0x1c4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:11.553761959 CET	192.168.2.5	8.8.8.8	0x40ed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:11.800241947 CET	192.168.2.5	8.8.8.8	0x1d4c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:11.997239113 CET	192.168.2.5	8.8.8.8	0xbaf8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:12.131275892 CET	192.168.2.5	8.8.8.8	0x3b8e	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 21:06:12.174395084 CET	192.168.2.5	8.8.8.8	0xa8a5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:12.431009054 CET	192.168.2.5	8.8.8.8	0xe862	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:14.960942984 CET	192.168.2.5	8.8.8.8	0xc20d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:15.144355059 CET	192.168.2.5	8.8.8.8	0x2ad7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:15.331216097 CET	192.168.2.5	8.8.8.8	0x31ff	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:16.744563103 CET	192.168.2.5	8.8.8.8	0x3ccd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:16.906570911 CET	192.168.2.5	8.8.8.8	0x497c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:17.084588051 CET	192.168.2.5	8.8.8.8	0xc79c	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:18.430932999 CET	192.168.2.5	8.8.8.8	0x98a1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:18.594903946 CET	192.168.2.5	8.8.8.8	0xa8de	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:18.834065914 CET	192.168.2.5	8.8.8.8	0x4b70	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:22.463624954 CET	192.168.2.5	8.8.8.8	0x471d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:25.071058035 CET	192.168.2.5	8.8.8.8	0x577d	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.249953985 CET	192.168.2.5	8.8.8.8	0x710e	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.282507896 CET	192.168.2.5	8.8.8.8	0x8279	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.451266050 CET	192.168.2.5	8.8.8.8	0x7bba	Standard query (0)	ipwhois.app	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.736634016 CET	192.168.2.5	8.8.8.8	0xcbd5	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.026542902 CET	192.168.2.5	8.8.8.8	0xa536	Standard query (0)	c9d0e790b353537889bd47a364f5acff43c11f248.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.214611053 CET	192.168.2.5	8.8.8.8	0xd2fb	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.452898026 CET	192.168.2.5	8.8.8.8	0x9061	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:32.928822994 CET	192.168.2.5	8.8.8.8	0xd453	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.723789930 CET	192.168.2.5	8.8.8.8	0xa787	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.852749109 CET	192.168.2.5	8.8.8.8	0x332d	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 21:04:56.163722038 CET	8.8.8.8	192.168.2.5	0x7494	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:56.340941906 CET	8.8.8.8	192.168.2.5	0x4933	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:56.779325962 CET	8.8.8.8	192.168.2.5	0xe41d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:57.214174986 CET	8.8.8.8	192.168.2.5	0xf2bd	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:57.386841059 CET	8.8.8.8	192.168.2.5	0x4af2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:57.824347973 CET	8.8.8.8	192.168.2.5	0x1f4c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:04:59.204412937 CET	8.8.8.8	192.168.2.5	0xd444	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 21:04:59.685348034 CET	8.8.8.8	192.168.2.5	0x992b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:00.174863100 CET	8.8.8.8	192.168.2.5	0x1977	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:02.064315081 CET	8.8.8.8	192.168.2.5	0x7b24	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:02.544847012 CET	8.8.8.8	192.168.2.5	0xf3bf	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:03.024291039 CET	8.8.8.8	192.168.2.5	0x3fda	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:03.308669090 CET	8.8.8.8	192.168.2.5	0xb555	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:03.767642975 CET	8.8.8.8	192.168.2.5	0xea8f	No error (0)	privacy-tools-for-you-780.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:06.007678986 CET	8.8.8.8	192.168.2.5	0x14b4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:06.259608984 CET	8.8.8.8	192.168.2.5	0xadd5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.209027052 CET	8.8.8.8	192.168.2.5	0x7f70	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.444776058 CET	8.8.8.8	192.168.2.5	0x3d00	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.674513102 CET	8.8.8.8	192.168.2.5	0x147d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:07.866856098 CET	8.8.8.8	192.168.2.5	0x31d8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:08.102863073 CET	8.8.8.8	192.168.2.5	0xb57c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:08.270349026 CET	8.8.8.8	192.168.2.5	0x9388	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.264030933 CET	8.8.8.8	192.168.2.5	0xf22f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.432816982 CET	8.8.8.8	192.168.2.5	0x2e3a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.602001905 CET	8.8.8.8	192.168.2.5	0x11d1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:10.796231985 CET	8.8.8.8	192.168.2.5	0xe372	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:13.323513985 CET	8.8.8.8	192.168.2.5	0x55	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:13.770212889 CET	8.8.8.8	192.168.2.5	0xf6a9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:13.964700937 CET	8.8.8.8	192.168.2.5	0x3e41	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:14.163177967 CET	8.8.8.8	192.168.2.5	0x7e8a	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:14.163177967 CET	8.8.8.8	192.168.2.5	0x7e8a	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:14.163177967 CET	8.8.8.8	192.168.2.5	0x7e8a	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:14.163177967 CET	8.8.8.8	192.168.2.5	0x7e8a	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 21:05:14.163177967 CET	8.8.8.8	192.168.2.5	0x7e8a	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:16.828425884 CET	8.8.8.8	192.168.2.5	0x780d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:16.997550011 CET	8.8.8.8	192.168.2.5	0x5162	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:17.479644060 CET	8.8.8.8	192.168.2.5	0xdbe6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.908535957 CET	8.8.8.8	192.168.2.5	0xc6ab	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.908535957 CET	8.8.8.8	192.168.2.5	0xc6ab	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.908535957 CET	8.8.8.8	192.168.2.5	0xc6ab	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.908535957 CET	8.8.8.8	192.168.2.5	0xc6ab	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.908535957 CET	8.8.8.8	192.168.2.5	0xc6ab	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:28.908535957 CET	8.8.8.8	192.168.2.5	0xc6ab	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:31.855371952 CET	8.8.8.8	192.168.2.5	0xd6fa	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:38.808269978 CET	8.8.8.8	192.168.2.5	0x5d88	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:39.260253906 CET	8.8.8.8	192.168.2.5	0xc0e2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:39.431783915 CET	8.8.8.8	192.168.2.5	0x35d4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:39.887650013 CET	8.8.8.8	192.168.2.5	0xda93	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.091041088 CET	8.8.8.8	192.168.2.5	0x6de5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.254775047 CET	8.8.8.8	192.168.2.5	0x6600	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.434448957 CET	8.8.8.8	192.168.2.5	0xc569	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.613733053 CET	8.8.8.8	192.168.2.5	0xd440	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.777997971 CET	8.8.8.8	192.168.2.5	0xe780	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:40.949367046 CET	8.8.8.8	192.168.2.5	0xf572	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.115518093 CET	8.8.8.8	192.168.2.5	0x6af7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.289719105 CET	8.8.8.8	192.168.2.5	0x53f1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:41.467417002 CET	8.8.8.8	192.168.2.5	0xf55f	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 21:05:41.669790030 CET	8.8.8.8	192.168.2.5	0x9aa7	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.002109051 CET	8.8.8.8	192.168.2.5	0x6528	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.177006006 CET	8.8.8.8	192.168.2.5	0x8d7c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.388562918 CET	8.8.8.8	192.168.2.5	0xaab3	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.388562918 CET	8.8.8.8	192.168.2.5	0xaab3	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:45.901753902 CET	8.8.8.8	192.168.2.5	0xc70f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.076894999 CET	8.8.8.8	192.168.2.5	0x618a	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.273220062 CET	8.8.8.8	192.168.2.5	0x1909	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.460666895 CET	8.8.8.8	192.168.2.5	0xa099	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.649183035 CET	8.8.8.8	192.168.2.5	0x2c58	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:46.880328894 CET	8.8.8.8	192.168.2.5	0x4dac	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:47.054697990 CET	8.8.8.8	192.168.2.5	0xda7c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:54.481074095 CET	8.8.8.8	192.168.2.5	0x1e0c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:54.648716927 CET	8.8.8.8	192.168.2.5	0xc241	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.130471945 CET	8.8.8.8	192.168.2.5	0x927a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.298561096 CET	8.8.8.8	192.168.2.5	0xa1d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.462627888 CET	8.8.8.8	192.168.2.5	0x77e6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:56.639723063 CET	8.8.8.8	192.168.2.5	0xdc86	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:05:59.990679026 CET	8.8.8.8	192.168.2.5	0x109b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:00.174967051 CET	8.8.8.8	192.168.2.5	0xa8a6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:00.559953928 CET	8.8.8.8	192.168.2.5	0xa441	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:03.830070972 CET	8.8.8.8	192.168.2.5	0x1cf8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:04.031857014 CET	8.8.8.8	192.168.2.5	0xab6b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:04.479187965 CET	8.8.8.8	192.168.2.5	0xc3c1	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:05.771756887 CET	8.8.8.8	192.168.2.5	0xcdcd	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:06.013828039 CET	8.8.8.8	192.168.2.5	0x1c4	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 21:06:11.572953939 CET	8.8.8.8	192.168.2.5	0x40ed	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:11.819535017 CET	8.8.8.8	192.168.2.5	0x1d4c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:12.016437054 CET	8.8.8.8	192.168.2.5	0xbaf8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:12.193625927 CET	8.8.8.8	192.168.2.5	0xa8a5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:12.238771915 CET	8.8.8.8	192.168.2.5	0x3b8e	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:12.452526093 CET	8.8.8.8	192.168.2.5	0xe862	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:14.980345964 CET	8.8.8.8	192.168.2.5	0xc20d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:15.163513899 CET	8.8.8.8	192.168.2.5	0x2ad7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:15.351063967 CET	8.8.8.8	192.168.2.5	0x31ff	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:16.761666059 CET	8.8.8.8	192.168.2.5	0x3ccd	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:16.924042940 CET	8.8.8.8	192.168.2.5	0x497c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:17.104187012 CET	8.8.8.8	192.168.2.5	0xc79c	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:18.450618029 CET	8.8.8.8	192.168.2.5	0x98a1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:18.614340067 CET	8.8.8.8	192.168.2.5	0xa8de	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:18.853131056 CET	8.8.8.8	192.168.2.5	0x4b70	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:22.483175039 CET	8.8.8.8	192.168.2.5	0x471d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:25.090707064 CET	8.8.8.8	192.168.2.5	0x577d	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:25.090707064 CET	8.8.8.8	192.168.2.5	0x577d	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:25.090707064 CET	8.8.8.8	192.168.2.5	0x577d	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:25.090707064 CET	8.8.8.8	192.168.2.5	0x577d	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:25.090707064 CET	8.8.8.8	192.168.2.5	0x577d	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.273663998 CET	8.8.8.8	192.168.2.5	0x710e	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 21:06:29.303054094 CET	8.8.8.8	192.168.2.5	0x8279	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 21:06:29.475207090 CET	8.8.8.8	192.168.2.5	0x7bba	No error (0)	ipwhois.app		136.243.172.101	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.765475035 CET	8.8.8.8	192.168.2.5	0xcbd5	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 21:06:29.765475035 CET	8.8.8.8	192.168.2.5	0xcbd5	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.765475035 CET	8.8.8.8	192.168.2.5	0xcbd5	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.765475035 CET	8.8.8.8	192.168.2.5	0xcbd5	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.765475035 CET	8.8.8.8	192.168.2.5	0xcbd5	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:29.765475035 CET	8.8.8.8	192.168.2.5	0xcbd5	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.046150923 CET	8.8.8.8	192.168.2.5	0xa536	No error (0)	c9d0e790b353537889bd47a364f5acff43c11f248.xyz		185.112.83.97	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.232129097 CET	8.8.8.8	192.168.2.5	0xd2fb	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.232129097 CET	8.8.8.8	192.168.2.5	0xd2fb	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.232129097 CET	8.8.8.8	192.168.2.5	0xd2fb	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.232129097 CET	8.8.8.8	192.168.2.5	0xd2fb	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.232129097 CET	8.8.8.8	192.168.2.5	0xd2fb	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:30.473182917 CET	8.8.8.8	192.168.2.5	0x9061	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:32.947655916 CET	8.8.8.8	192.168.2.5	0xd453	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.743685961 CET	8.8.8.8	192.168.2.5	0xa787	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.869694948 CET	8.8.8.8	192.168.2.5	0x332d	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.869694948 CET	8.8.8.8	192.168.2.5	0x332d	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.869694948 CET	8.8.8.8	192.168.2.5	0x332d	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Jan 14, 2022 21:06:34.869694948 CET	8.8.8.8	192.168.2.5	0x332d	No error (0)	raw.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- xmmufccsxa.net
  - host-data-coin-11.com
- ejoocwvno.net
- ymxxgm.org
- vxhncf.com
- csftwsmo.net

- fdbmpnrkfj.org
- jxeebf.com
- kxkku.net
- data-host-coin-8.com
- fdcyfq.net
- lujat.com
- ttjdaam.net
- uqfbvly.com
- privacy-tools-for-you-780.com
- hwyvhm.net
- idmvulr.net
- unicupload.top
- vooxhw.org
- vvdrjru.com
- ubjcetayse.org
- sxcrq.org
- ywlgtk.net
- foglcav.com
- hnhyhp.org
- nefwc.net
- 185.7.214.171:8080
- fsakwxty.com
- jcjkx.net
- lhgju.net
- bsjhi.org
- bypwmjeu.org
- tmxneir.net
- ukskogxssc.org
- lnvtcbw.net
- skipwlik.net

- stogr.net
- ldxocdirn.net
- usarcmaqw.net
- drmput.com
- wktbs.org
- ycnydaydt.net
- ymgfpln.net
- dxepeeelwv.net
- rynnvo.org
- kahaurdys.org
- ttbac.net
- aubfgyajhw.net
- ryxvaojf.com
- dusqhhm.org
- wuqgjbcank.net
- rcwmq.org
- fgphlloppj.net
- fasyb.com
- 81.163.30.181
- qajnwkj.net
- xcbxaaktm.org
- 74.201.28.62
- pwvhyavumw.com
- elaxxedw.com
- wfytf.org
- phwtttkmh.net
- xdhynq.com
- kpspxwto.net
- fnyafy.net
- cwjtumctb.net

- psthjovmnc.org
- takjt.net
- umolln.net
- ptkbedc.org
- uoymbdayk.org
- mqousgs.net
- uhxofu.com
- gmykjkt.net
- quwfn.net
- plgevhj.net
- jwsdnsli.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: OG9rNsihJ7.exe PID: 4948 Parent PID: 5408

General

Start time:	21:04:12
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\OG9rNsihJ7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OG9rNsihJ7.exe"
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	5C7B46771055043F59E0451A342B7ED1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: OG9rNsihJ7.exe PID: 5424 Parent PID: 4948

General

Start time:	21:04:14
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\OG9rNsihJ7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OG9rNsihJ7.exe"
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	5C7B46771055043F59E0451A342B7ED1
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: 00000001.00000002.298084613.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.298215878.0000000001FA1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3472 Parent PID: 5424

General

Start time:	21:04:21
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000000.279897390.0000000003031000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 3756 Parent PID: 556

General

Start time:	21:04:24
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000

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

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4840 Parent PID: 556

General

Start time:	21:04:25
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6092 Parent PID: 556

General

Start time:	21:04:35
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 2600 Parent PID: 556

General

Start time:	21:04:36
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4568 Parent PID: 556

General

Start time:	21:04:36
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 2076 Parent PID: 556

General

Start time:	21:04:37
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6999d0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 1188 Parent PID: 556

General

Start time:	21:04:37
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

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

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6656 Parent PID: 556

General

Start time:	21:04:42
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: vfgiwcs PID: 6824 Parent PID: 904

General

Start time:	21:04:56
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\vfgiwcs
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vfgiwcs
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	5C7B46771055043F59E0451A342B7ED1
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: vfgiwcs PID: 6840 Parent PID: 6824

General

Start time:	21:04:58
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\vfgiwcs
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vfgiwcs
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	5C7B46771055043F59E0451A342B7ED1
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.349879535.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.349992094.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: B1B2.exe PID: 6924 Parent PID: 3472

General

Start time:	21:05:00
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B1B2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B1B2.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
Reputation:	moderate

Analysis Process: svchost.exe PID: 6976 Parent PID: 556

General

Start time:	21:05:03
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: BFBD.exe PID: 6984 Parent PID: 3472

General

Start time:	21:05:04
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\BFBD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BFBD.exe
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	5C7B46771055043F59E0451A342B7ED1

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

Analysis Process: WerFault.exe PID: 7020 Parent PID: 6976

General

Start time:	21:05:04
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 6924 -ip 6924
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: BFBD.exe PID: 7140 Parent PID: 6984

General

Start time:	21:05:08
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\BFBD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BFBD.exe
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	5C7B46771055043F59E0451A342B7ED1
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: 00000018.00000002.366966979.00000000004B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000018.00000002.366989519.00000000004D1000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 7148 Parent PID: 556

General

Start time:	21:05:08
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 7156 Parent PID: 6924

General

Start time:	21:05:08
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6924 -s 520
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: 254E.exe PID: 1268 Parent PID: 3472

General

Start time:	21:05:08
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\254E.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\254E.exe
Imagebase:	0x400000
File size:	324096 bytes
MD5 hash:	41AB3EFA04441E560A279BD0F7C0503D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001C.00000002.357825450.000000000083A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000001C.00000002.357825450.000000000083A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000001C.00000002.357794608.000000000081A000.00000004.00000020.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: 3136.exe PID: 5060 Parent PID: 3472

General

Start time:	21:05:12
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3136.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3136.exe
Imagebase:	0x400000
File size:	321536 bytes
MD5 hash:	023802260A0216012A5F00079406D967
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: 0000001D.00000002.380383276.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001D.00000003.362218485.00000000007F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001D.00000002.380671348.00000000006C0000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 3BC6.exe PID: 6244 Parent PID: 3472

General

Start time:	21:05:15
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3BC6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3BC6.exe
Imagebase:	0x650000
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: 0000001E.00000002.412827478.0000000003991000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 89%, ReversingLabs

Analysis Process: cmd.exe PID: 5992 Parent PID: 5060

General

Start time:	21:05:16
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\ffiawxs\
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6028 Parent PID: 5992

General

Start time:	21:05:17
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1928 Parent PID: 5060

General

Start time:	21:05:17
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\xqfkd fcl.exe" C:\Windows\SysWOW64\ffiawxs\
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2272 Parent PID: 1928

General

Start time:	21:05:18
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 3532 Parent PID: 5060

General

Start time:	21:05:18
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create ffiawxs binPath= "C:\Windows\SysWOW64\ffiawxs \xqfkdfcl.exe /d\"C:\Users\user\AppData\Local\Temp\3136.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xa0000
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: 5328 Parent PID: 3532

General

Start time:	21:05:19
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5500 Parent PID: 5060

General

Start time:	21:05:19
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description ffiawxs "wifi internet conection
Imagebase:	0xa0000
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: 5580 Parent PID: 5500

General

Start time:	21:05:20
Start date:	14/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff64e5e0000
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: 7068 Parent PID: 5060

General

Start time:	21:05:21
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start ffiawxs
Imagebase:	0xa0000
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: 6896 Parent PID: 7068

General

Start time:	21:05:21
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 3720 Parent PID: 5060

General

Start time:	21:05:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x11f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: xqfkdfcl.exe PID: 5432 Parent PID: 556

General

Start time:	21:05:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\ffiawxs\xqfkdfcl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ffiawxs\xqfkdfcl.exe /d"C:\Users\user\AppData\Local\Temp\3136.exe"
Imagebase:	0x400000
File size:	13666304 bytes
MD5 hash:	5C50CF4AF77D12BF94B3FC09437C8B16
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: 0000002A.00000003.388526176.00000000007F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002A.00000002.391463142.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002A.00000002.391805380.0000000000680000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002A.00000002.391938773.0000000000840000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4560 Parent PID: 3720

General

Start time:	21:05:22
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3440 Parent PID: 5432

General

Start time:	21:05:26
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xb90000
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: 0000002C.00000002.524985253.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 3BC6.exe PID: 7064 Parent PID: 6244

General

Start time:	21:05:29
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3BC6.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\3BC6.exe
Imagebase:	0x3c0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002D.00000000.408848131.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002D.00000000.407524125.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002D.00000000.408441992.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002D.00000002.429951321.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002D.00000000.408078077.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 7140 Parent PID: 556

General

Start time:	21:05:32
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis