ID: 553220
Sample Name:
9ro85QVN0F.exe
Cookbook: default.jbs
Time: 13:57:19
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

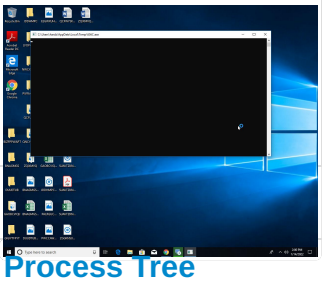
Windows Analysis Report 9ro85QVN0F.exe

Overview

General Information

Sample Name:	9ro85QVN0F.exe
Analysis ID:	553220
MD5:	4e806c42b23b04..
SHA1:	39d29853690f371.
SHA256:	847fd5a4cae442a.
Tags:	CoinMiner exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

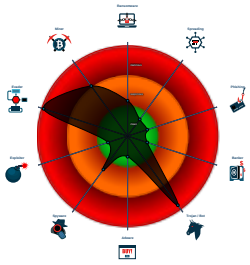
RedLine SmokeLoader Tofsee Vidar

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
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected Vidar stealer
- Multi AV Scanner detection for doma…

Classification



Process Tree

- **System is w10x64**
- 9ro85QVN0F.exe (PID: 6156 cmdline: "C:\Users\user\Desktop\9ro85QVN0F.exe" MD5: 4E806C42B23B043FA7409D108EECAADB)
  - 9ro85QVN0F.exe (PID: 6980 cmdline: "C:\Users\user\Desktop\9ro85QVN0F.exe" MD5: 4E806C42B23B043FA7409D108EECAADB)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 411E.exe (PID: 4256 cmdline: C:\Users\user\AppData\Local\Temp\411E.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 6752 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4256 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 53DC.exe (PID: 1740 cmdline: C:\Users\user\AppData\Local\Temp\53DC.exe MD5: 4E806C42B23B043FA7409D108EECAADB)
        - 53DC.exe (PID: 6976 cmdline: C:\Users\user\AppData\Local\Temp\53DC.exe MD5: 4E806C42B23B043FA7409D108EECAADB)
      - E6C4.exe (PID: 6924 cmdline: C:\Users\user\AppData\Local\Temp\E6C4.exe MD5: C94FBEF580C7CD0BA874360D0B997F22)
      - F4CF.exe (PID: 6380 cmdline: C:\Users\user\AppData\Local\Temp\F4CF.exe MD5: 50BADD524B2E3FAF0FF050DD5BE8A584)
        - cmd.exe (PID: 6228 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\jdijwvkg\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5092 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\bzxmernq.exe" C:\Windows\SysWOW64\jdijwvkg\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - FD6B.exe (PID: 6972 cmdline: C:\Users\user\AppData\Local\Temp\FD6B.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - FD6B.exe (PID: 5976 cmdline: C:\Users\user\AppData\Local\Temp\FD6B.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - wuapihost.exe (PID: 6700 cmdline: C:\Windows\System32\wuapihost.exe -Embedding MD5: 85C9C161B102A164EC09A23CACDDD09E)
- svchost.exe (PID: 2224 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6672 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6596 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6580 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4776 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5388 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5020 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5224 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6956 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 672 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- iscgwer (PID: 6784 cmdline: C:\Users\user\AppData\Roaming\iscgwer MD5: 4E806C42B23B043FA7409D108EECAADB)
  - iscgwer (PID: 6780 cmdline: C:\Users\user\AppData\Roaming\iscgwer MD5: 4E806C42B23B043FA7409D108EECAADB)
- svchost.exe (PID: 6756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4848 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.340237120.000000000530000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000019.00000002.458534378.000000000650000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000018.00000002.406836326.000000000582000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000018.00000002.406836326.000000000582000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0000000B.00000000.326990095.0000000004DE1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.iscgwer.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
17.0.iscgwer.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
22.0.53DC.exe.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
22.0.53DC.exe.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
17.0.iscgwer.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 18 entries				

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Bitcoin Miner:

Found strings related to Crypto-Mining

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)

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 method to dynamically call methods (often used by packers)

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

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)

Sample uses process hollowing technique

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, 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

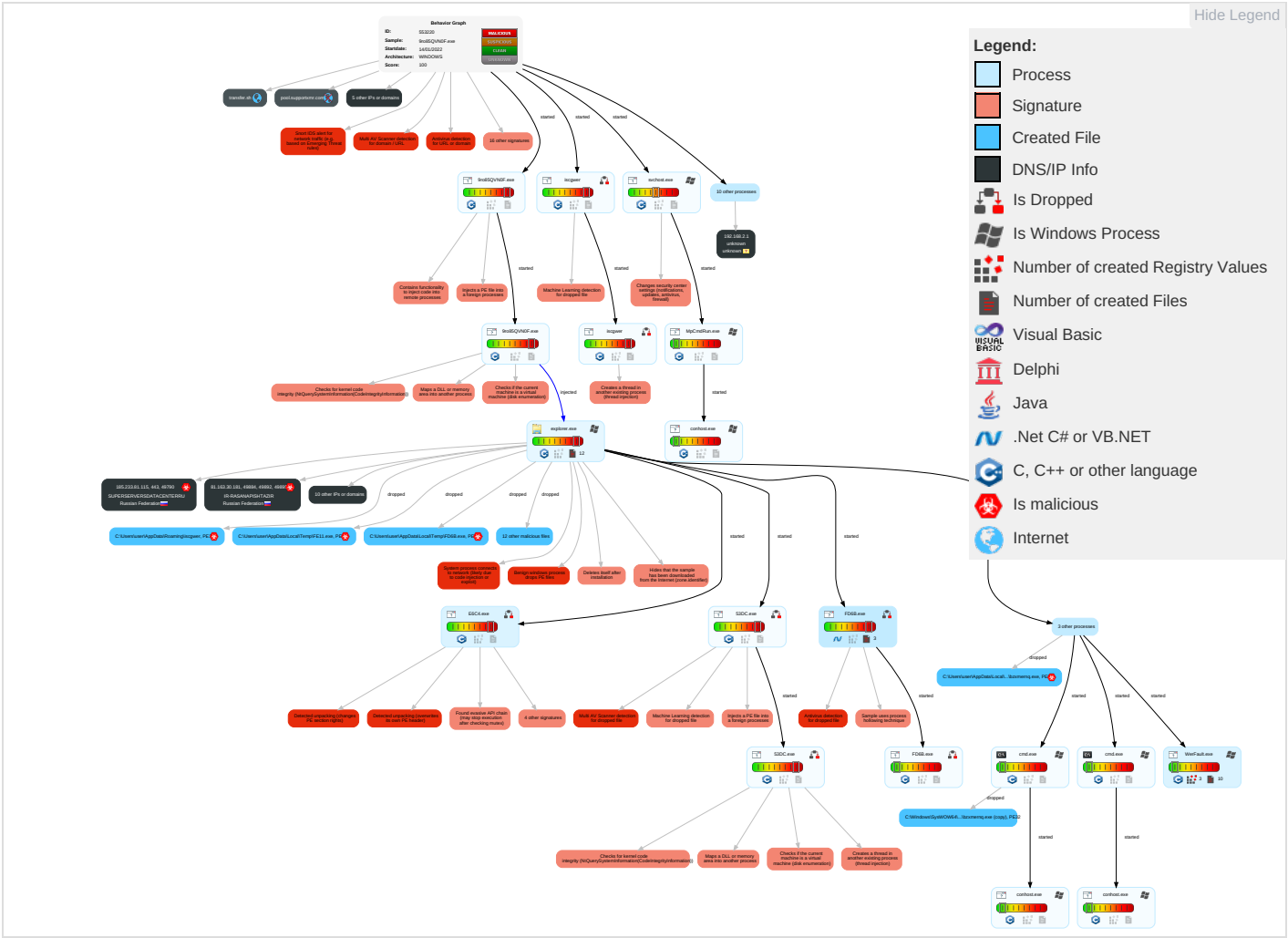
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service
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	Ingress Transfe
Domain Accounts	Shared Modules 1	Windows Service 3	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	Encryp Channe
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Windows Service 3	Software Packing 3 3	NTDS	System Information Discovery 2 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-St Port 1
Cloud Accounts	Command and Scripting Interpreter 3	Network Logon Script	Process Injection 6 1 3	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Non-Applica Layer Protocc
Replication Through Removable Media	Service Execution 2	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applica Layer Protocc
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	Commo Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
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 Protocc
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 Tra Protocc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 3 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 6 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
9ro85QVN0F.exe	37%	Virustotal		Browse
9ro85QVN0F.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FD6B.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\bzxmernq.exe	100%	Avira	TR/Crypt.XPACK.Gen	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\D54.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\iscgwer	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\656C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E6C4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F4CF.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\53A8.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\14F6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\53DC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FE11.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\433C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\411E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\27E3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7480.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FD6B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bzxmernq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\411E.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\411E.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\433C.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\433C.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\53A8.exe	50%	ReversingLabs	Win32.Infostealer.Generic	
C:\Users\user\AppData\Local\Temp\53DC.exe	47%	ReversingLabs	Win32.Trojan.DiskWriter	
C:\Users\user\AppData\Local\Temp\656C.exe	28%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\D54.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\D54.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.0.53DC.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.53DC.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.iscgwer.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.FD6B.exe.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.0.53DC.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.9ro85QVN0F.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.iscgwer.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.iscgwer.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
17.0.iscgwer.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.iscgwer.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.53DC.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
20.2.53DC.exe.6315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.iscgwer.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
42.0.FD6B.exe.1a0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.2.53DC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.FD6B.exe.1a0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.2.411E.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.E6C4.exe.680000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.0.411E.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.iscgwer.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
25.2.F4CF.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
25.3.F4CF.exe.780000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.2.FD6B.exe.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.0.FD6B.exe.cf0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.3.411E.exe.510000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.FD6B.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.0.53DC.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
19.0.411E.exe.500e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.9ro85QVN0F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.iscgwer.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
24.2.E6C4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.FD6B.exe.cf0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
42.2.FD6B.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
25.2.F4CF.exe.650e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.0.53DC.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File

Source	Detection	Scanner	Label	Link	Download
24.2.E6C4.exe.660e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.1.53DC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.1.iscgwer.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.9ro85QVN0F.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.411E.exe.500e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.53DC.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
0.2.9ro85QVN0F.exe.6315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.411E.exe.500e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.411E.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.9ro85QVN0F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.FD6B.exe.1a0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.9ro85QVN0F.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.iscgwer.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.FD6B.exe.cf0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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	13%	Virustotal		Browse
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://81.163.30.181/2.exe	1%	Virustotal		Browse
http://81.163.30.181/2.exe	100%	Avira URL Cloud	malware	
http://81.163.30.181/101.exe	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	16%	Virustotal		Browse
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	100%	Avira URL Cloud	malware	
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://81.163.30.181/1.exe	100%	Avira URL Cloud	malware	
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://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://81.163.30.181/11.msi	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://81.163.30.181/6236.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
pool-fr.supportxmr.com	37.187.95.110	true	false		high
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	8.209.70.0	true	false		high
cdn.discordapp.com	162.159.130.233	true	false		high
privacy-tools-for-you-780.com	8.209.70.0	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
data-host-coin-8.com	8.209.70.0	true	false		high
a0621686.xsph.ru	141.8.192.193	true	false		high
pool.supportxmr.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
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	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://81.163.30.181/2.exe	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://81.163.30.181/101.exe	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://81.163.30.181/1.exe	true	• Avira URL Cloud: malware	unknown
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://81.163.30.181/11.msi	true	• Avira URL Cloud: safe	unknown
http://81.163.30.181/6236.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
172.67.139.105	goo.su	United States		13335	CLOUDFLARENETUS	false
8.209.70.0	host-data-coin-11.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
81.163.30.181	unknown	Russian Federation		58303	IR-RASANAPISHTAZIR	true
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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553220
Start date:	14.01.2022
Start time:	13:57:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 38s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	9ro85QVN0F.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:	43
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.mine.winEXE@41/30@88/11
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.9% (good quality ratio 15.8%) • Quality average: 49.2% • Quality standard deviation: 40.4%
HCA Information:	• Successful, ratio: 56% • 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
13:58:53	Task Scheduler	Run new task: Firefox Default Browser Agent D5FEEC786DC5C0BA path: C:\Users\user\AppData\Roaming\iscgwer
13:59:10	API Interceptor	1x Sleep call for process: E6C4.exe modified
13:59:12	API Interceptor	1x Sleep call for process: WerFault.exe modified
13:59:18	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
13:59:22	API Interceptor	7x Sleep call for process: svchost.exe modified
13:59:53	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
14:00:06	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe
14:00:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe
14:01:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run RegHost C:\Users\user\AppData\Roaming\Microsoft\RegHost.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_411E.exe_136b771e572cd787a55eb6b4a02adbff53ae1a72_57e8a279_1a0b6c9c\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):	0.8137658224565194
Encrypted:	false
SSDEEP:	192:beMd8rgzkz8HQ0l/XjjIq/u7shS274IteYtA:FzeEQ0lLjN/u7shX4ltLA
MD5:	54030922AB757909919668CCE6BDFE26
SHA1:	F7C7360D8229C3B9B9282873D87A1BA1DB940EA9
SHA-256:	7CBEB7A9C2D918533091E4B7F000F889999399AAE61B5D6240906A35490F0582
SHA-512:	CB7B2EBBF569B33482720D2B17C73A939E6906B679EF69537288DE7171F923AC1237C5EE467F5FD60F089FE34CD334B265F5CDB4AE98ABEEFCA043DA187A1B89
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.=.1.3.2.8.6.6.7.1.1.4.8.4.9.2.1.7.5.1.....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.=.1.3.2.8.6.6.7.1.1.5.0.9.4.5.2.9.7.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.5.d.5.1.0.a.d.-.5.2.5.6.-.4.6.f.6.-.b.9.f.4.-.c.8.4.5.a.e.1.2.8.5.b.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.b.4.8.6.6.e.f.-.b.3.7.1.-.4.9.a.2.-.8.1.7.f.-.6.7.f.8.d.8.6.e.2.9.a.2.....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.=.4.1.1.E...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.a.0.-.0.0.0.1.-.0.0.1.c.-.1.5.c.0.-.9.6.e.f.9.1.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.1.a.5.1.6.0.7.b.f.b.d.1.3.3.7.e.3.8.2.1.9.1.6.3.b.7.9.4.9.e.d.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.!.4.1.1.E...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\WER5DF6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 21:59:09 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.1217822657706638
Encrypted:	false
SSDEEP:	192:ihDigrUJrLROeh0kGb4j+icei5FJvEHKPPt7juIp:iSZweeBY2fp
MD5:	7BAAB78ECED1127F2905C0DB7BD9E54A
SHA1:	D83E4F1F16068D95ED7E589FFBCA6A5805E15293
SHA-256:	FC0AC1AB27D249802E1C4175AAC4E198BDD028A4C3507C7DCFF68855B92B4C96
SHA-512:	840696EFB7E86435C32CE9A3D2792BDBD43BA196A0259C2987F1D4531E9ECC1A0CACC75D5DE4E8907105FA14EDCA736D056162952B46F2CF331A3FD2A3A4FAB5
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....-..a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....$..a..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6394.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):	8388
Entropy (8bit):	3.699114705496345
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi8ul6u6YF8mSU7Kgmf/eRS6CpD689bK8sfZtum:RrlsNi36u6Y/SU7Kgmf2RSpKPfD
MD5:	F79F27A8134D52B4589E5C28B3ECD2BB
SHA1:	166E199AC5C5EF78EBD4D23D0E155595C09CF4DD

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6394.tmp.WERInternalMetadata.xml	
SHA-256:	3680569F87C99CCC37A6E30AA68654FA0F78A74D4F0A847E6BD2EE268402B53C
SHA-512:	CC8E2C3B52AB4C1202946F2AE00C55639831880EC4BDE63B37E09BC01D96DC0CEC9F33BCD7B1955AC679308D7A5A5A8BD30B223F301404452E4A10E7D73E745
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.>.4.2.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER65C8.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):	4.471314868456998
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI99JWSC8BO/8fm8M4Jd8qF7+q8vL8tiWmKRgTd:uITfq+4SNRJBKKDmKRgTd
MD5:	5DBE7B67816566709F3ACF0B172F033A
SHA1:	09A9B5D572149E224529D966BAA7F9727C67DED6
SHA-256:	D441D8FBF876BCEE9B18B8F06C904948DB9EE3A8F916B98DF959EE32A9FF7B58
SHA-512:	A3A7ACB4A1CD8529A24821501076D45F680633DC97186337C88CE5E393A9333407A5D4F30D27EE59335F6CD5BC1F702DA64EA42B4BAA7E73D3895D5B07B3E0E
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="1342509" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FD6B.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\FD6B.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11022541052871243
Encrypted:	false
SSDEEP:	12:26uXm/Ey6q9995ahq3qQ10nMCldimE8eawHjcxRH:267l68vLyMCldzE9BHjcxR
MD5:	E125A0B0D33FEA7326D8F39DDADEDBE4
SHA1:	D74F3115620849008B523785B5A106C57A51F949
SHA-256:	F6E52C6DFAEB03E2D0AF3A4C41111580BB9783D7E9B8D5AF75644E84CD429D1D
SHA-512:	479D5119E66E51345436BB6311D342A36039961A7A37129BE6AF9E23EDA33F42C1EAAB2DCAC3A01B33F8A473BA2C773AA8F840D88AF6B9D1FD19EADAED0719CE

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Malicious:	false
Reputation:	unknown
Preview:	.....\.....f..|.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....W.}..... .....;z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s .\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.\.....O..|..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11267307713306338
Encrypted:	false
SSDEEP:	12:f/lTXm/Ey6q9995abOL1miM3qQ10nMCldimE8eawHza1miIl/:3lKl68k61tMLyMCldzE9BHza1tIl/
MD5:	7B28FA88D1E22EC7DB348008C787F608
SHA1:	8E5BE4EF718FAD2722F84787388AA48A0C010D96
SHA-256:	EA8CA5EE6AD32D729B991484A4E48FE308EDA7D6BC0C6E91FB63D84DF3D7253B
SHA-512:	9CF77D6FA866211F06E4FA296A567D8FE6914DE065F830AD725268FA0D238B20F25040ACBCF5298E340E12ABF3FCA25C84B86AEA055CD9DFB4E88CC6F9A9B8 D
Malicious:	false
Reputation:	unknown
Preview:	.....\.....b..|.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....W.}..... .....5.s.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.\.....|..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11272810934557069
Encrypted:	false
SSDEEP:	12:AuTXm/Ey6q9995ajL1mK2P3qQ10nMCldimE8eawHza1mKRP/:/Kl68QL1iPLyMCldzE9BHza11/
MD5:	C6EE22D81C57583D05F2D3770AA07F2F
SHA1:	EDD0CF3C45CCDC26681C28B1512DC7AE4C291CA3
SHA-256:	AC595BDD3D34C82BB67344DC1143EEF8CC6D1D049C6A2F4A25EC7F78EE0BF03E
SHA-512:	2E8BCB7CFA7ACB98047ECDF6401B40FC930562E3EE09D4623C59570DCFBA905A01384338A8EA268C2643A9ED4C70B648EAE83B2F8FB66A8C6192B25EF1C478 F
Malicious:	false
Reputation:	unknown
Preview:	.....\.....0..|.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....W.}..... .....i.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.\.....<..|..... ....

C:\Users\user\AppData\Local\Temp\14F6.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.848740173602419
Encrypted:	false
SSDEEP:	6144:P5aWbksiNTB6VcYEL6MQU9KKqmUhZiZs3lyiFiznt804G+YCN+0ORduk:P5atNTQVcYE9KKqfziZs3EznX4mCN+0Y
MD5:	1A92A9C5ED159ED0914F2E4570661A15
SHA1:	46E7A169436AE366758CB3C01A40552CD59C0AEE
SHA-256:	F3AA18EC1D6075E859622E8AF114DF28939EB5414CC8B0F0094B43B0C55D1DE8
SHA-512:	428A91128D57EE07198A1494CFF8047C8F4F47916920259B81188680A0C99D4AB7F7447271EAB99A414D956255332E23969BE32314714283E8655DAC985A383C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\14F6.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....\.....0....@..... ....lq.....pt..<.....code...~8.....`..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... ....

C:\Users\user\AppData\Local\Temp\27E3.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\411E.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0 ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i. hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@..... .....e..P.....2..... Y..@..... .0.....text..... ..`.rdata..D?...0...@..."..... @..@.data...X....p...$...b.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\433C.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\433C.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..''?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\53A8.exe

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

C:\Users\user\AppData\Local\Temp\53DC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.687125826295423
Encrypted:	false
SSDEEP:	6144:+WbLfFa4xe0ga5Pvt8Cta8wm/jso47Qtgi5aR8vuz+sGfeqK:+SFes5PvHtayQoDtgpR8vuy6
MD5:	4E806C42B23B043FA7409D108EECAADB
SHA1:	39D29853690F371FB690D427D34EACE3946B6553
SHA-256:	847FD5A4CAE442AFC596F09B8A8F2DE13BC85356DCD8B897A3B4A89081F5046F
SHA-512:	24DA5692EE3AFBBC71D62CBBAC33BB094E326E0FA3F234C580C7A994F1C47A768AD1579F9652BF2B7174541C0E447BBD5952F8457F3CBC3B4BD9613B165D732
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=..S..S..S.....S....g.S..](..S..R...S....S.....S.....S.Rich.S..... ....PE..L...m.h_.....@.....u_.....(.....@.....H..... ..text...V..... ..`.data.....@....tad.....@....lux.....@....civujo.....@....rsrc.....@..@ .reloc..\F.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\656C.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.8500958922173165
Encrypted:	false
SSDEEP:	6144:P5aWbksiNTBQlCuchwPuVbIn97yYUdL6TVrp/LbU7LY6TzeWJwN:P5atNTqlCl84wJyYUpUrLbU9SWJwN
MD5:	FEB8ADD569247306CB0271C907607238
SHA1:	BB9353D602A82FF174AFE7574F4AFD6009E2A8B0
SHA-256:	E7587776ADECF859E137E7AF3DA4B9B6FD9428E6F89CC48D3A63886D490BAACA
SHA-512:	6F650A1D44A11B2205E59DC915E244AC43988C7AC32972280CC5C5CA1ED668B683C2B06F61AEF8D2E91CE1C83FC4E0788207023B6CA81372ACDB4935F040268

C:\Users\user\AppData\Local\Temp\656C.exe

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....\.....0....@..... .....lq.....pt..<.....code...~8.....:..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... ....

C:\Users\user\AppData\Local\Temp\7480.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3595648
Entropy (8bit):	**7.997561940529216**
Encrypted:	**true**
SSDEEP:	98304:a084oJCztB83FsWOotbBDtRexIIJFzGfb7Wgyp5:a084RxEFsWHD90Ia5
MD5:	7BD7AFEFAC0B988373D1CDB929602689
SHA1:	75760C800B95B61EB2F0E4C4D27667C05DB52619
SHA-256:	D50B018DBE38F8FF4FD5DDA66F03830B2208ADAF0FF43E8F2D965CC25E20B7E4
SHA-512:	FD30725AB5CD93BA1DDDD1761894993A8B858144C32BA301529695DCF05DC495EA91CA1A0D43C2ADB8C7397320E5D40626A9E19524A6B678294D7B5BFEA4BC C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S....?.6. .....|.O. ....pM.....6..#..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....C...P.....@.....1.....@....rsrc.....pM.....p0.....@....HQIHSjN.....O.....2..... ..@....adata.....S.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\D54.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427 D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..U(...(...(...6.).1...6.?.W....I..+...(.....6.8....6.(.)...6.-.)...Rich(..... .....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8..... .....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|..... @..@.reloc..4F...0...H...I.....@..B..... .....

C:\Users\user\AppData\Local\Temp\E6C4.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	322560
Entropy (8bit):	6.703621223316465
Encrypted:	false
SSDEEP:	6144:RZO3M89ge8ZiiVaOcOCgireB6RgkO4/hzNzGf+GP6f:RZagD5Vovvr9RgA/hZEPa
MD5:	C94FBEF580C7CD0BA874360D0B997F22
SHA1:	6533AF2DAEB72A2E9C8E52194052C1444E203DB1

C:\Users\user\AppData\Local\Temp\E6C4.exe	
SHA-256:	19CEF530181D49F24A3513EE5546BF69A12482F66466DB0D8A5C45DA206BE569
SHA-512:	89C0270B8239624F7F2FD1D1D26BC1A5DBBCD7397908230FBA5F80DE69326BC9F52A488EF1D53BD227AB22346484445846A89322224574E02837D04A3BDA511D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=..S..S..S.....S....g.S..](..S..R...S.....S.....S.....S.Rich.S..... ....PE..L....._.....@.....x.....4...(.....@.....H..... .text..... ..`.data.....@....zufow.....@....ruh.....@....yilub.....@....rsrc..... .....@..@. reloc..fF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\F4CF.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.687273736877821
Encrypted:	false
SSDEEP:	6144:H9ccaRn35MCCXxwaUbmV/nCEHF1qgkruPOaZUGfa5:H+9PMtwFUfCG1qglPOSG
MD5:	50BADD524B2E3FAF0FF050DD5BE8A584
SHA1:	E03B18A84F9926BB68D23D993A859FF0BA6B0BDE
SHA-256:	B3396E7D185C1CA1FAD9A33382ECE95F9DC5CEBCC8E259F7D16A94D4DB74CF21
SHA-512:	F892699F20B1965277B3D594073C2903A40F8C611D9CC467826E9D33F0A9AD315C0CDC4458595F440EB7DB6C9FB70587B7702D8DAB508A26248BE6F674F1D271
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=..S..S..S.....S....g.S..](..S..R...S.....S.....S.....S.Rich.S..... ....PE..L.....h_.....@.....(.....@.....H..... .text...F..... ..`.data.....@....gemuta.....@....yid.....@....yofuyiz.....@....rsrc..... .....@..@.reloc..\F.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\FD6B.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....I.. ...`....@.. ..... ..@.....`I..K....`..... ..... ..H.....text....).. ...*..... ..`.rsrc.....`.....@....reloc..... .....0.....@..B.....I.....H.....?.....hX..}.....(....*..0.....(d...8....*.~....u....s....z&8.....8.....*.....*....(d...(....*...j*..... ..*.....*.....*.....*....(....*.~(....(^...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\FE11.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

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\FE11.exe</th></tr>
<tr><td>SHA-512:</td><td>B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE
7</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Antivirus:</td><td>• Antivirus: Joe Sandbox ML, Detection: 100%</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>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.....................@..@..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\bzxmernq.exe</th></tr>
<tr><td>Process:</td><td>C:\Users\user\AppData\Local\Temp\F4CF.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (GUI) Intel 80386, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>13996032</td></tr>
<tr><td>Entropy (8bit):</td><td>3.7880507743534038</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24576:++6Vg1VGTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTL:r1n</td></tr>
<tr><td>MD5:</td><td>19D1F6C45BAA1FAB9256C4AA8ECCA231</td></tr>
<tr><td>SHA1:</td><td>E32408B2B06F13F48D9BA597BD53CCD3ED57CE68</td></tr>
<tr><td>SHA-256:</td><td>5DD26C035DB298110EE036225F2041DD52B863F9B8A8DDEDD6D23093E7DBBEFA</td></tr>
<tr><td>SHA-512:</td><td>C08B4A2744D73B0BAB93A71B135934E4FCF5B850A6AE8524C08C8119FEF35016AD604D5B38AA0BA75A2E437125F2B88BCDF8A649214723954DBED59D3C6CA43
B</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Antivirus:</td><td>• Antivirus: Avira, Detection: 100%
• Antivirus: Joe Sandbox ML, Detection: 100%</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.........=..S..S..S......S....g.S..](..S..R...S.....S......S......S.Rich.S..... ....PE..L.....h_..@..(...@..............H.......................... .text...F.......................... ..`.data...............................@....gemuta............................@....yid...............................@....yofuyiz...........................@....rsrc......................... .....@..@.reloc..\F.........................@..B.. ....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001 (copy)</th></tr>
<tr><td>Process:</td><td>C:\Windows\System32\svchost.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>65536</td></tr>
<tr><td>Entropy (8bit):</td><td>0.11022541052871243</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:26uXm/Ey6q9995ahq3qQ10nMCldimE8eawHjcxRH:267l68vLyMCldzE9BHjcxR</td></tr>
<tr><td>MD5:</td><td>E125A0B0D33FEA7326D8F39DDADEDBE4</td></tr>
<tr><td>SHA1:</td><td>D74F3115620849008B523785B5A106C57A51F949</td></tr>
<tr><td>SHA-256:</td><td>F6E52C6DFAEB03E2D0AF3A4C41111580BB9783D7E9B8D5AF75644E84CD429D1D</td></tr>
<tr><td>SHA-512:</td><td>479D5119E66E51345436BB6311D342A36039961A7A37129BE6AF9E23EDA33F42C1EAAB2DCAC3A01B33F8A473BA2C773AA8F840D88AF6B9D1FD19EADAED0719
CE</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>..\.......f..|.....................B.............Zb...@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..W.}..... ......;z...........S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s .\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l..........P.P.\.......O..|.. ....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)</th></tr>
<tr><td>Process:</td><td>C:\Windows\System32\svchost.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>65536</td></tr>
<tr><td>Entropy (8bit):</td><td>0.11267307713306338</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:f/lTXm/Ey6q9995abOL1miM3qQ10nMCldimE8eawHza1mill/:3lKl68k61tMLyMCldzE9BHza1tll/</td></tr>
<tr><td>MD5:</td><td>7B28FA88D1E22EC7DB348008C787F608</td></tr>
<tr><td>SHA1:</td><td>8E5BE4EF718FAD2722F84787388AA48A0C010D96</td></tr>
<tr><td>SHA-256:</td><td>EA8CA5EE6AD32D729B991484A4E48FE308EDA7D6BC0C6E91FB63D84DF3D7253B</td></tr>
</table>

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
SHA-512:	9CF77D6FA866211F06E4FA296A567D8FE6914DE065F830AD725268FA0D238B20F25040ACBCF5298E340E12ABF3FCA25C84B86AEA055CD9DFB4E88CC6F9A9B8 D
Malicious:	false
Reputation:	unknown
Preview:	.....\.....b..|.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....W.}..... .....5.s.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.\.....|..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001O (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11272810934557069
Encrypted:	false
SSDEEP:	12:AuTXm/Ey6q9995ajL1mK2P3qQ10nMCldimE8eawHza1mKRP/:/Kl68QL1iPLyMCldzE9BHza11/
MD5:	C6EE22D81C57583D05F2D3770AA07F2F
SHA1:	EDD0CF3C45CCDC26681C28B1512DC7AE4C291CA3
SHA-256:	AC595BDD3D34C82BB67344DC1143EEF8CC6D1D049C6A2F4A25EC7F78EE0BF03E
SHA-512:	2E8BCB7CFA7ACB98047ECDF6401B40FC930562E3EE09D4623C59570DCFBA905A01384338A8EA268C2643A9ED4C70B648EAE83B2F8FB66A8C6192B25EF1C478 F
Malicious:	false
Reputation:	unknown
Preview:	.....\.....0..|.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....W.}..... .....i.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.\.....<..|..... ....

C:\Users\user\AppData\Roaming\iscgwer	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.687125826295423
Encrypted:	false
SSDEEP:	6144:+WbLfFa4xe0ga5Pvt8Cta8wm/jso47Qtgi5aR8vuz+sGfeqK:+SFes5PvHtayQoDtgpR8vuy6
MD5:	4E806C42B23B043FA7409D108EECAADB
SHA1:	39D29853690F371FB690D427D34EACE3946B6553
SHA-256:	847FD5A4CAE442AFC596F09B8A8F2DE13BC85356DCD8B897A3B4A89081F5046F
SHA-512:	24DA5692EE3AFBBC71D62CBBAC33BB094E326E0FA3F234C580C7A994F1C47A768AD1579F9652BF2B7174541C0E447BBD5952F8457F3CBC3B4BD9613B165D73 2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=..S..S..S.....S....g.S..](..S..R...S....S.....S.....S.Rich.S..... ....PE..L...m.h_.....@.....u_.....(.....@.....H..... ..text...V..... ..`.data.....@....tad.....@....lux.....@....civujo.....@....rsrc.....@..@ .reloc..\F.....H.....@..B..... .....

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

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.163844099475939
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zg+b:j+s+v+b+P+m+0+Q+q+3+b
MD5:	B5DE6DD84C98809EF316370957DAFC67
SHA1:	77B67A0D1C9330A407DF002E7379F6D18CA80B1A
SHA-256:	CDAF524879DD680A9371DD50A89837DED2D5E354468EDBFDEE62FB5CB75EC16C
SHA-512:	D9E65B73D9EE9245318B340EF9862AD9355480107D33537F89342C2B1B92A04EC4B256269E767915D535664DEBDA98A24120AD43CDEA0700BCC8DFE0CFED4C3
Malicious:	false
Reputation:	unknown
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220114_215814_003.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3009477934568885
Encrypted:	false
SSDEEP:	96:eCHWdj/o+ol5MJ96/YIHCkvI2lHSk+P4klT2YjFzeNMC3dJRW:d2Vgen2ctbCTw
MD5:	79150C3DE7A59F9D91DE45304057AEA2
SHA1:	D04203330C99D91B4726F18611E495829C830F9E
SHA-256:	184C0723489AF3CB59A19B1C8F580CD58C00AEDDBB06EFFAC1BD0D2B2961DA8E
SHA-512:	10B99CBE8C3DF31F63526ED0933A41321EDE3E585967FFD01D0024C662F2E4C0280084D2A472940E8FAC9DA2488EA1C7C7BA25EA8C418246B24A7EDF4BB1043 B
Malicious:	false
Reputation:	unknown
Preview:	....!...................................T........................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1... ......h............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...2.0.2.2.0.1.1.4._.2.1.5.8.1.4._.0.0.3...e.t.l.........P.P.........T.. ....

C:\Windows\SysWOW64\jdijwvkg\bzxmernq.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13996032
Entropy (8bit):	3.7880507743534038
Encrypted:	false
SSDEEP:	24576:++6Vg1VGTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTL:r1n
MD5:	19D1F6C45BAA1FAB9256C4AA8ECCA231
SHA1:	E32408B2B06F13F48D9BA597BD53CCD3ED57CE68
SHA-256:	5DD26C035DB298110EE036225F2041DD52B863F9B8A8DDEDD6D23093E7DBBEFA
SHA-512:	C08B4A2744D73B0BAB93A71B135934E4FCF5B850A6AE8524C08C8119FEF35016AD604D5B38AA0BA75A2E437125F2B88BCDF8A649214723954DBED59D3C6CA43 B
Malicious:	false
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........=..S..S..S......S....g.S..](..S..R...S.....S......S......S.Rich.S..... ....PE..L.....h_...@...(..@...............H.......................... .text...F.......................... ..`.data...............................@....gemuta............................@....yid................................@....yofuyiz............................@....rsrc......................... .....@..@.reloc..\F.........................@..B... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.687125826295423
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:	9ro85QVN0F.exe
File size:	320000
MD5:	4e806c42b23b043fa7409d108eecaadb
SHA1:	39d29853690f371fb690d427d34eace3946b6553
SHA256:	847fd5a4cae442afc596f09b8a8f2de13bc85356dcd8b897a3b4a89081f5046f
SHA512:	24da5692ee3afbbc71d62cbbac33bb094e326e0fa3f234c580c7a994f1c47a768ad1579f9652bf2b7174541c0e447bbd5952f8457f3cbc3b4bd9613b165d7332
SSDEEP:	6144:+WbLfFa4xe0ga5Pvt8Cta8wm/jso47Qtgi5aR8vuz+sGfeqK:+SFes5PvHtayQoDtgpR8vuy6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=...S...S...S.....S....g.S..](...S...R...S.....S.....S.....S.....S.Rich..S.....PE..L...m.h_.....

File Icon

Icon Hash:	c8d0d8e0f8e0f4e8

Static PE Info

General

Entrypoint:	0x41b690
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F68886D [Mon Sep 21 11:03:09 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:	bfce8d99da2229492c7de3a8a6087683

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e756	0x3e800	False	0.58257421875	data	6.96623040888	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x40000	0x10c988	0x1800	False	0.341145833333	data	3.46431598321	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tad	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.lux	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.civujo	0x14f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x83d0	0x8400	False	0.597212357955	data	5.82312083073	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x465c	0x4800	False	0.347927517361	data	3.69266698613	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 13:58:53.260260105 CET	192.168.2.3	8.8.8.8	0x3c03	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:53.708993912 CET	192.168.2.3	8.8.8.8	0x59ae	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:54.152388096 CET	192.168.2.3	8.8.8.8	0xeea9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:54.600578070 CET	192.168.2.3	8.8.8.8	0xc87a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:55.176249981 CET	192.168.2.3	8.8.8.8	0x3339	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:55.350025892 CET	192.168.2.3	8.8.8.8	0xc30c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:56.748620987 CET	192.168.2.3	8.8.8.8	0xe92a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:56.916774035 CET	192.168.2.3	8.8.8.8	0x406d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:57.091743946 CET	192.168.2.3	8.8.8.8	0x5486	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 13:59:01.984139919 CET	192.168.2.3	8.8.8.8	0x377b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:02.226161957 CET	192.168.2.3	8.8.8.8	0xd52e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:02.495044947 CET	192.168.2.3	8.8.8.8	0xd9b2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:03.614922047 CET	192.168.2.3	8.8.8.8	0x5a92	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:03.849128962 CET	192.168.2.3	8.8.8.8	0xae9f	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:05.220077038 CET	192.168.2.3	8.8.8.8	0xae9f	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:06.978780031 CET	192.168.2.3	8.8.8.8	0x8c4b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.150871992 CET	192.168.2.3	8.8.8.8	0x3c08	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.323868990 CET	192.168.2.3	8.8.8.8	0x96d9	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.548402071 CET	192.168.2.3	8.8.8.8	0xa642	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.716831923 CET	192.168.2.3	8.8.8.8	0x16f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.880069971 CET	192.168.2.3	8.8.8.8	0x6064	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:08.048026085 CET	192.168.2.3	8.8.8.8	0x5295	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:08.214258909 CET	192.168.2.3	8.8.8.8	0x8ac3	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:10.068484068 CET	192.168.2.3	8.8.8.8	0xd7ba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:10.264724016 CET	192.168.2.3	8.8.8.8	0xa8db	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:10.880444050 CET	192.168.2.3	8.8.8.8	0x4cf2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:11.389574051 CET	192.168.2.3	8.8.8.8	0x6d73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:13.573808908 CET	192.168.2.3	8.8.8.8	0x78d9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:13.742561102 CET	192.168.2.3	8.8.8.8	0x527e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:13.907990932 CET	192.168.2.3	8.8.8.8	0xfcd7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:14.116682053 CET	192.168.2.3	8.8.8.8	0x439e	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:18.014628887 CET	192.168.2.3	8.8.8.8	0xdc8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:18.222428083 CET	192.168.2.3	8.8.8.8	0x13b1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:18.427845955 CET	192.168.2.3	8.8.8.8	0x3ba6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:39.986620903 CET	192.168.2.3	8.8.8.8	0xad11	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:40.566854954 CET	192.168.2.3	8.8.8.8	0xa2f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:40.800518036 CET	192.168.2.3	8.8.8.8	0x522f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.198199034 CET	192.168.2.3	8.8.8.8	0xe169	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.388201952 CET	192.168.2.3	8.8.8.8	0x2944	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.600965023 CET	192.168.2.3	8.8.8.8	0x5775	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.790718079 CET	192.168.2.3	8.8.8.8	0x98e8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.984402895 CET	192.168.2.3	8.8.8.8	0xf863	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:43.252228975 CET	192.168.2.3	8.8.8.8	0x1351	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:43.448209047 CET	192.168.2.3	8.8.8.8	0x8c40	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:43.757477999 CET	192.168.2.3	8.8.8.8	0x609f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:44.071616888 CET	192.168.2.3	8.8.8.8	0x5705	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 13:59:44.276002884 CET	192.168.2.3	8.8.8.8	0x752b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:44.734683990 CET	192.168.2.3	8.8.8.8	0x4bfb	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:46.515445948 CET	192.168.2.3	8.8.8.8	0x8865	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:46.708954096 CET	192.168.2.3	8.8.8.8	0xcff2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.107867002 CET	192.168.2.3	8.8.8.8	0xdf5f	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.683250904 CET	192.168.2.3	8.8.8.8	0x8325	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.858074903 CET	192.168.2.3	8.8.8.8	0x492a	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.043952942 CET	192.168.2.3	8.8.8.8	0x852d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.292716980 CET	192.168.2.3	8.8.8.8	0x6f9e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.464782000 CET	192.168.2.3	8.8.8.8	0x8624	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.693960905 CET	192.168.2.3	8.8.8.8	0xec81	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.977354050 CET	192.168.2.3	8.8.8.8	0xeef8	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:50.308330059 CET	192.168.2.3	8.8.8.8	0x2db8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:50.510072947 CET	192.168.2.3	8.8.8.8	0x8e7b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:52.339437962 CET	192.168.2.3	8.8.8.8	0xc02a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:52.766990900 CET	192.168.2.3	8.8.8.8	0xc0f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:52.990679026 CET	192.168.2.3	8.8.8.8	0xe6a3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:53.387569904 CET	192.168.2.3	8.8.8.8	0x43c6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:53.887733936 CET	192.168.2.3	8.8.8.8	0x4d58	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:57.324872971 CET	192.168.2.3	8.8.8.8	0x35ab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:57.495378971 CET	192.168.2.3	8.8.8.8	0x27c5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:58.096651077 CET	192.168.2.3	8.8.8.8	0x905a	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:59.126961946 CET	192.168.2.3	8.8.8.8	0x905a	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.069653988 CET	192.168.2.3	8.8.8.8	0x9da2	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.617562056 CET	192.168.2.3	8.8.8.8	0xa04d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.927841902 CET	192.168.2.3	8.8.8.8	0xcc76	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:05.279290915 CET	192.168.2.3	8.8.8.8	0xe601	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:09.830545902 CET	192.168.2.3	8.8.8.8	0x4a2b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:10.643510103 CET	192.168.2.3	8.8.8.8	0xe07f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:12.873323917 CET	192.168.2.3	8.8.8.8	0x79eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:13.268222094 CET	192.168.2.3	8.8.8.8	0xd5a6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:13.874664068 CET	192.168.2.3	8.8.8.8	0x563	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.087749958 CET	192.168.2.3	8.8.8.8	0xc4f5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.303622961 CET	192.168.2.3	8.8.8.8	0xb39c	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:16.296823025 CET	192.168.2.3	8.8.8.8	0x4af4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:17.093225956 CET	192.168.2.3	8.8.8.8	0x75b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:18.008430958 CET	192.168.2.3	8.8.8.8	0x1eb9	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:00:20.643426895 CET	192.168.2.3	8.8.8.8	0xbd42	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:22.402417898 CET	192.168.2.3	8.8.8.8	0x892b	Standard query (0)	pool.supportxmr.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:31.145945072 CET	192.168.2.3	8.8.8.8	0x69a2	Standard query (0)	a0621686.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:38.237560034 CET	192.168.2.3	8.8.8.8	0xa2ef	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:43.658696890 CET	192.168.2.3	8.8.8.8	0x7572	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 13:58:53.545952082 CET	8.8.8.8	192.168.2.3	0x3c03	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:53.998173952 CET	8.8.8.8	192.168.2.3	0x59ae	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:54.439436913 CET	8.8.8.8	192.168.2.3	0xeea9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:55.028279066 CET	8.8.8.8	192.168.2.3	0xc87a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:55.195472002 CET	8.8.8.8	192.168.2.3	0x3339	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:55.369292974 CET	8.8.8.8	192.168.2.3	0xc30c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:56.768579960 CET	8.8.8.8	192.168.2.3	0xe92a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:56.934833050 CET	8.8.8.8	192.168.2.3	0x406d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:58:57.437783957 CET	8.8.8.8	192.168.2.3	0x5486	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:02.003447056 CET	8.8.8.8	192.168.2.3	0x377b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:02.245398045 CET	8.8.8.8	192.168.2.3	0xd52e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:02.514441013 CET	8.8.8.8	192.168.2.3	0xd9b2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:03.635468006 CET	8.8.8.8	192.168.2.3	0x5a92	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:04.165971994 CET	8.8.8.8	192.168.2.3	0xae9f	No error (0)	privacy-tools-for-you-780.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:05.566719055 CET	8.8.8.8	192.168.2.3	0xae9f	No error (0)	privacy-tools-for-you-780.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:06.997880936 CET	8.8.8.8	192.168.2.3	0x8c4b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.170008898 CET	8.8.8.8	192.168.2.3	0x3c08	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.429474115 CET	8.8.8.8	192.168.2.3	0x96d9	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.567471981 CET	8.8.8.8	192.168.2.3	0xa642	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.734281063 CET	8.8.8.8	192.168.2.3	0x16f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:07.899265051 CET	8.8.8.8	192.168.2.3	0x6064	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 13:59:08.065099001 CET	8.8.8.8	192.168.2.3	0x5295	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:08.233400106 CET	8.8.8.8	192.168.2.3	0x8ac3	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:10.087042093 CET	8.8.8.8	192.168.2.3	0xd7ba	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:10.696794987 CET	8.8.8.8	192.168.2.3	0xa8db	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:11.195509911 CET	8.8.8.8	192.168.2.3	0x4cf2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:11.408962011 CET	8.8.8.8	192.168.2.3	0x6d73	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:13.593172073 CET	8.8.8.8	192.168.2.3	0x78d9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:13.761769056 CET	8.8.8.8	192.168.2.3	0x527e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:13.925363064 CET	8.8.8.8	192.168.2.3	0xfcd7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:14.143767118 CET	8.8.8.8	192.168.2.3	0x439e	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:14.143767118 CET	8.8.8.8	192.168.2.3	0x439e	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:14.143767118 CET	8.8.8.8	192.168.2.3	0x439e	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:14.143767118 CET	8.8.8.8	192.168.2.3	0x439e	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:14.143767118 CET	8.8.8.8	192.168.2.3	0x439e	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:18.034032106 CET	8.8.8.8	192.168.2.3	0xdc8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:18.241882086 CET	8.8.8.8	192.168.2.3	0x13b1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:18.452987909 CET	8.8.8.8	192.168.2.3	0x3ba6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:40.005820990 CET	8.8.8.8	192.168.2.3	0xad11	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:40.588044882 CET	8.8.8.8	192.168.2.3	0xa2f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:40.819777966 CET	8.8.8.8	192.168.2.3	0x522f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.217735052 CET	8.8.8.8	192.168.2.3	0xe169	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.407866955 CET	8.8.8.8	192.168.2.3	0x2944	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.620006084 CET	8.8.8.8	192.168.2.3	0x5775	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:42.810046911 CET	8.8.8.8	192.168.2.3	0x98e8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:43.003878117 CET	8.8.8.8	192.168.2.3	0xf863	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:43.271547079 CET	8.8.8.8	192.168.2.3	0x1351	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 13:59:43.465672970 CET	8.8.8.8	192.168.2.3	0x8c40	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:43.776849985 CET	8.8.8.8	192.168.2.3	0x609f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:44.088958025 CET	8.8.8.8	192.168.2.3	0x5705	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:44.563781977 CET	8.8.8.8	192.168.2.3	0x752b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:45.022387981 CET	8.8.8.8	192.168.2.3	0x4bfb	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:46.535403967 CET	8.8.8.8	192.168.2.3	0x8865	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:46.729526043 CET	8.8.8.8	192.168.2.3	0xcff2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.132339954 CET	8.8.8.8	192.168.2.3	0xdf5f	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.132339954 CET	8.8.8.8	192.168.2.3	0xdf5f	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.702605963 CET	8.8.8.8	192.168.2.3	0x8325	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:47.877559900 CET	8.8.8.8	192.168.2.3	0x492a	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.061381102 CET	8.8.8.8	192.168.2.3	0x852d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.312066078 CET	8.8.8.8	192.168.2.3	0x6f9e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.482312918 CET	8.8.8.8	192.168.2.3	0x8624	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.713406086 CET	8.8.8.8	192.168.2.3	0xec81	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:48.996695042 CET	8.8.8.8	192.168.2.3	0xeef8	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:50.326821089 CET	8.8.8.8	192.168.2.3	0x2db8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:50.528990984 CET	8.8.8.8	192.168.2.3	0x8e7b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:52.363843918 CET	8.8.8.8	192.168.2.3	0xc02a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:52.786081076 CET	8.8.8.8	192.168.2.3	0xc0f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:53.010150909 CET	8.8.8.8	192.168.2.3	0xe6a3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:53.405926943 CET	8.8.8.8	192.168.2.3	0x43c6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:53.907783985 CET	8.8.8.8	192.168.2.3	0x4d58	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:57.344748974 CET	8.8.8.8	192.168.2.3	0x35ab	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:57.514636993 CET	8.8.8.8	192.168.2.3	0x27c5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 13:59:59.385862112 CET	8.8.8.8	192.168.2.3	0x905a	No error (0)	data-host-coin-8.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 13:59:59.555340052 CET	8.8.8.8	192.168.2.3	0x905a	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.096995115 CET	8.8.8.8	192.168.2.3	0x9da2	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.096995115 CET	8.8.8.8	192.168.2.3	0x9da2	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.096995115 CET	8.8.8.8	192.168.2.3	0x9da2	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.096995115 CET	8.8.8.8	192.168.2.3	0x9da2	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.096995115 CET	8.8.8.8	192.168.2.3	0x9da2	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.636590958 CET	8.8.8.8	192.168.2.3	0xa04d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:04.946705103 CET	8.8.8.8	192.168.2.3	0xcc76	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:05.298472881 CET	8.8.8.8	192.168.2.3	0xe601	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:10.144378901 CET	8.8.8.8	192.168.2.3	0x4a2b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:10.661026955 CET	8.8.8.8	192.168.2.3	0xe07f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:12.891941071 CET	8.8.8.8	192.168.2.3	0x79eb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:13.590600967 CET	8.8.8.8	192.168.2.3	0xd5a6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:13.892220020 CET	8.8.8.8	192.168.2.3	0x563	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.104923964 CET	8.8.8.8	192.168.2.3	0xc4f5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.323115110 CET	8.8.8.8	192.168.2.3	0xb39c	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.323115110 CET	8.8.8.8	192.168.2.3	0xb39c	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.323115110 CET	8.8.8.8	192.168.2.3	0xb39c	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.323115110 CET	8.8.8.8	192.168.2.3	0xb39c	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:14.323115110 CET	8.8.8.8	192.168.2.3	0xb39c	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:16.315987110 CET	8.8.8.8	192.168.2.3	0x4af4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:17.113708973 CET	8.8.8.8	192.168.2.3	0x75b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:18.030103922 CET	8.8.8.8	192.168.2.3	0x1eb9	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:20.665946960 CET	8.8.8.8	192.168.2.3	0xbd42	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:20.665946960 CET	8.8.8.8	192.168.2.3	0xbd42	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:20.665946960 CET	8.8.8.8	192.168.2.3	0xbd42	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:00:20.665946960 CET	8.8.8.8	192.168.2.3	0xbd42	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:20.665946960 CET	8.8.8.8	192.168.2.3	0xbd42	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:22.436964989 CET	8.8.8.8	192.168.2.3	0x892b	No error (0)	pool.supportxmr.com	pool-fr.supportxmr.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 14:00:22.436964989 CET	8.8.8.8	192.168.2.3	0x892b	No error (0)	pool-fr.supportxmr.com		37.187.95.110	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:22.436964989 CET	8.8.8.8	192.168.2.3	0x892b	No error (0)	pool-fr.supportxmr.com		91.121.140.167	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:22.436964989 CET	8.8.8.8	192.168.2.3	0x892b	No error (0)	pool-fr.supportxmr.com		149.202.83.171	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:22.436964989 CET	8.8.8.8	192.168.2.3	0x892b	No error (0)	pool-fr.supportxmr.com		94.23.247.226	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:22.436964989 CET	8.8.8.8	192.168.2.3	0x892b	No error (0)	pool-fr.supportxmr.com		94.23.23.52	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:31.169972897 CET	8.8.8.8	192.168.2.3	0x69a2	No error (0)	a0621686.xsph.ru		141.8.192.193	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:38.257224083 CET	8.8.8.8	192.168.2.3	0xa2ef	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 14:00:43.675483942 CET	8.8.8.8	192.168.2.3	0x7572	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- doekvpclh.net
  - host-data-coin-11.com
- cfaivcludy.net
- ydoois.net
- jpiiaqw.org
- aoblnua.org
- riacbys.net
- elxvnyxk.com
- mcvlfhw.net
- data-host-coin-8.com
- wrbmaiqv.net
- wqgqp.com
- fenydm.net
- firfcooyt.net
- privacy-tools-for-you-780.com
- rwudvrtrt.net

- omhff.net
- unicupload.top
- fbfbuopuh.org
- fdhmpp.org
- yyvmhh.org
- carudedeao.net
- ihkfjyj.org
- sqcnkaq.com
- nbxmbl.org
- ecbfled.com
- 185.7.214.171:8080
- emncntmtow.net
- qsefotqodc.org
- mbnpyehjf.org
- pehjgpd.org
- vpoejhbse.org
- xemsp.com
- juqsasu.org
- vmgenst.org
- bfkxhfurw.com
- jldaqud.net
- yoawoahu.org
- ulvvu.com
- jndibx.com
- aifro.com
- awvcsqp.com
- hsqarkq.org
- ucyfot.org
- xjtksbsy.com
- ppqljylf.org

- fxxlivvp.net
- kkdbsrky.com
- deegamxl.com
- xcxiyncehq.org
- wsvmrr.com
- jqpeh.com
- oaaiijnxpe.org
- jaevdkvwx.net
- jqjxcwg.net
- 81.163.30.181
- rllyqcpmf.net
- yftnkjjlq.org
- ufufplcjp.net
- kbvly.com
- lhythml.org
- xfgpe.org
- dleeejmcen.net
- owkrx.com
- tqglpd.org
- vednhhpcxu.org
- asmhpljw.com
- kakoewy.org
- ukwfgyyso.com
- yqamoj.com
- fqxsvrlwpv.net
- bjxsvd.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 9ro85QVN0F.exe PID: 6156 Parent PID: 3412

General

Start time:	13:58:09
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\9ro85QVN0F.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9ro85QVN0F.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	4E806C42B23B043FA7409D108EECAADB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 9ro85QVN0F.exe PID: 6980 Parent PID: 6156

General

Start time:	13:58:11
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\9ro85QVN0F.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9ro85QVN0F.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	4E806C42B23B043FA7409D108EECAADB
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: 00000001.00000002.340237120.0000000000530000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.340386924.00000000022F1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 2224 Parent PID: 572

General

Start time:	13:58:12
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6672 Parent PID: 572

General

Start time:	13:58:12
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:	0x7ff70d6e0000
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: 6596 Parent PID: 572

General

Start time:	13:58:13
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:	0x7ff70d6e0000
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: 6580 Parent PID: 572

General

Start time:	13:58:13
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000

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

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4776 Parent PID: 572

General

Start time:	13:58:14
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:	0x7ff70d6e0000
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: 5388 Parent PID: 572

General

Start time:	13:58:14
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff793b50000
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: 5020 Parent PID: 572

General

Start time:	13:58:15
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:	0x7ff70d6e0000
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: explorer.exe PID: 3352 Parent PID: 6980

General

Start time:	13:58:18
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000000.326990095.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6956 Parent PID: 572

General

Start time:	13:58:24
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:	0x7ff70d6e0000
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: 672 Parent PID: 572

General

Start time:	13:58:39
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:	0x7ff70d6e0000
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: iscgwer PID: 6784 Parent PID: 664

General

Start time:	13:58:53
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\iscgwer
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\iscgwer
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	4E806C42B23B043FA7409D108EECAADB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: iscgwer PID: 6780 Parent PID: 6784

General

Start time:	13:58:55
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\iscgwer
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\iscgwer
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	4E806C42B23B043FA7409D108EECAADB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.395898272.00000000004D1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.395779805.0000000000460000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6756 Parent PID: 572

General

Start time:	13:58:56
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:	0x7ff70d6e0000
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: 411E.exe PID: 4256 Parent PID: 3352

General

Start time:	13:59:00
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\411E.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\411E.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs

Analysis Process: 53DC.exe PID: 1740 Parent PID: 3352

General

Start time:	13:59:04
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\53DC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\53DC.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	4E806C42B23B043FA7409D108EECAADB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, ReversingLabs

Analysis Process: 53DC.exe PID: 6976 Parent PID: 1740

General

Start time:	13:59:07
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\53DC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\53DC.exe
Imagebase:	0x400000
File size:	320000 bytes

MD5 hash:	4E806C42B23B043FA7409D108EECAADB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.420944310.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.420623827.0000000000430000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 6752 Parent PID: 4256

General

Start time:	13:59:07
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4256 -s 520
Imagebase:	0x150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Analysis Process: E6C4.exe PID: 6924 Parent PID: 3352

General

Start time:	13:59:08
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E6C4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E6C4.exe
Imagebase:	0x400000
File size:	322560 bytes
MD5 hash:	C94FBEF580C7CD0BA874360D0B997F22
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.406836326.0000000000582000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000018.00000002.406836326.0000000000582000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: F4CF.exe PID: 6380 Parent PID: 3352

General

Start time:	13:59:11
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\F4CF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F4CF.exe
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	50BADD524B2E3FAF0FF050DD5BE8A584
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000002.458534378.0000000000650000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000003.413183404.0000000000780000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000002.458185502.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: FD6B.exe PID: 6972 Parent PID: 3352

General

Start time:	13:59:14
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\FD6B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\FD6B.exe
Imagebase:	0xcf0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001A.00000002.474578999.0000000004111000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001A.00000002.474770371.0000000004281000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: MpCmdRun.exe PID: 5224 Parent PID: 5020

General

Start time:	13:59:16
Start date:	14/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6b8fe0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4848 Parent PID: 572

General

Start time:	13:59:16
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5320 Parent PID: 5224

General

Start time:	13:59:17
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wuapihost.exe PID: 6700 Parent PID: 744

General

Start time:	13:59:18
Start date:	14/01/2022
Path:	C:\Windows\System32\wuapihost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wuapihost.exe -Embedding
Imagebase:	0x7ff7d3830000
File size:	10752 bytes
MD5 hash:	85C9C161B102A164EC09A23CACDDD09E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6228 Parent PID: 6380

General

Start time:	13:59:24
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\jdijwvkg\
Imagebase:	0xd80000
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: 6344 Parent PID: 6228

General

Start time:	13:59:24
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 5092 Parent PID: 6380

General

Start time:	13:59:27
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\bzxmernq.exe" C:\Windows\SysWOW64\jdijwvkg\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: FD6B.exe PID: 5976 Parent PID: 6972

General

Start time:	13:59:28
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\FD6B.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\FD6B.exe
Imagebase:	0x1a0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3932 Parent PID: 5092

General

Start time:	13:59:28
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis