ID: 553399
Sample Name:
ZA3cYU28Yl.exe
Cookbook: default.jbs
Time: 20:21:27
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

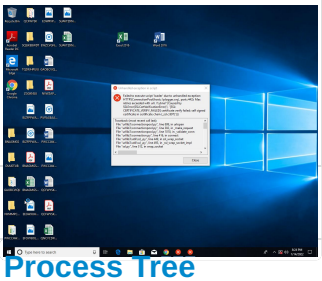
Windows Analysis Report ZA3cYU28Yl.exe

Overview

General Information

Sample Name:	ZA3cYU28Yl.exe
Analysis ID:	553399
MD5:	679831cf1f00950..
SHA1:	f4aa59829222d5e.
SHA256:	760d44ea1a90c1..
Tags:	exe TeamBot
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

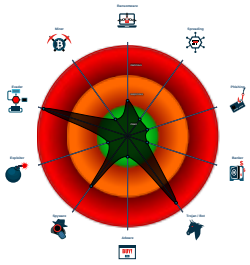
RedLine SmokeLoader Tofsee Vidar

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

Classification



Process Tree

- **System is w10x64**
- ZA3cYU28Yl.exe (PID: 6600 cmdline: "C:\Users\user\Desktop\ZA3cYU28Yl.exe" MD5: 679831CF1F00950B4ADFFBBBA7E6AB46)
  - ZA3cYU28Yl.exe (PID: 6620 cmdline: "C:\Users\user\Desktop\ZA3cYU28Yl.exe" MD5: 679831CF1F00950B4ADFFBBBA7E6AB46)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 9460.exe (PID: 6608 cmdline: C:\Users\user\AppData\Local\Temp\9460.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 4820 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6608 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - A019.exe (PID: 3340 cmdline: C:\Users\user\AppData\Local\Temp\A019.exe MD5: 679831CF1F00950B4ADFFBBBA7E6AB46)
        - A019.exe (PID: 5000 cmdline: C:\Users\user\AppData\Local\Temp\A019.exe MD5: 679831CF1F00950B4ADFFBBBA7E6AB46)
      - 9779.exe (PID: 2228 cmdline: C:\Users\user\AppData\Local\Temp\9779.exe MD5: 043B44289E31BD54357F9A5C21833259)
      - A881.exe (PID: 7004 cmdline: C:\Users\user\AppData\Local\Temp\A881.exe MD5: 9AF71C74219794F100EA801B528339AF)
        - cmd.exe (PID: 6520 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\gebcmxiz\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 956 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\lnagngtg.exe" C:\Windows\SysWOW64\gebcmxiz\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5872 cmdline: C:\Windows\SysWOW64\sc.exe" create gebcmxiz binPath= "C:\Windows\SysWOW64\gebcmxiz\lnagngtg.exe /d\"C:\Users\user\AppData\Local\Temp\A881.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - B217.exe (PID: 4400 cmdline: C:\Users\user\AppData\Local\Temp\B217.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - B217.exe (PID: 6824 cmdline: C:\Users\user\AppData\Local\Temp\B217.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 5672 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6112 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5024 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6376 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 3676 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3608 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6812 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7100 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4520 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- rcvfbte (PID: 1308 cmdline: C:\Users\user\AppData\Roaming\rcvfbte MD5: 679831CF1F00950B4ADFFBBBA7E6AB46)
  - rcvfbte (PID: 5888 cmdline: C:\Users\user\AppData\Roaming\rcvfbte MD5: 679831CF1F00950B4ADFFBBBA7E6AB46)
- svchost.exe (PID: 1324 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6868 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6608 -ip 6608 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4580 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\969F.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x3b87:$x1: https://cdn.discordapp.com/attachments/

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.479069139.0000000003E01000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000003.00000002.333262137.000000000005B1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000003.00000002.333204148.000000000004A0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000A.00000000.327467083.0000000005AC1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000001B.00000002.481840914.0000000004005000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.1.A019.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
26.3.A881.exe.7f0000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
26.2.A881.exe.400000.0.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
26.2.A881.exe.6c0e50.1.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
15.1.rcvfbte.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

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

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

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

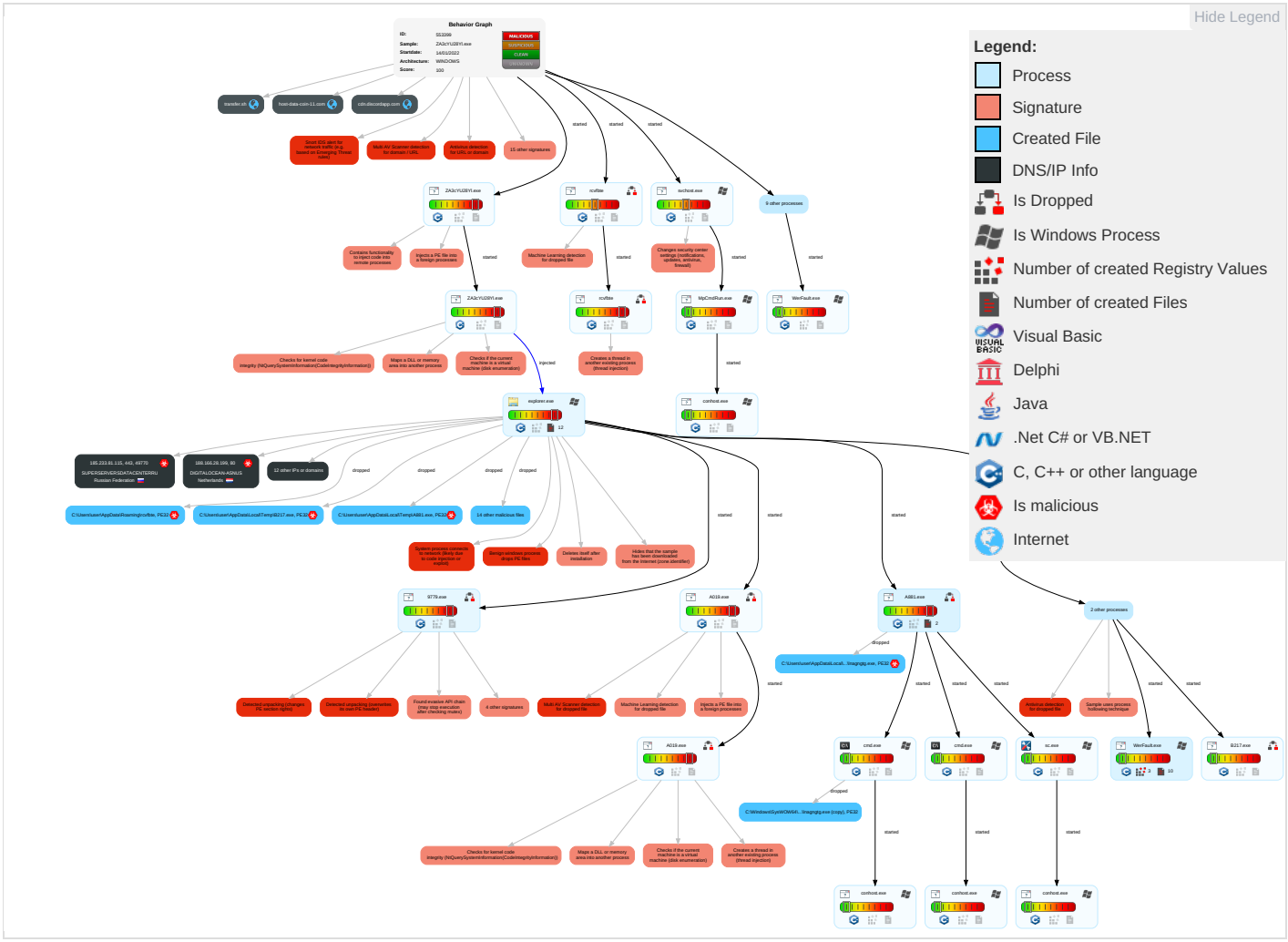
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	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	Ingress Transfe
Default Accounts	Native API 5 3 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	Shared Modules 1	Windows Service 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-St Port 1
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Windows Service 4	Software Packing 4 3	NTDS	System Information Discovery 2 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
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	Applica Layer Protoc
Replication Through Removable Media	Service Execution 3	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	Multiba Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
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 Pr
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 Protoc
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

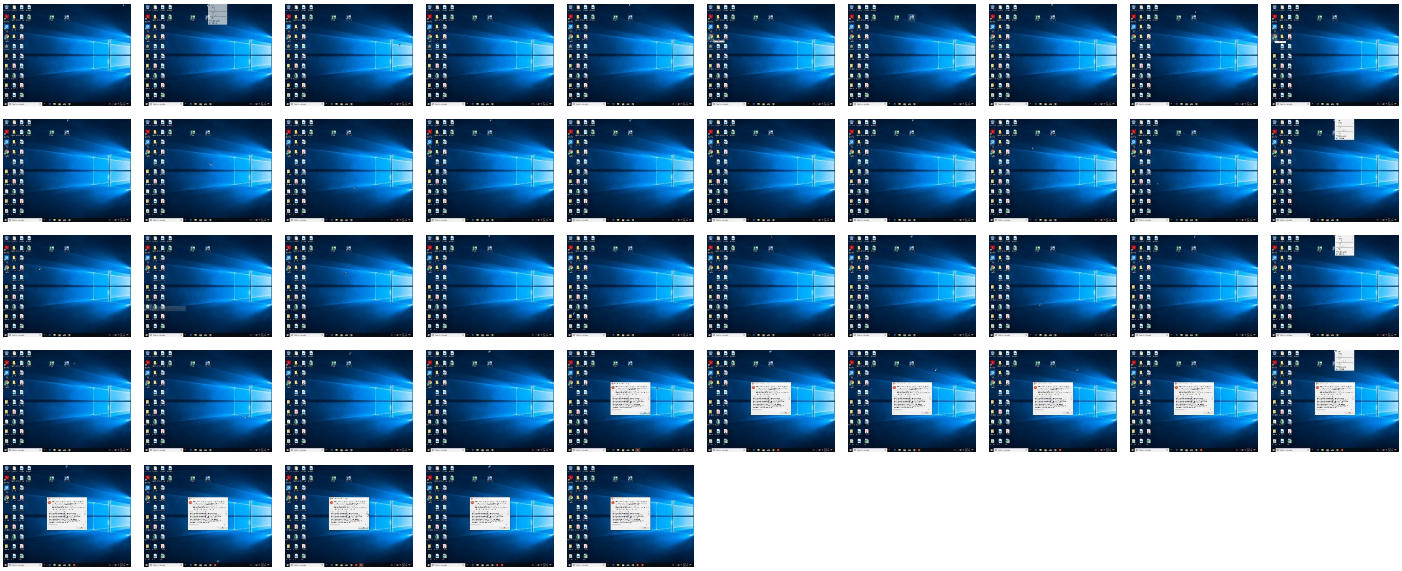
Behavior Graph



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
ZA3cYU28Yl.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\72B9.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\B217.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\2EE4.exe	100%	Avira	HEUR/AGEN.1212012	
C:\Users\user\AppData\Local\Temp\9779.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7F9A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A881.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8ECE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9460.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rcvfbte	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\293.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\41A3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3657.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\48E7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\969F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B217.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A019.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\lnagngtg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\50E7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\293.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\293.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\48E7.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\48E7.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\50E7.exe	50%	ReversingLabs	Win32.Infostealer.Generic	
C:\Users\user\AppData\Local\Temp\9460.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\9460.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\969F.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
C:\Users\user\AppData\Local\Temp\A019.exe	47%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.0.B217.exe.a90000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
3.0.ZA3cYU28Yl.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
15.0.rcvfbte.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.1.A019.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.A019.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.9460.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.A019.exe.6c15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.3.A881.exe.7f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.2.A881.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
22.2.9779.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.9460.exe.480e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.3.9779.exe.7f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
42.0.B217.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
15.0.rcvfbte.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.ZA3cYU28Yl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
15.0.rcvfbte.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.B217.exe.1b0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
15.1.rcvfbte.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.9460.exe.480e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.B217.exe.a90000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.2.A019.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.ZA3cYU28Yl.exe.5715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.A881.exe.6c0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.9460.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
42.0.B217.exe.1b0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
15.2.rcvfbte.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.ZA3cYU28Yl.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.9460.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.ZA3cYU28Yl.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.B217.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
3.2.ZA3cYU28Yl.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.ZA3cYU28Yl.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
3.0.ZA3cYU28Yl.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.3.9460.exe.5f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.A019.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.B217.exe.a90000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.2.rcvfbte.5f15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.B217.exe.1b0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.0.A019.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.ZA3cYU28Yl.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
27.2.B217.exe.a90000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
27.0.B217.exe.a90000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.2.9779.exe.7d0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.ZA3cYU28Yl.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.9460.exe.480e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://81.163.30.181/l2.exe	100%	Avira URL Cloud	malware	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	17%	Virustotal		Browse
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://74.201.28.62/book/KB5009812.png	0%	Avira URL Cloud	safe	
http://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://activity.windows.comr	0%	URL Reputation	safe	
http://74.201.28.62/book/KB5009812.exe	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://81.163.30.181/l3.exe	100%	Avira URL Cloud	malware	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	8.209.70.0	true	false		high
cdn.discordapp.com	162.159.129.233	true	false		high
privacy-tools-for-you-780.com	8.209.70.0	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://81.163.30.181/l2.exe	true	• Avira URL Cloud: malware	unknown
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://74.201.28.62/book/KB5009812.png	true	• Avira URL Cloud: safe	unknown
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	true	• Avira URL Cloud: malware	unknown
http://74.201.28.62/book/KB5009812.exe	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://81.163.30.181/l3.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
74.201.28.62	unknown	United States		35913	DEDIPATH-LLCUS	true
8.209.70.0	host-data-coin-11.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
104.21.38.221	goo.su	United States		13335	CLOUDFLARENETUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
81.163.30.181	unknown	Russian Federation		58303	IR-RASANAPISHTAZIR	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
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:	553399
Start date:	14.01.2022
Start time:	20:21:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZA3cYU28Yl.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:	44
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.spyw.evad.winEXE@47/28@87/12
EGA Information:	• Successful, ratio: 90%
HDC Information:	• Successful, ratio: 25.7% (good quality ratio 18%) • Quality average: 52.7% • Quality standard deviation: 40.1%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:22:59	Task Scheduler	Run new task: Firefox Default Browser Agent F2854DB1E573CD13 path: C:\Users\user\AppData\Roaming\rcv fbte
20:23:14	API Interceptor	1x Sleep call for process: 9779.exe modified
20:23:17	API Interceptor	7x Sleep call for process: svchost.exe modified
20:23:24	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
20:23:27	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_9460.exe_a795f71fcebe6b2e8adb61dbd3d258672ff4a7_b23f96db_139a0798\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):	0.813617660062026
Encrypted:	false
SSDEEP:	96:j4jgF/9bh+pmLiubWOQoJ7R3V6tpXIQcQec6tycEfcw3G+HbHg/8BRTf3o8Fa9iT:AgV9ZiuV8HQ0l7jIq/u7sGS274It7S
MD5:	A60CCEFB33BAB838A0842CE35C11B296
SHA1:	F9D2E8B7F00B0CCCC3628A83DD8BAB2CA02358B8
SHA-256:	985F759F3AC2C2682B9DA5D2DC3D5AEE1A5EA8595612DE30B49F43CD6D7AEE17
SHA-512:	12CFA5CA972022E82E47B97CFBBBD2D22BB9474C921FF2B0D4BCA5EE0D371D5E62F50A72A89F3F6F0192B47A9A42347AC44B3D6FAB4B64C3F7BEA616EDAD218A
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.9.4.1.9.5.0.7.4.3.4.7.1.....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.=.1.3.2.8.6.6.9.4.2.0.5.8.2.4.2.8.7.5.....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.=.6.0.a.e.5.6.e.7.-.8.e.e.b.-.4.e.f.7.-.8.4.b.5.-.f.c.b.4.e.6.8.2.d.a.f.a.....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.=.2.8.4.3.2.1.2.6.-.b.1.1.9.-.4.6.9.1.-.9.1.7.f.-.3.8.c.0.4.9.4.3.e.3.9.5.....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.=.9.4.6.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.d.0.-.0.0.0.1.-.0.0.1.c.-.4.9.4.9.-.1.2.9.7.c.7.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.0.7.2.6.a.4.5.5.3.5.8.c.8.2.d.c.a.e.5.6.7.a.f.4.f.3.5.6.6.a.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.!.9.4.6.0...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\WER61A4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jan 15 04:23:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	42152
Entropy (8bit):	2.001519542059326
Encrypted:	false
SSDEEP:	192:AqyPvcFZtwUnOeh0kA4pNOuh5pJN+pnv162COtEjU:DN/2eOcBfnQvHujU
MD5:	B7A83B68D7813C5F6EE4A8C08D3CABE0
SHA1:	5FD3BA4981C8B276FB5CA3003693E54BB27A42C5
SHA-256:	AACA056F1CFB12EFB8F3CAEC53ECF0F509FA017B166726784FD3FECE706811FF
SHA-512:	D6E974EE11C64540E0B3DC8314873E69A0E8FE7B34509150E148121E65B5CD02A5A0E1017A0D06AD7B2A36B7D34DC4646CF0D62673CE24EB7A98E16B3E0859E4
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....4L.a.....4...v(.....T.....8.....T.....x.....d.....U.....B.....GenuineIntelW.....T.....(L.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\WER6A11.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8392
Entropy (8bit):	3.700484672359636
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyl6h6YFjSUYZ64gmfIRSvCpDlb89bO0sfs9Oam:RrlsNiY6h6YhSUY7gmfIRSpOnfsq
MD5:	0B7724FCFB03841A321D2C0F6F53A7A5
SHA1:	ABF661A74D8E477B637D1C03A72B31017669DCA9
SHA-256:	3EE72172DB782E753D2497C4F209B933F976A916BAAFB3DB80813E9F04D91C8F
SHA-512:	9138CDFA618C891CA853EF8FA2577C4D0E4AED35F258CD938D5FA18663CEEF739A2C6C275DF5AE91FF9ECF87767CCD5B3DFBEB8D1954AE556992A2EF0773CE3
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A11.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E58.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):	4.475137069137135
Encrypted:	false
SSDEEP:	48:cvIwSD8zsYNJgtWI9CsWSC8B/8fm8M4JB8qFz+q8vZ8WGP+Md:uITfGJFSNGJtKjGP+Md
MD5:	A33297D249A4C58DD86EC3E200BFF672
SHA1:	E75531810FA3D1DD508D5C3B25E56E0C4C79B0D8
SHA-256:	CCAB04CB11A5EAD4FC23C03D8D54C6507DC04465D061871E4EEB773D877A7952
SHA-512:	82C9907345C2D0C3DCA0EE5A0651CB9141838468012386F2D17E61D5D7E64D6F4F98B42181B44F4BCACC0E02693C73A58084404C1E558581423EF2F94407D26C
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="1342893" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8697.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51890
Entropy (8bit):	3.0460149625790156
Encrypted:	false
SSDEEP:	1536:C/H4tWOnf0/Tb1/b+0l4Rydn5pbpF6Ftr6e2O9bB7d7cF:C/H4tWOnf0/Tb1/b+0l4Rydn51pF6FtK
MD5:	13395807C13FB08FB931641359AB795A
SHA1:	8AE0B8AE275A37A1C79B897A0DCF9A93AD4D502F
SHA-256:	0FC39CE42D88AABF23DDD4BC5FEF804DF4630C19540F1EF2D4CE5FF4F1300131
SHA-512:	2E0F41ADF15593D761D8754C5CE4C0B53BEEEAF7620FF39F37EF7B6A57FBF9DC8A08371405AD673FB7E9DE07849CA7807CDCA965BABA51986CE5D5104442C07F
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B7A.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6960283297412
Encrypted:	false
SSDEEP:	96:9GiZYWyxWpTYgYFWXGLH0YEZV5t2iFOxDAwlcZdgaoI7Ot2IfX3:9jZDnHJwckaoI7OtxfX3
MD5:	FDBF9CAA9D523FEEA1B571086287CD5E
SHA1:	4B8D9B60F59810A690638F7C31339B1C7F9581C4
SHA-256:	0573A32B634212500AD0FBD5423788CF7A3075F94B76045BF7861889639DB414
SHA-512:	9F32E558A86F8AC7C06E69A9A1701C1E66BE3B4BFA7AC5DDDF33A3DD9B993F8AF96028639FD70CF3146D27896867C9B9C4070D0AE68A693A1FF3DFA13C4A2DD
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B7A.tmp.txt	
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B217.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\B217.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:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55 D
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\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Vers ion=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Sy stem.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\293.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\2EE4.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7336391
Entropy (8bit):	**7.993025428513385**
Encrypted:	**true**
SSDEEP:	196608:76+hvICteEroXxqENE+sKsXXgvkz+AlnhMCRKsAN2aL:DInEroXjsKkXgsCMhkrNF
MD5:	CBE604877A46CEEBA112802BC17FFEF8
SHA1:	E85AB4CCBE491348C39F751162FFF71A90643ECA
SHA-256:	32703A3D88B3E9B8FE1A64FD1CBCC0925FC2C74BCBDEFBBD6944CBFAD0029FEC
SHA-512:	86F3946B813FB457D95B6635FA308DA1BF5F2C0FBD5BDCA75F7776D1A01A2D3C67A8A9E268DCC145FF575D70FBE84BE9BEB112A0D2269B955795C74468C005 8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\2EE4.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'X.8c9.kc9.kc9.kwR.jh9.kwR.jd9.kwR.j.9.k.V#kg9.k1L.jE9.k1L.jr9 .k1L.jj9.kwR.jh9.kc9.k.9.k.L.jp9.k.L.jb9.kRichc9.k.....PE..d...Q..a.....".....6...T.....@.....p...`.....[..x..... .....H... 9.....@9..8.....P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data.....p.....T.....@....pdata..... .....`.....@..@_RDATA.....~.....@..@.rsrc.....@..@.reloc..H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\3657.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	54272
Entropy (8bit):	4.125149292696976
Encrypted:	false
SSDEEP:	192:s7yxMfjf6NrLqKZ6mXS9LzL1pvULIRPqY2F3991ZuBhyY8PGCz9QwAOSZCGQyBbf:KyufjSLq86mXS9LzLdqY2LHZ4cZA
MD5:	1B1E4286625BB189A526E910F2031C7B
SHA1:	650C0550F12C65D9841D10AB589FF39261018957
SHA-256:	C9D7CB68DEC80469C3C03B0E90C7AF1972462CA7779424DB3BFD9D44AEBAA624
SHA-512:	68F2366606B658FDDB2B5E9BAE2E6931FB455A230F8A4813EACB38A3D7853B9640F46FE9EE6FFD9862A509558B66C30A3494CB7231C3EF7CD784950771273155
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....vL....."...0.....5... ...@....@.. ....@.....4..O....@..\.....4..... ....H.....text..... ....`.rsrc...\....@.....@..@.rel oc.....@..B.....4.....H.....#..`.....3.....0.:.....(.....(....(.....s.....o.....(.....(....(.....+..*".(....*..0..... ...(....r...p.....%.." ...(.....(.....%. N..."....o....&. ....(.....&.....&...(....r...pr5..pr9..p(.....%..'...(.....(....s.....%.r;..p.o....t.....+..*.....B..Q.....0..7.....(.....,....i(.....(....o....&s .....(... .o!...o"....s#.....o$.....+...(%.....o&...o'.....((..

C:\Users\user\AppData\Local\Temp\41A3.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\48E7.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\48E7.exe

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\50E7.exe

Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	557664
Entropy (8bit):	7.687250283474463
Encrypted:	false
SSDEEP:	12288:fWxcQhhhhhn8bieAtJlllLtrHWnjkQrK8iBHZkshvesxViA9Og+:fWZhhhhhUATlLtrUbK8oZphveoMA9
MD5:	6ADB5470086099B9169109333FADAB86
SHA1:	87EB7A01E9E54E0A308F8D5EDFD3AF6EBA4DC619
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3ED CD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$..*..... ...`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...'',..

C:\Users\user\AppData\Local\Temp\72B9.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7336385
Entropy (8bit):	**7.993036026488077**
Encrypted:	**true**
SSDEEP:	196608:l++hvICteEroXxqENE+sKsXXgvkwuUxNhMC/CKN7kL:BInEroXjsKkXgs/EhWKNY
MD5:	AE6510D9815C44A818F722ECAE6844B8
SHA1:	2A34B5110F5C3C2424AE9685F57261E2546BD963
SHA-256:	C3CAD582268B165711E2F2B1834891C7BCB5E57A7EFB1E709E3DF19D011AD656
SHA-512:	8CAA9E661403D5D86F69E7C35E45CDF927EF9EC0C6045ED2CA5AF2EAAF26B4F99291EADAF2F0C8C00A31B05B228C6DF0C4BD205A7B3EC70E263313A08FFEF 4F8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'X.8c9.kc9.kc9.kwR.jh9.kwR.jd9.kwR.j.9.k.V#kg9.k1L.jE9.k1L.jr9 .k1L.jj9.kwR.jh9.kc9.k.9.k.L.jp9.k.L.jb9.kRichc9.k.....PE..d.....a....."....6...T.....@.....%.p..`.....[..x..... .....H... 9.....@9..8.....P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data.....p.....T.....@....pdata..... .....`.....@..@_RDATA.....~.....@..@.rsrc.....@..@.reloc..H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\7F9A.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3596288
Entropy (8bit):	**7.997492170986202**
Encrypted:	**true**
SSDEEP:	49152:x+8QEA1GN2zhieKqcTe0f3nWNHiZWf5dxQNPY7wUE9E8gnH43lvn/3juAVUk3Imp:xZ3KKqcTMNIWBnYAlRo7uOUk3ll4UMS
MD5:	8897C1354CB525DE5F4DE514D6FE836D
SHA1:	2F92D4CCA4D7576603A442BBACB87450F41CFE6E
SHA-256:	407C68405D373D2C8EF66B004B293BE25D571348E8922D02D7B79EB20A5138DB
SHA-512:	A46C6F7BAF298C34607701353E136120153521326A77C787F62F8BF439BB7DEC188A757271B4C8E47E650E86272159FD5D072A1530195D60900FEB8C481F671D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\7F9A.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....6. .....|.N. ....0M..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....?....P.....@.....1..p.....@....rsrc.....0M.....0.....@....2pZFPAB.....N.....02..... ..@....adata.....S.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\8ECE.exe

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

C:\Users\user\AppData\Local\Temp\9460.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\969F.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.021094695416705
Encrypted:	false
SSDEEP:	384:1P27QR0ir3uqVQ1Tf+1rkZlgEdLcHIH+2f9sFIILCbj4KQWylH28iYfx:1PYQR0i4krj58LIL0zy2
MD5:	9DA91D9E3AD909FB8EBA4D3D74344982
SHA1:	D5B6872D062043478CBA1002A815A013952D3837
SHA-256:	0417281135837E3CCC11F35B2D17A6A3672B011E85C18884F54F6FEABA7B8069
SHA-512:	29D672F0BB8AEE885F008F7B7EBED499E7C5D8738B9373BF169896BE85C271FAAB5BD9792C176C7CDCB1C39606F07041E1E54E8F893D1D91F49509DF927AA8A 0
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\969F.exe	
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\969F.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!.....0..J.....rh... .....@.. .....1... .@..... h..O.....Tg..8..... ....H.....text....H... ...J..... ..`.rsrc.....L.....@..@.relo c.....N.....@..B.....Th.....H.....C..."....e..p.....^..}.....(.....(....*..*..0.....(...%.-...(....s.....s..... ....o..... ....o.....(....r...p o..... ....s.....o.....[o....o.....o ....[o....o!.....o"....o#....s$.....io%.....o&.....,..o'.....o(.....,.o'.....,.o'.....+...*..(.....".....0.....o).....(*.....s +....+..*...0.....s,.... ....(-.....(.....r%..po/.

C:\Users\user\AppData\Local\Temp\9779.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	324608
Entropy (8bit):	6.705560699768563
Encrypted:	false
SSDEEP:	6144:8cXfhxLWOCPRZa9XQ9XuxYADj5QTM44lq46Ue:8cXfhxKPZyK+x3NQN4l3Je
MD5:	043B44289E31BD54357F9A5C21833259
SHA1:	C042C1D364887BBF71B070C8DD6C66C08A818834
SHA-256:	8DC59F6481C6FE183ADAC2B720FFA276CC9F52D83521200B1A85BB5FF8E4046A
SHA-512:	AC7098ED6CC6922577D0C87F4E3BA6EF32973C1641C98B3C675EFBBC548A63346DE87A0026ADB850144B120604BB7B9982A69E1AA2859D0E0A3A0CCE0857375
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...o.}`.....P.....@.....[.....t...P.....(.....@..... .....L.....text..... ..`.data.....@....zic.....@....wuvuhus.....@....jufot.....@....rsrc... (.....$.....@..@.reloc..dF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\A019.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.6829606926024825
Encrypted:	false
SSDEEP:	6144:+/jCnwGXFliTnwC2aJLQt55gPnHswDcEgoJgnyyB:+/jZR2GK7g/swdgoiF
MD5:	679831CF1F00950B4ADFFBBBA7E6AB46
SHA1:	F4AA59829222D5ED000849EA0167082F54B59E03
SHA-256:	760D44EA1A90C1B235133258A8F03BED049B5B51328AEFE4A2595B6F085DD99D
SHA-512:	5D88BC6FA746628F9EB792612B857D7724DA4827445EDF2A7850190358A3C9C08CAA602DF2CC92EBA96571D4C34A0E311007C8688FA437203F8EEC3185C2ED8
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....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L.....`.....@.....i.....P.....(.....@..... .....L.....text...n..... ..`.data.....@....wumened.....@....kilohe.....@....putohox.....@ ....rsrc...(.....@..@.reloc..ZF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\A881.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	321024
Entropy (8bit):	6.689067457982047
Encrypted:	false
SSDEEP:	6144:XxPbeuhFMQH+prd0WRRa/CMjXOfo68JRD0QsGrnysp:XPTWRRZM+fuJR5sG
MD5:	9AF71C74219794F100EA801B528339AF
SHA1:	DDE2BB10F1E77E03CF9190467DB85E515D720012
SHA-256:	84AEC628E2903022FBC5737746812D983B65A1D1EFD1110FF7D15BA49D6D15B0

C:\Users\user\AppData\Local\Temp\A881.exe	
SHA-512:	602ACA3D539FF09F384B35FA8C2B8521F20113362E33657FCB645D3171A402DBADFF7F4E564D57B34B896CBB55E55718CFC947F61CABAD1C9058E624B9B9E6B B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...i.`.....@.....s.....P.....(.....@..... ....L.....text..... ..`.data.....@....mekafe.....@....tuxu.....@....hawoz.....@. ...rsrc...(.....@..@.reloc..ZF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\B217.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\lnagngtg.exe	
Process:	C:\Users\user\AppData\Local\Temp\A881.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11619840
Entropy (8bit):	3.8195691800841227
Encrypted:	false
SSDEEP:	6144:rxPbeuhFMQH+prd0WRRa/CMjXOfo68JRD0QsGrnyspaaaaaaaaaaaaaaaaaaaaaH:rPTWRRZM+fuJR5sG
MD5:	673D618D671523049906C3308A9AAD4F
SHA1:	D0ED8C79559CE9000A8196E62B127E40A8C61CB7
SHA-256:	5D2E5FFDA32AC3FEEA1526B4F05363B6F1994F18C1F27993FED00ACD4FCF7C88
SHA-512:	57622653554190523F7BFC4C127B33974335D3C8B98C041940545B9AEF53C69555D7E858542FCA08441EF6350B9D2E5926C97C70623783C8848DE0789FE65DE8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...i.`.....@.....s.....P.....(.....@..... ....L.....text..... ..`.data.....@....mekafe.....@....tuxu.....@....hawoz.....@. ...rsrc...(.....@..@.reloc..ZF.....@..B.....

C:\Users\user\AppData\Roaming\rcvfbte	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.6829606926024825
Encrypted:	false
SSDEEP:	6144:+/jCnwGXFliTnwC2aJLQt55gPnHswDcEgoJgnyyB:+/jZR2GK7g/swdgoiF
MD5:	679831CF1F00950B4ADFFBBBA7E6AB46
SHA1:	F4AA59829222D5ED000849EA0167082F54B59E03
SHA-256:	760D44EA1A90C1B235133258A8F03BED049B5B51328AEFE4A2595B6F085DD99D
SHA-512:	5D88BC6FA746628F9EB792612B857D7724DA4827445EDF2A7850190358A3C9C08CAA602DF2CC92EBA96571D4C34A0E311007C8688FA437203F8EEC3185C2ED8

C:\Users\user\AppData\Roaming\rcvfbte	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.........PE..L......`..........................................@..................................i..........................................P.......(...............................................................@.......... .....L...........................text...n.......................... ..`.data..............................@....wumened...........................@....kilohe............................@....putohox...........................@ ....rsrc...(..........................@..@.reloc..ZF.......H.................@..B.. ....

C:\Users\user\AppData\Roaming\rcvfbte:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\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):	3.1625951749021364
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z2+h:j+s+v+b+P+m+0+Q+q+9+h
MD5:	44A7B0493CF5DB2EA4B3AA98E369F59D
SHA1:	60322A1984D18CEB3F7105F9086584FFAEEDBBC5
SHA-256:	4248B10ADC263B0A71E1458C5A950B9387DFD5124DD8B91928684262E1DABF11
SHA-512:	7081E092B955DEEA6B1BCF1504EF3812A1ABF0A33BF13F33B8BBBA8ACF22941288A7BA0A9CF5F6E50BFFE52CDF60670A9DB3AC5E18E87BFA296367E8EAF4F D1A
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.20220115_042221_285.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.318412811253484
Encrypted:	false
SSDEEP:	96:jC/C42o+WK5Su912YnmC0vI2lXSk4P4mlT2WYFzqUMCv6JRW:2YtkyX2YvnCAw
MD5:	EFF2FE31D906DBDDEC1625C346AC4F99
SHA1:	C265CAF999BC43A36D61FB235CDFE77C1AB4916D
SHA-256:	2EB779DDF0FD27ED793FBA33F606DDDEA5CAC283DA2810E3932B43E6F3347DFB
SHA-512:	897D7F6E59C9041C5DB3FC1975382F61B4465CBD6BEA91198238EF0BDEC2064794F2C7BBD77725F75E38E1504617227262CAFF5186AD96E1384F7EC2E583730E
Malicious:	false
Reputation:	unknown
Preview:	....!...B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1... ......PR}............8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.:.\.W.i.n. d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o.s.v.c... 2.0.2.2.0.1.1.5._.0.4.2.2.2.1._.2.8.5...e.t.l.........P.P.. ....

C:\Windows\SysWOW64\gebcmxiz\lnagngtg.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11619840
Entropy (8bit):	3.8195691800841227
Encrypted:	false
SSDEEP:	6144:rxPbeuhFMQH+prd0WRRa/CMjXOfo68JRD0QsGrnyspaaaaaaaaaaaaaaaaaaaaaH:rPTWRRZM+fuJR5sG
MD5:	673D618D671523049906C3308A9AAD4F
SHA1:	D0ED8C79559CE9000A8196E62B127E40A8C61CB7
SHA-256:	5D2E5FFDA32AC3FEEA1526B4F05363B6F1994F18C1F27993FED00ACD4FCF7C88
SHA-512:	57622653554190523F7BFC4C127B33974335D3C8B98C041940545B9AEF53C69555D7E858542FCA08441EF6350B9D2E5926C97C70623783C8848DE0789FE65DE8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...i.`.....@.....s.....P.....(.....@..... ....L.....text..... ..`.data.....@....mekafe.....@....tuxu.....@....hawoz.....@. ...rsrc...(.....@..@.reloc..ZF.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.6829606926024825
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:	ZA3cYU28YI.exe
File size:	320000
MD5:	679831cf1f00950b4adffbbba7e6ab46
SHA1:	f4aa59829222d5ed000849ea0167082f54b59e03
SHA256:	760d44ea1a90c1b235133258a8f03bed049b5b51328aefe 4a2595b6f085dd99d
SHA512:	5d88bc6fa746628f9eb792612b857d7724da4827445edf2 a7850190358a3c9c08caa602df2cc92eba96571d4c34a0 e311007c8688fa437203f8eec3185c2ed8f
SSDEEP:	6144:+/jCnwGXFliTnwC2aJLQt55gPnHswDcEgoJgnyy B:+/jZR2GK7g/swdgoiF
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....m.9.)~W .)~W.)~W.7,..3~W.7,...~W...,..~W.)~V..~W.7,...~W.7,..(~ W.7,..(~W.Rich)~W.....PE..L.....`.....

File Icon

Icon Hash:	c8d0d8e0f0e0f4e0

Static PE Info

General

Entrypoint:	0x41b290
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x602EA3B5 [Thu Feb 18 17:28:21 2021 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6801e04a0c2ca60ac2497c0d8723846b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e36e	0x3e400	False	0.581129204317	data	6.95926809019	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.3408203125	data	3.46519187176	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.wumened	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.kilohe	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.putohox	0x14f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x8728	0x8800	False	0.595042509191	data	5.83826747573	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x465a	0x4800	False	0.344672309028	data	3.68878313517	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 20:22:59.593086958 CET	192.168.2.3	8.8.8.8	0xdb2a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:00.090055943 CET	192.168.2.3	8.8.8.8	0xb64c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:00.553119898 CET	192.168.2.3	8.8.8.8	0xd5c3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:00.720731974 CET	192.168.2.3	8.8.8.8	0x5141	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:01.224791050 CET	192.168.2.3	8.8.8.8	0xe843	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:01.448460102 CET	192.168.2.3	8.8.8.8	0x2ea4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:03.074909925 CET	192.168.2.3	8.8.8.8	0x97a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:03.562218904 CET	192.168.2.3	8.8.8.8	0x3215	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:04.002065897 CET	192.168.2.3	8.8.8.8	0x1642	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:05.775187969 CET	192.168.2.3	8.8.8.8	0xc79c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:05.961374998 CET	192.168.2.3	8.8.8.8	0xfb5a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:06.147183895 CET	192.168.2.3	8.8.8.8	0x1527	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:06.739689112 CET	192.168.2.3	8.8.8.8	0x5108	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:06.903386116 CET	192.168.2.3	8.8.8.8	0xc95b	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:08.851147890 CET	192.168.2.3	8.8.8.8	0x908b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.027312994 CET	192.168.2.3	8.8.8.8	0x2c44	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.206108093 CET	192.168.2.3	8.8.8.8	0x7051	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.277249098 CET	192.168.2.3	8.8.8.8	0xac5c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.484148026 CET	192.168.2.3	8.8.8.8	0xe140	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:10.085179090 CET	192.168.2.3	8.8.8.8	0x9e93	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:10.289695978 CET	192.168.2.3	8.8.8.8	0xbfa0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:10.465589046 CET	192.168.2.3	8.8.8.8	0xc084	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:13.875395060 CET	192.168.2.3	8.8.8.8	0x4e00	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:14.052778006 CET	192.168.2.3	8.8.8.8	0x5d57	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:14.231143951 CET	192.168.2.3	8.8.8.8	0x2c7d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:14.428993940 CET	192.168.2.3	8.8.8.8	0xda0e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.116410971 CET	192.168.2.3	8.8.8.8	0xe276	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.282830954 CET	192.168.2.3	8.8.8.8	0x1741	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.730241060 CET	192.168.2.3	8.8.8.8	0x1230	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.898772955 CET	192.168.2.3	8.8.8.8	0xdf88	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:19.761039019 CET	192.168.2.3	8.8.8.8	0xfd1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:19.934057951 CET	192.168.2.3	8.8.8.8	0x62c5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:20.122881889 CET	192.168.2.3	8.8.8.8	0xb96f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:41.619885921 CET	192.168.2.3	8.8.8.8	0x77df	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 20:23:41.816992044 CET	192.168.2.3	8.8.8.8	0x2e1a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:41.993643999 CET	192.168.2.3	8.8.8.8	0xc72f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.160722971 CET	192.168.2.3	8.8.8.8	0x2d01	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.342725039 CET	192.168.2.3	8.8.8.8	0xb2c1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.516983986 CET	192.168.2.3	8.8.8.8	0x4563	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.683554888 CET	192.168.2.3	8.8.8.8	0xff7a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.872464895 CET	192.168.2.3	8.8.8.8	0xefc8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.068180084 CET	192.168.2.3	8.8.8.8	0x8ed9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.260879040 CET	192.168.2.3	8.8.8.8	0x12b6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.448460102 CET	192.168.2.3	8.8.8.8	0xcee	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.622994900 CET	192.168.2.3	8.8.8.8	0x53c2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.790278912 CET	192.168.2.3	8.8.8.8	0xb3a0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.991139889 CET	192.168.2.3	8.8.8.8	0x20de	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:45.729631901 CET	192.168.2.3	8.8.8.8	0x8df9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:45.928921938 CET	192.168.2.3	8.8.8.8	0x4292	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:46.106477022 CET	192.168.2.3	8.8.8.8	0x7729	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:46.783490896 CET	192.168.2.3	8.8.8.8	0xcc15	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:46.994508028 CET	192.168.2.3	8.8.8.8	0xd21d	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:47.961041927 CET	192.168.2.3	8.8.8.8	0x59e0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.111679077 CET	192.168.2.3	8.8.8.8	0xbdcf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.293678999 CET	192.168.2.3	8.8.8.8	0x6782	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.463077068 CET	192.168.2.3	8.8.8.8	0x55b3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.634524107 CET	192.168.2.3	8.8.8.8	0x603d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:57.143260956 CET	192.168.2.3	8.8.8.8	0x29e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:57.313873053 CET	192.168.2.3	8.8.8.8	0x512a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:58.725483894 CET	192.168.2.3	8.8.8.8	0xe13b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:58.901207924 CET	192.168.2.3	8.8.8.8	0x1574	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:59.081888914 CET	192.168.2.3	8.8.8.8	0x8015	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:59.302086115 CET	192.168.2.3	8.8.8.8	0xbb59	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:01.871258974 CET	192.168.2.3	8.8.8.8	0xf250	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:02.044727087 CET	192.168.2.3	8.8.8.8	0x69ff	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:02.216252089 CET	192.168.2.3	8.8.8.8	0xd2dd	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:03.665247917 CET	192.168.2.3	8.8.8.8	0x50d1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:04.127317905 CET	192.168.2.3	8.8.8.8	0xc30f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:04.312788963 CET	192.168.2.3	8.8.8.8	0xe4e8	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:06.022989988 CET	192.168.2.3	8.8.8.8	0x71d6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:06.312561035 CET	192.168.2.3	8.8.8.8	0x4ae7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 20:24:14.684118032 CET	192.168.2.3	8.8.8.8	0x4fd3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:14.937835932 CET	192.168.2.3	8.8.8.8	0x8837	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:15.105503082 CET	192.168.2.3	8.8.8.8	0x3864	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:17.843784094 CET	192.168.2.3	8.8.8.8	0x91d5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.013364077 CET	192.168.2.3	8.8.8.8	0x872f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.182811975 CET	192.168.2.3	8.8.8.8	0xb763	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.355863094 CET	192.168.2.3	8.8.8.8	0xb072	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.527890921 CET	192.168.2.3	8.8.8.8	0x634a	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:21.727242947 CET	192.168.2.3	8.8.8.8	0xb1d4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:21.889111042 CET	192.168.2.3	8.8.8.8	0x293a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:22.071381092 CET	192.168.2.3	8.8.8.8	0x6ba6	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:24.095540047 CET	192.168.2.3	8.8.8.8	0xac86	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:25.046252012 CET	192.168.2.3	8.8.8.8	0x2983	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:25.351382017 CET	192.168.2.3	8.8.8.8	0xe2ab	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:31.004300117 CET	192.168.2.3	8.8.8.8	0xf809	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:36.338799953 CET	192.168.2.3	8.8.8.8	0xe4e6	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:22:59.911616087 CET	8.8.8.8	192.168.2.3	0xdb2a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:00.403337955 CET	8.8.8.8	192.168.2.3	0xb64c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:00.572498083 CET	8.8.8.8	192.168.2.3	0xd5c3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:01.048615932 CET	8.8.8.8	192.168.2.3	0x5141	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:01.244103909 CET	8.8.8.8	192.168.2.3	0xe843	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:01.748825073 CET	8.8.8.8	192.168.2.3	0x2ea4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:03.391123056 CET	8.8.8.8	192.168.2.3	0x97a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:03.856426954 CET	8.8.8.8	192.168.2.3	0x3215	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:04.293950081 CET	8.8.8.8	192.168.2.3	0x1642	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:05.792773008 CET	8.8.8.8	192.168.2.3	0xc79c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:05.980930090 CET	8.8.8.8	192.168.2.3	0xfb5a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:06.433780909 CET	8.8.8.8	192.168.2.3	0x1527	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:06.758944035 CET	8.8.8.8	192.168.2.3	0x5108	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:23:07.238167048 CET	8.8.8.8	192.168.2.3	0xc95b	No error (0)	privacy-tools-for-you-780.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:08.870402098 CET	8.8.8.8	192.168.2.3	0x908b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.045989990 CET	8.8.8.8	192.168.2.3	0x2c44	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.228575945 CET	8.8.8.8	192.168.2.3	0x7051	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.296737909 CET	8.8.8.8	192.168.2.3	0xac5c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:09.503681898 CET	8.8.8.8	192.168.2.3	0xe140	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:10.105284929 CET	8.8.8.8	192.168.2.3	0x9e93	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:10.308665991 CET	8.8.8.8	192.168.2.3	0xbfa0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:10.785981894 CET	8.8.8.8	192.168.2.3	0xc084	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:13.894783020 CET	8.8.8.8	192.168.2.3	0x4e00	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:14.072632074 CET	8.8.8.8	192.168.2.3	0x5d57	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:14.249980927 CET	8.8.8.8	192.168.2.3	0x2c7d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:14.448292971 CET	8.8.8.8	192.168.2.3	0xda0e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.133790970 CET	8.8.8.8	192.168.2.3	0xe276	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.569967985 CET	8.8.8.8	192.168.2.3	0x1741	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.747776031 CET	8.8.8.8	192.168.2.3	0x1230	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.920452118 CET	8.8.8.8	192.168.2.3	0xdf88	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.920452118 CET	8.8.8.8	192.168.2.3	0xdf88	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.920452118 CET	8.8.8.8	192.168.2.3	0xdf88	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.920452118 CET	8.8.8.8	192.168.2.3	0xdf88	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:17.920452118 CET	8.8.8.8	192.168.2.3	0xdf88	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:19.778841972 CET	8.8.8.8	192.168.2.3	0xfd1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:19.951246977 CET	8.8.8.8	192.168.2.3	0x62c5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:20.142239094 CET	8.8.8.8	192.168.2.3	0xb96f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:41.639306068 CET	8.8.8.8	192.168.2.3	0x77df	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:41.836302996 CET	8.8.8.8	192.168.2.3	0x2e1a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:23:42.013575077 CET	8.8.8.8	192.168.2.3	0xc72f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.180665016 CET	8.8.8.8	192.168.2.3	0x2d01	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.362310886 CET	8.8.8.8	192.168.2.3	0xb2c1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.536467075 CET	8.8.8.8	192.168.2.3	0x4563	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.703030109 CET	8.8.8.8	192.168.2.3	0xff7a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:42.891748905 CET	8.8.8.8	192.168.2.3	0xefc8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.085407019 CET	8.8.8.8	192.168.2.3	0x8ed9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.280286074 CET	8.8.8.8	192.168.2.3	0x12b6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.467264891 CET	8.8.8.8	192.168.2.3	0xcee	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.642393112 CET	8.8.8.8	192.168.2.3	0x53c2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:43.809518099 CET	8.8.8.8	192.168.2.3	0xb3a0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:44.295824051 CET	8.8.8.8	192.168.2.3	0x20de	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:45.748609066 CET	8.8.8.8	192.168.2.3	0x8df9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:45.948498964 CET	8.8.8.8	192.168.2.3	0x4292	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:46.127774000 CET	8.8.8.8	192.168.2.3	0x7729	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:46.127774000 CET	8.8.8.8	192.168.2.3	0x7729	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:46.803097963 CET	8.8.8.8	192.168.2.3	0xcc15	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:47.014014006 CET	8.8.8.8	192.168.2.3	0xd21d	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:47.980468988 CET	8.8.8.8	192.168.2.3	0x59e0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.133007050 CET	8.8.8.8	192.168.2.3	0xbdcf	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.313539028 CET	8.8.8.8	192.168.2.3	0x6782	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.482646942 CET	8.8.8.8	192.168.2.3	0x55b3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:49.654067993 CET	8.8.8.8	192.168.2.3	0x603d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:57.160844088 CET	8.8.8.8	192.168.2.3	0x29e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:57.332928896 CET	8.8.8.8	192.168.2.3	0x512a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:58.744246006 CET	8.8.8.8	192.168.2.3	0xe13b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:23:58.920618057 CET	8.8.8.8	192.168.2.3	0x1574	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:59.098858118 CET	8.8.8.8	192.168.2.3	0x8015	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:23:59.322348118 CET	8.8.8.8	192.168.2.3	0xbb59	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:01.890768051 CET	8.8.8.8	192.168.2.3	0xf250	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:02.064228058 CET	8.8.8.8	192.168.2.3	0x69ff	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:02.234983921 CET	8.8.8.8	192.168.2.3	0xd2dd	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:03.976593971 CET	8.8.8.8	192.168.2.3	0x50d1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:04.148250103 CET	8.8.8.8	192.168.2.3	0xc30f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:04.332371950 CET	8.8.8.8	192.168.2.3	0xe4e8	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:06.042289019 CET	8.8.8.8	192.168.2.3	0x71d6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:06.331660986 CET	8.8.8.8	192.168.2.3	0x4ae7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:14.704119921 CET	8.8.8.8	192.168.2.3	0x4fd3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:14.957201004 CET	8.8.8.8	192.168.2.3	0x8837	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:15.122947931 CET	8.8.8.8	192.168.2.3	0x3864	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:17.861490965 CET	8.8.8.8	192.168.2.3	0x91d5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.030811071 CET	8.8.8.8	192.168.2.3	0x872f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.202325106 CET	8.8.8.8	192.168.2.3	0xb763	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.373193026 CET	8.8.8.8	192.168.2.3	0xb072	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:18.547805071 CET	8.8.8.8	192.168.2.3	0x634a	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:21.744167089 CET	8.8.8.8	192.168.2.3	0xb1d4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:21.906145096 CET	8.8.8.8	192.168.2.3	0x293a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:22.090316057 CET	8.8.8.8	192.168.2.3	0x6ba6	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:24.114954948 CET	8.8.8.8	192.168.2.3	0xac86	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:25.066088915 CET	8.8.8.8	192.168.2.3	0x2983	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:25.371095896 CET	8.8.8.8	192.168.2.3	0xe2ab	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:31.025305033 CET	8.8.8.8	192.168.2.3	0xf809	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 20:24:31.025305033 CET	8.8.8.8	192.168.2.3	0xf809	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:31.025305033 CET	8.8.8.8	192.168.2.3	0xf809	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:31.025305033 CET	8.8.8.8	192.168.2.3	0xf809	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:31.025305033 CET	8.8.8.8	192.168.2.3	0xf809	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 20:24:36.358298063 CET	8.8.8.8	192.168.2.3	0xe4e6	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cosjvii.net
  - host-data-coin-11.com
- efywdpqsv.com
- vucofkhoh.org
- glphw.com
- oyaibbgc.net
- nkvfp.net
- ojffxid.net
- qctnjb.net
- data-host-coin-8.com
- vjrurwpaf.net
- cadsuqagh.net
- meblvhu.com
- nyxemdoi.net
- privacy-tools-for-you-780.com
- syoeagb.org
- xlertqbun.net
- unicupload.top
- blagu.org
- kkmdou.net
- qbjnsl.com
- ornpwmrp.net
- rlhvsc.org

- rtrryuils.com
- scgsgbtih.com
- akyloc.org
- 185.7.214.171:8080
- ahoawm.net
- pmfhwtjj.com
- lfyjw.org
- sipqy.org
- jnlltxxq.com
- mdbgmr.net
- vxwgswks.com
- ksfdeabujk.com
- bsgftsru.com
- hfmcm.net
- hiwcjtiwj.org
- tmqcl.net
- opsdg.org
- fdqepw.org
- qbbvlw.net
- giykrj.com
- dnoukoye.com
- fpoovg.net
- inyhvk.org
- oabgm.com
- iaimu.net
- mwapt.com
- lmtsfedit.net
- cvdnubldkb.net
- crxfds.net
- yuhcl.com

- owybkq.org
- 81.163.30.181
- ddkkslyotn.com
- qsbkvqwnoj.com
- 74.201.28.62
- wmqdweotts.net
- vbcrt.com
- yldgixbqm.org
- wlqxaynuuq.org
- qochog.com
- drvwc.net
- tsgnkffj.org
- ylqihxvnug.org
- tvrhmio.org
- oeaexcj.net
- fcifwg.net
- rffngorjcd.com
- bfwxl.net
- takmxbc.com
- ftcxosy.com
- bhlwowqbr.org
- ykguadbgli.com
- ircqiowi.com
- hnvpcgnd.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ZA3cYU28Yl.exe PID: 6600 Parent PID: 5844

General

Start time:	20:22:18
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\ZA3cYU28Yl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ZA3cYU28Yl.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	679831CF1F00950B4ADFFBBBA7E6AB46
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ZA3cYU28Yl.exe PID: 6620 Parent PID: 6600

General

Start time:	20:22:19
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\ZA3cYU28Yl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ZA3cYU28Yl.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	679831CF1F00950B4ADFFBBBA7E6AB46
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: 00000003.00000002.333262137.00000000005B1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.333204148.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 5672 Parent PID: 572

General

Start time:	20:22:20
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: 6112 Parent PID: 572

General

Start time:	20:22:20
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: 5024 Parent PID: 572

General

Start time:	20:22:21
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: 6376 Parent PID: 572

General

Start time:	20:22:22
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff657f80000
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: 3676 Parent PID: 572

General

Start time:	20:22:22
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: svchost.exe PID: 6812 Parent PID: 572

General

Start time:	20:22:22
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: explorer.exe PID: 3352 Parent PID: 6620

General

Start time:	20:22:26
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: 0000000A.00000000.327467083.0000000005AC1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 7100 Parent PID: 572

General

Start time:	20:22:44
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: 4520 Parent PID: 572

General

Start time:	20:22:58
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: rcvfbte PID: 1308 Parent PID: 664

General

Start time:	20:22:59
Start date:	14/01/2022

Path:	C:\Users\user\AppData\Roaming\rcvfbte
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rcvfbte
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	679831CF1F00950B4ADFFBBBA7E6AB46
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: rcvfbte PID: 5888 Parent PID: 1308

General

Start time:	20:23:01
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\rcvfbte
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rcvfbte
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	679831CF1F00950B4ADFFBBBA7E6AB46
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: 0000000F.00000002.385289105.0000000000530000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000F.00000002.385864770.0000000002441000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 9460.exe PID: 6608 Parent PID: 3352

General

Start time:	20:23:04
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\9460.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\9460.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
Reputation:	moderate

Analysis Process: A019.exe PID: 3340 Parent PID: 3352

General

Start time:	20:23:07

Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\A019.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A019.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	679831CF1F00950B4ADFFBBBA7E6AB46
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: svchost.exe PID: 1324 Parent PID: 572

General

Start time:	20:23:07
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
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

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6868 Parent PID: 1324

General

Start time:	20:23:08
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6608 -ip 6608
Imagebase:	0x7ff70d6e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: A019.exe PID: 5000 Parent PID: 3340

General

Start time:	20:23:09
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\A019.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A019.exe

Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	679831CF1F00950B4ADFFBBBA7E6AB46
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: 00000014.00000002.407171768.00000000005C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000014.00000002.407257194.00000000005E1000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 4820 Parent PID: 6608

General

Start time:	20:23:10
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6608 -s 520
Imagebase:	0xdd0000
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: 9779.exe PID: 2228 Parent PID: 3352

General

Start time:	20:23:12
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\9779.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\9779.exe
Imagebase:	0x400000
File size:	324608 bytes
MD5 hash:	043B44289E31BD54357F9A5C21833259
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: 00000016.00000002.398828451.0000000000899000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000016.00000002.398828451.0000000000899000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: svchost.exe PID: 4580 Parent PID: 572

General

Start time:	20:23:14
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	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: A881.exe PID: 7004 Parent PID: 3352

General

Start time:	20:23:15
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\A881.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A881.exe
Imagebase:	0x400000
File size:	321024 bytes
MD5 hash:	9AF71C74219794F100EA801B528339AF
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: 0000001A.00000002.443373510.00000000006C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000002.443196839.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000003.404265838.00000000007F0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: B217.exe PID: 4400 Parent PID: 3352

General

Start time:	20:23:18
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B217.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B217.exe
Imagebase:	0xa90000
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: 0000001B.00000002.479069139.0000000003E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001B.00000002.481840914.0000000004005000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001B.00000002.480913132.0000000003F71000.00000004.00000001.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: 3608 Parent PID: 3676

General

Start time:	20:23:23
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:	0x7ff7c6120000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1244 Parent PID: 3608

General

Start time:	20:23:23
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: cmd.exe PID: 6520 Parent PID: 7004

General

Start time:	20:23:23
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\gebcmxiz\
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: 4588 Parent PID: 6520

General

Start time:	20:23:24
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: 956 Parent PID: 7004

General

Start time:	20:23:26
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\lnagngtg.exe" C:\Windows\SysWOW64\gebcmxiz\
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: 6748 Parent PID: 956

General

Start time:	20:23:27
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	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: B217.exe PID: 6824 Parent PID: 4400

General

Start time:	20:23:32
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B217.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\B217.exe
Imagebase:	0x1b0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5872 Parent PID: 7004

General

Start time:	20:23:32
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create gebcmxiz binPath= "C:\Windows\SysWOW64\gebcmxiz\lnagngtg.exe /d\"C:\Users\user\AppData\Local\Temp\A881.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xa70000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5932 Parent PID: 5872

General

Start time:	20:23:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	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