ID: 553073
Sample Name: tijXCZsbGe.exe
Cookbook: default.jbs
Time: 09:23:23
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

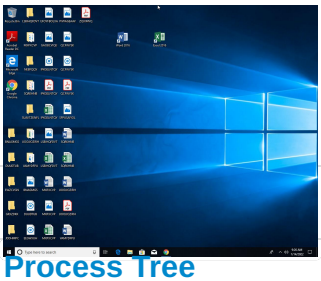
Windows Analysis Report tijXCZsbGe.exe

Overview

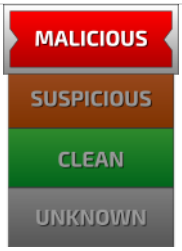
General Information

Sample Name:	tijXCZsbGe.exe
Analysis ID:	553073
MD5:	888928d26bd036..
SHA1:	37723b453fd3133.
SHA256:	1cf27ab77a771ff…
Tags:	exe RaccoonStealer
Infos:	

Most interesting Screenshot:



Detection



Amadey Raccoon RedLine SmokeLoader Tofsee Vidar

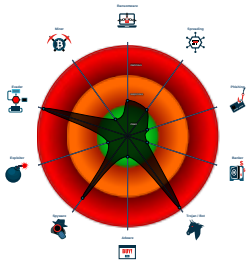
Score: 100
Range: 50 - 100

Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e.…
- Yara detected Amadeys stealer DLL
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- Yara detected Amadey bot
- System process connects to networ…
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Sigma detected: Suspect Svchost A…

Classification



Process Tree

- **System is w10x64**
- tijXCZsbGe.exe (PID: 6264 cmdline: "C:\Users\user\Desktop\tijXCZsbGe.exe" MD5: 888928D26BD03678AFD9FED0D92F6FC9)
  - tijXCZsbGe.exe (PID: 864 cmdline: "C:\Users\user\Desktop\tijXCZsbGe.exe" MD5: 888928D26BD03678AFD9FED0D92F6FC9)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 9334.exe (PID: 7100 cmdline: C:\Users\user\AppData\Local\Temp\9334.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 6552 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 264 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - DB31.exe (PID: 6560 cmdline: C:\Users\user\AppData\Local\Temp\DB31.exe MD5: 6009BCB680BE6C0F656AA157E56423DC)
      - E748.exe (PID: 5476 cmdline: C:\Users\user\AppData\Local\Temp\E748.exe MD5: 7C64BD730B6C9565F287278834A33618)
        - cmd.exe (PID: 6020 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\xzxafeeu\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5984 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\gecrjwsv.exe" C:\Windows\SysWOW64\xzxafeeu\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2972 cmdline: C:\Windows\System32\sc.exe" create xzxafeeu binPath= "C:\Windows\SysWOW64\xzxafeeu\gecrjwsv.exe /d\"C:\Users\user\AppData\Local\Temp\E748.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6584 cmdline: C:\Windows\System32\sc.exe" description xzxafeeu "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 7024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2848 cmdline: "C:\Windows\System32\sc.exe" start xzxafeeu MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - conhost.exe (PID: 6568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - reg.exe (PID: 5772 cmdline: REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\82aa4a6c48\ MD5: CEE2A7E57DF2A159A065A34913A055C2)
        - netsh.exe (PID: 6720 cmdline: "C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - F65C.exe (PID: 2980 cmdline: C:\Users\user\AppData\Local\Temp\F65C.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - F65C.exe (PID: 5348 cmdline: C:\Users\user\AppData\Local\Temp\F65C.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - 5C89.exe (PID: 5200 cmdline: C:\Users\user\AppData\Local\Temp\5C89.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - 6FB4.exe (PID: 5312 cmdline: C:\Users\user\AppData\Local\Temp\6FB4.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
        - mjlooy.exe (PID: 6756 cmdline: "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" MD5: 8B239554FE346656C8EEF9484CE8092F)
          - cmd.exe (PID: 1004 cmdline: "C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\82aa4a6c48\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - schtasks.exe (PID: 5836 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN mjlooy.exe /TR "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 6868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 8783.exe (PID: 3160 cmdline: C:\Users\user\AppData\Local\Temp\8783.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
        - AppLaunch.exe (PID: 2860 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - 9DFA.exe (PID: 4088 cmdline: C:\Users\user\AppData\Local\Temp\9DFA.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
      - B0F7.exe (PID: 6956 cmdline: C:\Users\user\AppData\Local\Temp\B0F7.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
- svchost.exe (PID: 2192 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3848 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- rifsswe (PID: 6952 cmdline: C:\Users\user\AppData\Roaming\rifsswe MD5: 888928D26BD03678AFD9FED0D92F6FC9)
  - rifsswe (PID: 7088 cmdline: C:\Users\user\AppData\Roaming\rifsswe MD5: 888928D26BD03678AFD9FED0D92F6FC9)
- svchost.exe (PID: 7020 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7128 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4972 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 7100 -ip 7100 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5016 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- gecrjwsv.exe (PID: 2860 cmdline: C:\Windows\SysWOW64\xzxafeeu\gecrjwsv.exe /d"C:\Users\user\AppData\Local\Temp\E748.exe" MD5: 6DD4312F6A305B72C1A1948F27068190)
  - svchost.exe (PID: 6732 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- mjlooy.exe (PID: 2928 cmdline: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000029.00000002.953737182.000000000821000.00000004.00000001.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
00000020.00000002.803587070.000000000400000.00000040.00020000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0000000A.00000002.767900095.000000000640000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000028.00000003.877844771.000000000382000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.719913794.000000000591000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 44 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
34.2.svchost.exe.5d0000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
32.2.gecrjwsv.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
35.0.F65C.exe.400000.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
18.2.F65C.exe.401f910.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
17.2.E748.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 29 entries				

Sigma Overview

System Summary:

- Sigma detected: Suspect Svchost Activity
- Sigma detected: Copying Sensitive Files with Credential Data
- Sigma detected: Suspicious Svchost Process
- Sigma detected: Suspicius Add Task From User AppData Temp
- Sigma detected: Netsh Port or Application Allowed
- Sigma detected: Direct Autorun Keys Modification
- Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Yara detected Raccoon Stealer
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for 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

E-Banking Fraud:

Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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

Persistence and Installation Behavior:

Yara detected Amadey bot

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

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

Tries to detect virtualization through RDTSC time measurements

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

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

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Raccoon Stealer

Yara detected Vidar stealer

Yara detected Tofsee

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Crypto Currency Wallets

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Raccoon Stealer

Yara detected Vidar stealer

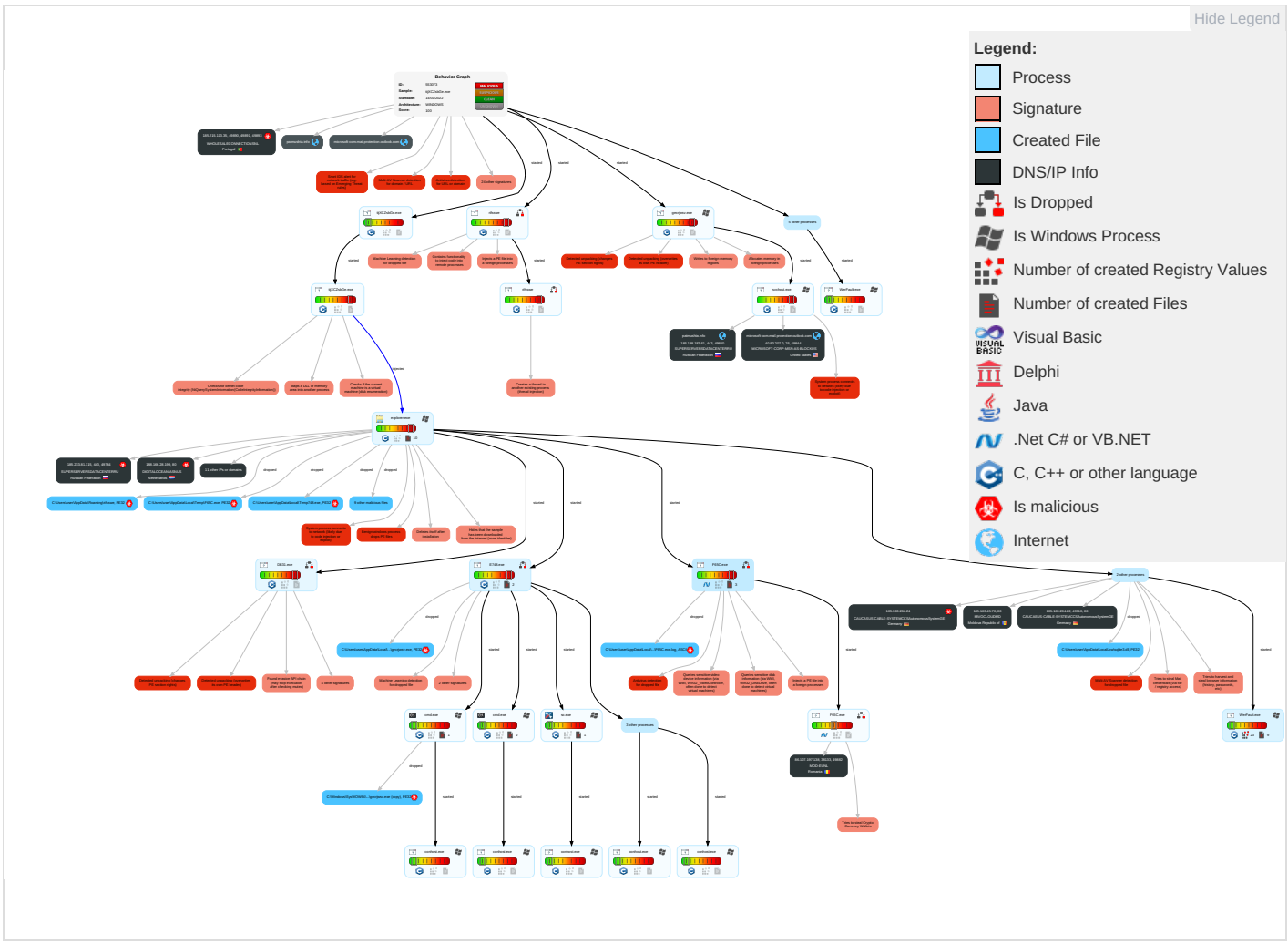
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 1	Windows Management Instrumentation 2 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Default Accounts	Native API 5 3 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Windows Service 1 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	Command and Scripting Interpreter 3	Scheduled Task/Job 1	Windows Service 1 4	Software Packing 3 3	NTDS	System Information Discovery 4 3 9	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Process Injection 7 1 3	Timestomp 1	LSA Secrets	Security Software Discovery 8 7 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Service Execution 3	Rc.common	Scheduled Task/Job 1	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Virtualization/Sandbox Evasion 4 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Modify Registry 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscat Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Virtualization/Sandbox Evasion 4 4 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Process Injection 7 1 3	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port
Trusted Relationship	Python	Hypervisor	Process Injection	Hidden Files and Directories 1	Web Portal Capture	Cloud Groups	Attack PC via USB Connection	Local Email Collection	Standard Application Layer Protocol

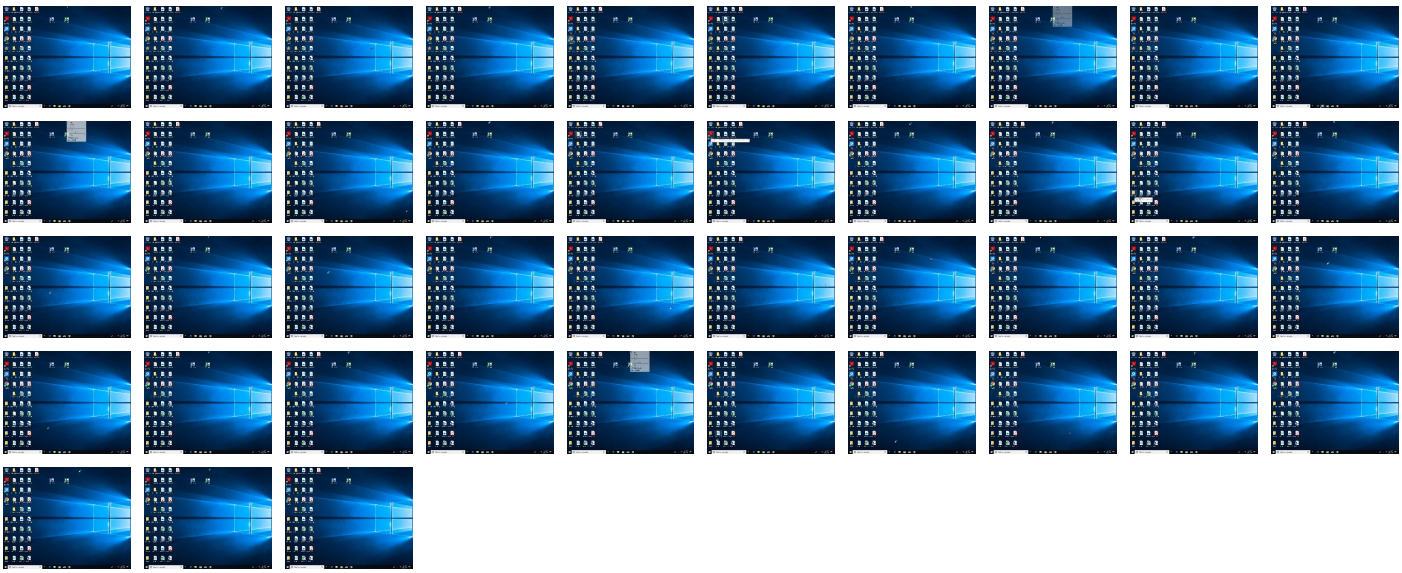
Behavior Graph



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
tijXCZsbGe.exe	34%	Virustotal		Browse
tijXCZsbGe.exe	40%	ReversingLabs	Win32.Trojan.Generic	
tijXCZsbGe.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\gecrjwsv.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\F65C.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\5C89.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rifsswe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\DB31.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\gecrjwsv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9334.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6FB4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B0F7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F65C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C7FA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8783.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9DFA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E748.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5C89.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5C89.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\6FB4.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6FB4.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Local\Temp\9334.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\9334.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\B0F7.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\B0F7.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.0.F65C.exe.ab0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
11.0.9334.exe.480e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.3.DB31.exe.660000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.2.DB31.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.rifsswe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
11.0.9334.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.9334.exe.5f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.0.F65C.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
18.0.F65C.exe.ab0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
32.2.gecrjwsv.exe.580e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.tijXCZsbGe.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.rifsswe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
38.3.5C89.exe.4d40000.2.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
35.0.F65C.exe.4d0000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
10.0.rifsswe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
35.0.F65C.exe.4d0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.tijXCZsbGe.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.rifsswe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.9334.exe.480e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.svchost.exe.5d0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
35.0.F65C.exe.4d0000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.0.F65C.exe.4d0000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.0.F65C.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
0.2.tijXCZsbGe.exe.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.0.F65C.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
32.3.gecrjwsv.exe.5a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.9334.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.F65C.exe.ab0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.0.F65C.exe.4d0000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.0.F65C.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
1.1.tijXCZsbGe.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.9334.exe.480e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.0.F65C.exe.4d0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
18.0.F65C.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.0.F65C.exe.4d0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.2.tijXCZsbGe.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.0.F65C.exe.4d0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
10.2.rifsswe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.E748.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
10.0.rifsswe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
11.2.9334.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.3.E748.exe.650000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.rifsswe.6315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.F65C.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.0.F65C.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
32.2.gecrjwsv.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
16.2.DB31.exe.640e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.rifsswe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
38.2.5C89.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1127993		Download File
32.2.gecrjwsv.exe.5a0000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
10.0.rifsswe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.0.F65C.exe.4d0000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
17.2.E748.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.1.rifsswe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.tijXCZsbGe.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.163.45.70/capibar	12%	Virustotal		Browse
http://185.163.45.70/capibar	100%	Avira URL Cloud	phishing	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/724da1c439bafff55600e6bd8e8cc799e96c03351	0%	Avira URL Cloud	safe	
http://185.215.113.35/d2VxjasuwS/index.php	12%	Virustotal		Browse
http://185.215.113.35/d2VxjasuwS/index.php	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	13%	Virustotal		Browse
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	0%	Avira URL Cloud	safe	
http://185.163.204.24/	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	100%	Avira URL Cloud	malware	
http://185.163.45.70/capibarvg	100%	Avira URL Cloud	phishing	
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/71fe7726da53cb25be1ef5cfcccec20e728d94fe	0%	Avira URL Cloud	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://crl.ver)	0%	Avira URL Cloud	safe	
http://185.163.204.22/capibar	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://178.62.113.205/capibard	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://185.163.204.22/capibar	100%	Avira URL Cloud	malware	
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://185.215.113.35/d2VxjasuwS/plugins/cred.dll	100%	Avira URL Cloud	malware	
http://185.163.204.24/22	0%	Avira URL Cloud	safe	
http://178.62.113.205/capibar	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/724da1c439bafff55600e6bd8e8cc799e96c0335	0%	Avira URL Cloud	safe	
http://185.163.204.22/capibarp	100%	Avira URL Cloud	malware	
http://help.disneyplus.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
patmushta.info	185.188.183.61	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high
microsoft-com.mail.protection.outlook.com	40.93.207.0	true	false		high
goo.su	172.67.139.105	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
data-host-coin-8.com	8.209.70.0	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://a0621298.xsph.ru/7.exe	false		high
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://185.215.113.35/d2VxjasuwS/index.php	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	true	• Avira URL Cloud: safe	unknown
http://185.163.204.24/	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	true	• Avira URL Cloud: malware	unknown
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/71fe7726da53cb25be1ef5cfcccec20e728d94fe	true	• Avira URL Cloud: safe	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://185.163.204.22/capibar	true	• Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/9.exe	false		high
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://185.215.113.35/d2VxjasuwS/plugins/cred.dll	true	• Avira URL Cloud: malware	unknown
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/724da1c439bafff55600e6bd8e8cc799e96c0335	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.163.45.70	unknown	Moldova Republic of		39798	MIVOCLOUDMD	false
40.93.207.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
185.215.113.35	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
172.67.139.105	goo.su	United States		13335	CLOUDFLARENETUS	false
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
8.209.70.0	host-data-coin-11.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.188.183.61	patmushta.info	Russian Federation		50113	SUPERSERVERSDATACENTERRU	false
185.7.214.171	unknown	France		42652	DELUNETDE	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false
185.163.204.22	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false
185.163.204.24	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553073
Start date:	14.01.2022
Start time:	09:23:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tijXCZsbGe.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:	50
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@59/23@82/18
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.1% (good quality ratio 19.3%) • Quality average: 60.8% • Quality standard deviation: 39.6%
HCA Information:	• Successful, ratio: 56% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:24:58	Task Scheduler	Run new task: Firefox Default Browser Agent 5309D4B020312F94 path: C:\Users\user\AppData\Roaming\rifsswe
09:25:10	API Interceptor	1x Sleep call for process: DB31.exe modified
09:25:22	API Interceptor	1x Sleep call for process: WerFault.exe modified
09:25:22	API Interceptor	8x Sleep call for process: svchost.exe modified
09:25:58	API Interceptor	6x Sleep call for process: 5C89.exe modified
09:25:58	API Interceptor	550x Sleep call for process: mjlooy.exe modified
09:25:59	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
09:26:19	API Interceptor	12x Sleep call for process: F65C.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_9334.exe_a5565ef87128e315374a33b3a55a1296f2841c6_94cfe485_18fbbefb\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):	0.8127421426857177
Encrypted:	false
SSDEEP:	96:wy4PvFoo+L8QJYOQoJ7R3V6tpXIQcQec6tycEfcw32+HbHg/8BRTf3o8Fa9iVfOn:9gvyV8Qh8HQ0lLjIq/u7snS274ltr
MD5:	6F6811213DC38FF2AFDB04F3CD55FF1A
SHA1:	64F43638AEC6C761650F890FF2CD403FA3D6DAC5
SHA-256:	E4404798C093AFDD465AADFACD5D3127BEE372A8939F9C3BFBF3202692A5A8FD
SHA-512:	5E8A8ECFC05DC3A0116077417A3BE790C38939CD383C817AE5FDD349BA2406CBFCD272BFB753205D84F25BDF689F72BB74FF013561A43C4DA18372E923DD11
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.=.1.3.2.8.6.6.2.2.3.0.9.4.4.9.0.0.8.7.....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.=.1.3.2.8.6.6.2.2.3.2.0.0.4.2.7.2.2.5.....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.=.8.4.d.d.1.c.7.e.-.4.7.e.3.-.4.3.b.a.-.8.5.f.1.-.a.a.c.4.e.4.5.7.7.1.f.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.f.5.b.3.d.3.3.-.c.7.8.2.-.4.4.f.f.-.9.6.5.e.-.f.5.8.7.d.e.3.5.d.8.6.9.....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.=.9.3.3.4...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.b.b.c.-.0.0.0.1.-.0.0.1.b.-.e.0.a.e.-.a.a.3.9.2.0.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.a.c.c.6.9.e.a.a.d.b.5.b.5.c.c.2.7.e.9.2.7.f.3.0.a.c.e.0.5.4.e.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.!.9.3.3.4...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\WER180D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 08:25:13 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.119769547883536
Encrypted:	false
SSDEEP:	192:/75VjONBOeh0kcSLWgKjM2Er8TDjRfvNeUkkt:TeK3lnt
MD5:	2C6138896A76E4B6272E90D3BDA15F56
SHA1:	D5DB3E974F8D4C01F98D71342BDB70004D9757DC
SHA-256:	0C14C62E9BD24CABEAC04A5C10614CCE9E66E3CDC8040F2C60A465CE5311FBEE
SHA-512:	9FA50441E67EC793DD839C1A474B427E372633817234BB645F04A41B0F43549057D4FAA0711C215081DC5FE4CDA00BE83CAF0DEBCF305D4126B420D6C75A310
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER180D.tmp.dmp	
Preview:	MDMP..... .....i3.a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....]3.a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER27DD.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):	3.7000265245349317
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiaZ6h6YrQSU6I6gmfSRSy/+pDp89bxvIcsfMbm:RrlsNiM6h6Y8SUQgmfSRSQxvIvft
MD5:	9728EFE3FCD1F2EDF2455C6C24A0E3A8
SHA1:	20CC9CA877B4F4FBE84ADFCF86985336F211DA16
SHA-256:	34E3320BCDFE5FC9DA5D259788C15BBC12D7A9EA8CF3EC9ED851E51C27C9DF31
SHA-512:	7FA47509ECF9AF82644E844110B79883B40CDAC1A881A778500D8A6A299176BC2D76FCE9DAD29BF898C4991A05A527F4912AE4874FC23CBA83CC53310BF268C
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B39.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):	4.47401591312699
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9YGWSC8B+b8fm8M4JUq8qF+LmHV+q8voq8XDt3efd:uITfRLHSNLJUrAVKoDDt3efd
MD5:	500A558B8AF1D586EF5471DEB82D8602
SHA1:	DF7939F10AAB10431EEC217AF7C43EB68C4AD4DD
SHA-256:	75C4307E165914D4F166FD85510231B7E5B0AA71E462E664DF1D9021D0508540
SHA-512:	0332FE01BE4694D34FFC2259FB9E4CC46352B9FA2983C26198776F498B174E10C0F26CA5E2AFD44443607C8A50C5C114CDFD5502580FC6C1BFD6D855D187BD2
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="1341695" />.. <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\WERFB48.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52752
Entropy (8bit):	3.033752492589164
Encrypted:	false
SSDEEP:	768:Z8Hq4E/6LytGTdG/xEaa6QZ7uw7qO2Ivta3ou1kfEvdO25:Z8Hqb6LvTdG/xyZ7urBzou1kfEvdp5
MD5:	41B4C10832B6C2E2EDBC4603B5751BCC
SHA1:	CE1FC1463DDFF7A19F40D09C25839C3A1424A0AA
SHA-256:	9E6AD05DA0DA5BCA00A6EE12209009741A352DAA4E78007CFB0AA97CC6A81A03
SHA-512:	88A36BE9A669C3D3CDF6212651DE769AF93921EABE0F46D11B9F29A46770B1C4D33595D14931D6FAE3D52D3B7B447F34AEABFB80249ECBB76669C997854843B
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB48.tmp.csv	
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6951624028803427
Encrypted:	false
SSDEEP:	96:9GiZYWUw0pVsYsaYtWjhJpyHQUYEZfRtriojXtt7wOxn07bja/8y/EcxINT3:9jZD32nh4dx6bja/8y/VuNT3
MD5:	32C5799696111CD15DF44F24AC2EEF77
SHA1:	4FD6DB5108A818C1DC4FD6EED09C6CF85FD8401E
SHA-256:	64AB345C0B68D01374BB3231B456712BDD34BAEE43B23B78A6962F9C5B1AA7DD
SHA-512:	AA873092EB6545AA15C123617C353509E2C4E40AC93AF706C39BA91587CBA79F6F42F7EA8AE8491950B4121A22CEF0F22F64D11853A40CF5E4C4E5C4A972E332
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\5C89.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\5C89.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\5C89.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\5C89.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sG8rM8v\dI3hX2r.zip	
Process:	C:\Users\user\AppData\Local\Temp\5C89.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Reputation:	unknown
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o.....[.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`.M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\.../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.\|k.5...XF.Y..lVVW..C..\|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..\|.!.....O....M....>.>.$\.%..L.zF.I...3

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\5C89.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\LocalLow\sqlite3.dll	
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\F65C.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\F65C.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\5C89.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:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x....f....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\6FB4.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368

C:\Users\user\AppData\Local\Temp\6FB4.exe

Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..U(...(...(...6.).1...6.?.W....I..+...(.....6.8.....6.(.)...6.-.)...Rich(.....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8.....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|.....@..@.reloc..4F...0...H...I.....@..B.....

C:\Users\user\AppData\Local\Temp\8783.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.....@....adata.....pS.....6.....@.....

C:\Users\user\AppData\Local\Temp\9334.exe

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

C:\Users\user\AppData\Local\Temp\9DFA.exe

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

C:\Users\user\AppData\Local\Temp\9DFA.exe

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\B0F7.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....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._ ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..''?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\C7FA.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%
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\DB31.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	322560

C:\Users\user\AppData\Local\Temp\DB31.exe	
Entropy (8bit):	6.7095586688781985
Encrypted:	false
SSDEEP:	6144:nOOJ91Tu9Vc1ye3MKfa+zqKnvDfsxa6hkZC15O5Pdz:nRJ91TYWym1ffzvD36YC15E
MD5:	6009BCB680BE6C0F656AA157E56423DC
SHA1:	FA9BA68D6B2026683BD392259BA26D7D468AEA7E
SHA-256:	5C037C7C1338CF54A9D1E81B74BB4AD003E1A254069A03499426EC1600A748D9
SHA-512:	5ECE7D9531051C951DFA0CF9533AB778B468EBE3EBE5D7B8A934D408E69BE910F244C59810A5FB41376B1CA7E5EB78DBF514032354EF047D00F043E2A17795E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...9.-`.....@.....$...(.....0...@.....D..... .text..... ..`.data.....@....gave.....@....noduf.....@....gafal.....@....rsrc..... ....@..@.reloc..dF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\E748.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.68576465213566
Encrypted:	false
SSDEEP:	6144:tFaYhNulUB/eDlvaOA2tm9gogt8nfF9TJwnGbQ5+:tFnhNulSEvYcOgonTTJwEQ5
MD5:	7C64BD730B6C9565F287278834A33618
SHA1:	0D36AF541B32F19FD18E7FDA3F55440C97D22407
SHA-256:	6CB775A7C9B0CF8BA308029DC623E1DE6D17CB2AB6B7EBBBD9C16BFCAA55EFE8
SHA-512:	A8A304220B0CCA1058449511BDE2973E90F9237BE36A909C070AF2C0C9B6D340DB21A0287BCDFA9D333C61FCA1A7D7C95E4CDF4288C8D192FD681ADA4F3220 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L.....`.....@.....(.....0...@.....D..... text...d..... ..`.data.....@....sop.....@....fob.....@....hasajo.....@....rsrc..... .....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\F65C.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\gecrjwsv.exe	
Process:	C:\Users\user\AppData\Local\Temp\E748.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11673600
Entropy (8bit):	3.816723429746929

C:\Users\user\AppData\Local\Temp\gecrjwsv.exe	
Encrypted:	false
SSDEEP:	6144:OFaYhNulUB/eDlvaOA2tm9gogt8nfF9TJwnGbQ5+:OFnhNulSEvYcOgonTTJwEQ5
MD5:	6DD4312F6A305B72C1A1948F27068190
SHA1:	1A76D5EB3D9CB7628B746A2C649DC6CCC03EACAC
SHA-256:	DD1F717452D1875BF3AF9FDE8D4AC06514FF9B05E58C579E6AD5F2B0A5F4D51F
SHA-512:	BC1742225A9FC18856424423C062E7CCA7CA28C0232F23FBF78661898144D92EA9A2EC6FF4EC91BCA50B69C2B33CB2F43E059A6AFAB8B0BFA86517A8BBA9140 5
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....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L.....`.....@.....(.....0...@.....D..... text...d..... ..`.data.....@....sop.....@....fob.....@....hasajo.....@....rsrc..... .....@..@.reloc..ZF.....@..B..... .....

C:\Users\user\AppData\Roaming\rifsswe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.691089236822667
Encrypted:	false
SSDEEP:	6144:0H4/g0hr5Y3eofIaxJGgOe8nQGo/GOEEmBbejvf:0Y4OuJI8pd8a/GAmBbe
MD5:	888928D26BD03678AFD9FED0D92F6FC9
SHA1:	37723B453FD3133C01E7A43892B73C6580EDD164
SHA-256:	1CF27AB77A771FF942B1E2947856844FBAB4991CF87ACA618968445B5C5D706D
SHA-512:	7007BA06A902089229F384650DE75ABCEC8740501F3E6A12F421951689F932582DD5749234B8B635D074B3BDD1061AC786449DD582BDAF840FBDEF9BF2BB76F2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L....U.`.....@.....P.....(.....0...@.....D..... .text...D..... ..`.data.....@....koyalef.....@....bopi.....@....cegem.....@....rsrc..... .....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Roaming\rifsswe: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\SysWOW64\xzxafeeu\gecrjwsv.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11673600
Entropy (8bit):	3.816723429746929
Encrypted:	false
SSDEEP:	6144:OFaYhNulUB/eDlvaOA2tm9gogt8nfF9TJwnGbQ5+:OFnhNulSEvYcOgonTTJwEQ5
MD5:	6DD4312F6A305B72C1A1948F27068190
SHA1:	1A76D5EB3D9CB7628B746A2C649DC6CCC03EACAC
SHA-256:	DD1F717452D1875BF3AF9FDE8D4AC06514FF9B05E58C579E6AD5F2B0A5F4D51F

C:\Windows\SysWOW64\xzxafeeu\gecrjwsv.exe (copy)	
SHA-512:	BC1742225A9FC18856424423C062E7CCA7CA28C0232F23FBF78661898144D92EA9A2EC6FF4EC91BCA50B69C2B33CB2F43E059A6AFAB8B0BFA86517A8BBA9140 5
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L.....`.....@.....(.....0...@.....D..... text...d..... ..`.data.....@....sop.....@....fob.....@....hasajo.....@....rsrc..... .....@..@.reloc..ZF.....@..B..... .....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.236352523388576
Encrypted:	false
SSDEEP:	12288:qCkTwSoKc2tIokbtAz9HlFkEwQVj9jNoD+d+qnG3miIAAQVi:nkTwSoKc2tjkbt23w
MD5:	9559FE849D365085D314F82D67F2A35E
SHA1:	CC18BA14948462C90BF7D9A82DF399FFDCD009E9
SHA-256:	095A6F3AC520C2FCA853EF867B55E04B72221523137DE58C8882C4F38117BA4E
SHA-512:	BBDABC4E7D8B64576FCFE31D1438E6A1C854772AE2EB0633C76676D72AB992B1F77C097DCEFEF9FBE4C5D9FB92EBAAF5D576F316A02180FD08E33A4C20794E CD
Malicious:	false
Reputation:	unknown
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.%C= ....H`..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.3460374001719013
Encrypted:	false
SSDEEP:	384:jjC5K5gBv4KgnVVeeDzeT1NKZtjbT8GxwQ3zeDM8y:P8KUg/eeDzeJNYtj0GxwQiM8
MD5:	B70CC5CA4245A261BB82B3C28B555A61
SHA1:	935103E48FCA22FF96AED36458371D966DA4594B
SHA-256:	FCB60B171A00416847309E79408CA0FC4AB0D093257417FD4C3BAB1BB9EF4D8D
SHA-512:	45EBF9B3A9848A4F94F04CF1B055ABDB90A166C286179DB9E394900EED75E7DF19368B83CFE63B0902FA49511706E057859287756D7D735D4CEDD57710A8270E
Malicious:	false
Reputation:	unknown
Preview:	regfG...G...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.%C= ....H`HvLE.N.....G.....&.....md..... ..hbin.....p.\..,.....nk,...E= .....x..... .....&...{ad79c032-a2ea-f756-e377- 72fb9332c3ae}.....nk ...E= ....Z.....Root.....lf.....Root....nk ...E= ....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.691089236822667
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:	tijXCZsbGe.exe

General

File size:	320512
MD5:	888928d26bd03678afd9fed0d92f6fc9
SHA1:	37723b453fd3133c01e7a43892b73c6580edd164
SHA256:	1cf27ab77a771ff942b1e2947856844fbab4991cf87aca618968445b5c5d706d
SHA512:	7007ba06a902089229f384650de75abcec8740501f3e6a12f421951689f932582dd5749234b8b635d074b3bdd1061ac786449dd582bdaf840fbdef9bf2bb76f2
SSDEEP:	6144:0H4/g0hr5Y3eofIaxJGgOe8nQGo/GOEEmBbejvf:0Y4OuJI8pd8a/GAmBbe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R.....g.R..])...R...S...R.....R.....R.....R.Rich..R.....PE..L....U.`.....

File Icon

Icon Hash:	c8d0d8e0f8e0f0e8

Static PE Info

General

Entrypoint:	0x41b7b0
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:	0x60A45518 [Wed May 19 00:00:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	80fec6fca6f81033220e34b44810dbfd

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e844	0x3ea00	False	0.582655002495	data	6.96511151774	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.340657552083	data	3.46253582216	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.koyalef	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bopi	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.cegem	0x14f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x83b8	0x8400	False	0.597005208333	data	5.81594555385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x159000	0x465a	0x4800	False	0.346625434028	data	3.69106106097	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	
Spanish	Colombia	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 09:24:58.504261971 CET	192.168.2.4	8.8.8.8	0x85fb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:58.950818062 CET	192.168.2.4	8.8.8.8	0x61cb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:59.455101967 CET	192.168.2.4	8.8.8.8	0x35d0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:59.623431921 CET	192.168.2.4	8.8.8.8	0x9b0a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:00.062973976 CET	192.168.2.4	8.8.8.8	0x5fa1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:00.258764029 CET	192.168.2.4	8.8.8.8	0xd8c1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:01.648228884 CET	192.168.2.4	8.8.8.8	0xe4b6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:01.821270943 CET	192.168.2.4	8.8.8.8	0x8084	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:01.988954067 CET	192.168.2.4	8.8.8.8	0x92df	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:04.468344927 CET	192.168.2.4	8.8.8.8	0x133b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:04.640755892 CET	192.168.2.4	8.8.8.8	0x824a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:05.106497049 CET	192.168.2.4	8.8.8.8	0x4276	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:05.744245052 CET	192.168.2.4	8.8.8.8	0xe630	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:05.910893917 CET	192.168.2.4	8.8.8.8	0x2f13	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:06.375499964 CET	192.168.2.4	8.8.8.8	0x6231	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:06.536884069 CET	192.168.2.4	8.8.8.8	0xdf03	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 09:25:06.966842890 CET	192.168.2.4	8.8.8.8	0xc429	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.441303968 CET	192.168.2.4	8.8.8.8	0x1c71	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.610197067 CET	192.168.2.4	8.8.8.8	0xdf90	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.781980991 CET	192.168.2.4	8.8.8.8	0x9e69	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.059603930 CET	192.168.2.4	8.8.8.8	0x36a9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.232727051 CET	192.168.2.4	8.8.8.8	0x93a7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.402065992 CET	192.168.2.4	8.8.8.8	0xbaac	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.569469929 CET	192.168.2.4	8.8.8.8	0x8806	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.421874046 CET	192.168.2.4	8.8.8.8	0x90eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.614980936 CET	192.168.2.4	8.8.8.8	0xfe69	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.780625105 CET	192.168.2.4	8.8.8.8	0x9c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.975579023 CET	192.168.2.4	8.8.8.8	0xa24e	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:16.770625114 CET	192.168.2.4	8.8.8.8	0x73ed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:16.948978901 CET	192.168.2.4	8.8.8.8	0xcf20	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:17.118690014 CET	192.168.2.4	8.8.8.8	0x702f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.734503031 CET	192.168.2.4	8.8.8.8	0xaa98	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.404217958 CET	192.168.2.4	8.8.8.8	0x571	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.500076056 CET	192.168.2.4	8.8.8.8	0xe74c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.686891079 CET	192.168.2.4	8.8.8.8	0x7390	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.855894089 CET	192.168.2.4	8.8.8.8	0x8cdc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.023346901 CET	192.168.2.4	8.8.8.8	0xffa9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.190979004 CET	192.168.2.4	8.8.8.8	0xfc72	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.357533932 CET	192.168.2.4	8.8.8.8	0x3b0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.527564049 CET	192.168.2.4	8.8.8.8	0x920	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.692435980 CET	192.168.2.4	8.8.8.8	0x24e6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.905060053 CET	192.168.2.4	8.8.8.8	0x4803	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.069976091 CET	192.168.2.4	8.8.8.8	0x5683	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.237016916 CET	192.168.2.4	8.8.8.8	0xf82a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.408840895 CET	192.168.2.4	8.8.8.8	0x3a0d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.596249104 CET	192.168.2.4	8.8.8.8	0x19d5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.764209986 CET	192.168.2.4	8.8.8.8	0x2a54	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.216681957 CET	192.168.2.4	8.8.8.8	0xb533	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.395333052 CET	192.168.2.4	8.8.8.8	0xf8e5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.580280066 CET	192.168.2.4	8.8.8.8	0x709a	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.040406942 CET	192.168.2.4	8.8.8.8	0x2e9c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.207436085 CET	192.168.2.4	8.8.8.8	0x4d69	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 09:25:45.357714891 CET	192.168.2.4	8.8.8.8	0x7264	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.525964975 CET	192.168.2.4	8.8.8.8	0x4cdb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.691128969 CET	192.168.2.4	8.8.8.8	0xec9a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.881808043 CET	192.168.2.4	8.8.8.8	0x4146	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:46.060853004 CET	192.168.2.4	8.8.8.8	0x3909	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:48.854824066 CET	192.168.2.4	8.8.8.8	0x387	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:49.086039066 CET	192.168.2.4	8.8.8.8	0xe7dc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:49.422725916 CET	192.168.2.4	8.8.8.8	0x9abc	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:50.660095930 CET	192.168.2.4	8.8.8.8	0x6f10	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:50.825428963 CET	192.168.2.4	8.8.8.8	0x450b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:51.017307043 CET	192.168.2.4	8.8.8.8	0xc9d6	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:55.965636969 CET	192.168.2.4	8.8.8.8	0x9c3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.136208057 CET	192.168.2.4	8.8.8.8	0xbfd2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.302062988 CET	192.168.2.4	8.8.8.8	0x9b36	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.494359016 CET	192.168.2.4	8.8.8.8	0xa220	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.717469931 CET	192.168.2.4	8.8.8.8	0xe9f1	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:02.268810034 CET	192.168.2.4	8.8.8.8	0x327	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:02.440820932 CET	192.168.2.4	8.8.8.8	0xd067	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:02.614178896 CET	192.168.2.4	8.8.8.8	0x6ba5	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.254791021 CET	192.168.2.4	8.8.8.8	0x56c5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.447556973 CET	192.168.2.4	8.8.8.8	0xd10b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.803284883 CET	192.168.2.4	8.8.8.8	0x33c6	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.037647009 CET	192.168.2.4	8.8.8.8	0x8385	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.210942030 CET	192.168.2.4	8.8.8.8	0xcd06	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.423469067 CET	192.168.2.4	8.8.8.8	0x5a80	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.783442020 CET	192.168.2.4	8.8.8.8	0x6be3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.954782009 CET	192.168.2.4	8.8.8.8	0x21f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:18.736825943 CET	192.168.2.4	8.8.8.8	0xe7c1	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.934835911 CET	192.168.2.4	8.8.8.8	0x8983	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:27:08.800683975 CET	192.168.2.4	8.8.8.8	0x62dd	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 09:24:58.794605017 CET	8.8.8.8	192.168.2.4	0x85fb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:59.283950090 CET	8.8.8.8	192.168.2.4	0x61cb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:59.474836111 CET	8.8.8.8	192.168.2.4	0x35d0	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 09:24:59.906702042 CET	8.8.8.8	192.168.2.4	0x9b0a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:00.082065105 CET	8.8.8.8	192.168.2.4	0x5fa1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:00.275962114 CET	8.8.8.8	192.168.2.4	0xd8c1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:01.666069984 CET	8.8.8.8	192.168.2.4	0xe4b6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:01.841012955 CET	8.8.8.8	192.168.2.4	0x8084	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:02.297612906 CET	8.8.8.8	192.168.2.4	0x92df	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:04.487859011 CET	8.8.8.8	192.168.2.4	0x133b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:04.958055973 CET	8.8.8.8	192.168.2.4	0x824a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:05.424448967 CET	8.8.8.8	192.168.2.4	0x4276	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:05.763828993 CET	8.8.8.8	192.168.2.4	0xe630	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:06.228406906 CET	8.8.8.8	192.168.2.4	0x2f13	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:06.478178978 CET	8.8.8.8	192.168.2.4	0x6231	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:06.824743986 CET	8.8.8.8	192.168.2.4	0xdf03	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.291708946 CET	8.8.8.8	192.168.2.4	0xc429	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.460710049 CET	8.8.8.8	192.168.2.4	0x1c71	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.627312899 CET	8.8.8.8	192.168.2.4	0xdf90	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:08.099401951 CET	8.8.8.8	192.168.2.4	0x9e69	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.078922033 CET	8.8.8.8	192.168.2.4	0x36a9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.251872063 CET	8.8.8.8	192.168.2.4	0x93a7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.421320915 CET	8.8.8.8	192.168.2.4	0xbaac	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.588691950 CET	8.8.8.8	192.168.2.4	0x8806	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.441111088 CET	8.8.8.8	192.168.2.4	0x90eb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.634314060 CET	8.8.8.8	192.168.2.4	0xfe69	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.799860001 CET	8.8.8.8	192.168.2.4	0x9c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.996831894 CET	8.8.8.8	192.168.2.4	0xa24e	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.996831894 CET	8.8.8.8	192.168.2.4	0xa24e	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 09:25:14.996831894 CET	8.8.8.8	192.168.2.4	0xa24e	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.996831894 CET	8.8.8.8	192.168.2.4	0xa24e	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:14.996831894 CET	8.8.8.8	192.168.2.4	0xa24e	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:16.788121939 CET	8.8.8.8	192.168.2.4	0x73ed	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:16.968163013 CET	8.8.8.8	192.168.2.4	0xcf20	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:17.136274099 CET	8.8.8.8	192.168.2.4	0x702f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.761554003 CET	8.8.8.8	192.168.2.4	0xaa98	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.761554003 CET	8.8.8.8	192.168.2.4	0xaa98	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.761554003 CET	8.8.8.8	192.168.2.4	0xaa98	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.761554003 CET	8.8.8.8	192.168.2.4	0xaa98	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.761554003 CET	8.8.8.8	192.168.2.4	0xaa98	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.761554003 CET	8.8.8.8	192.168.2.4	0xaa98	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.421423912 CET	8.8.8.8	192.168.2.4	0x571	No error (0)	patmushta.info		185.188.183.61	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.519500017 CET	8.8.8.8	192.168.2.4	0xe74c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.704005003 CET	8.8.8.8	192.168.2.4	0x7390	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:38.875216007 CET	8.8.8.8	192.168.2.4	0x8cdc	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.040910959 CET	8.8.8.8	192.168.2.4	0xffa9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.209981918 CET	8.8.8.8	192.168.2.4	0xfc72	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.377321959 CET	8.8.8.8	192.168.2.4	0x3b0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.547108889 CET	8.8.8.8	192.168.2.4	0x920	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.711781025 CET	8.8.8.8	192.168.2.4	0x24e6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:39.924561024 CET	8.8.8.8	192.168.2.4	0x4803	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.088764906 CET	8.8.8.8	192.168.2.4	0x5683	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.256330013 CET	8.8.8.8	192.168.2.4	0xf82a	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 09:25:40.428683043 CET	8.8.8.8	192.168.2.4	0x3a0d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.615529060 CET	8.8.8.8	192.168.2.4	0x19d5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:41.087089062 CET	8.8.8.8	192.168.2.4	0x2a54	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.236279964 CET	8.8.8.8	192.168.2.4	0xb533	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.412606001 CET	8.8.8.8	192.168.2.4	0xf8e5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.609112024 CET	8.8.8.8	192.168.2.4	0x709a	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.609112024 CET	8.8.8.8	192.168.2.4	0x709a	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.059613943 CET	8.8.8.8	192.168.2.4	0x2e9c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.226744890 CET	8.8.8.8	192.168.2.4	0x4d69	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.376952887 CET	8.8.8.8	192.168.2.4	0x7264	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.545367956 CET	8.8.8.8	192.168.2.4	0x4cdb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.710396051 CET	8.8.8.8	192.168.2.4	0xec9a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.907784939 CET	8.8.8.8	192.168.2.4	0x4146	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:46.080140114 CET	8.8.8.8	192.168.2.4	0x3909	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:48.871977091 CET	8.8.8.8	192.168.2.4	0x387	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:49.104904890 CET	8.8.8.8	192.168.2.4	0xe7dc	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:49.450273991 CET	8.8.8.8	192.168.2.4	0x9abc	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:50.677923918 CET	8.8.8.8	192.168.2.4	0x6f10	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:50.844213963 CET	8.8.8.8	192.168.2.4	0x450b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:51.036268950 CET	8.8.8.8	192.168.2.4	0xc9d6	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:55.984693050 CET	8.8.8.8	192.168.2.4	0x9c3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.155317068 CET	8.8.8.8	192.168.2.4	0xbfd2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.321657896 CET	8.8.8.8	192.168.2.4	0x9b36	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.513890982 CET	8.8.8.8	192.168.2.4	0xa220	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:56.740719080 CET	8.8.8.8	192.168.2.4	0xe9f1	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:02.287682056 CET	8.8.8.8	192.168.2.4	0x327	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 09:26:02.458193064 CET	8.8.8.8	192.168.2.4	0xd067	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:02.633424044 CET	8.8.8.8	192.168.2.4	0x6ba5	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.274209023 CET	8.8.8.8	192.168.2.4	0x56c5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.467144966 CET	8.8.8.8	192.168.2.4	0xd10b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.820511103 CET	8.8.8.8	192.168.2.4	0x33c6	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.056818962 CET	8.8.8.8	192.168.2.4	0x8385	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.230015039 CET	8.8.8.8	192.168.2.4	0xcd06	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.449105978 CET	8.8.8.8	192.168.2.4	0x5a80	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.800724030 CET	8.8.8.8	192.168.2.4	0x6be3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.973896980 CET	8.8.8.8	192.168.2.4	0x21f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:18.754103899 CET	8.8.8.8	192.168.2.4	0xe7c1	No error (0)	patmushta.info		185.188.183.61	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.962934971 CET	8.8.8.8	192.168.2.4	0x8983	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.962934971 CET	8.8.8.8	192.168.2.4	0x8983	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.962934971 CET	8.8.8.8	192.168.2.4	0x8983	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.962934971 CET	8.8.8.8	192.168.2.4	0x8983	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.962934971 CET	8.8.8.8	192.168.2.4	0x8983	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:25.962934971 CET	8.8.8.8	192.168.2.4	0x8983	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 09:27:08.820175886 CET	8.8.8.8	192.168.2.4	0x62dd	No error (0)	patmushta.info		185.188.183.61	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- rftojqy.com
  - host-data-coin-11.com
- oeicpl.com
- gmlcwn.org
- pmxge.org
- klnnrs.org

- sqgycmxrcw.org
- ordgyi.com
- gdpbobblv.org
- data-host-coin-8.com
- ojnph.org
- qnhvcpx.org
- ukmdaxlu.com
- cocugqsn.org
- bcdqnjq.com
- unicupload.top
- quobomy.org
- hfkcwyd.com
- lhmfcrnoc.net
- rwnoc.com
- hyhfejnsaf.org
- yupkrg.org
- xasgjbpj.net
- dlsrcuywsx.net
- 185.7.214.171:8080
- ygpvsdtxwa.net
- ctudyypa.org
- fnqfdlb.org
- qernbnk.net
- lymetcvj.org
- dwyid.net
- rtyuw.net
- iymvh.com
- aujnrph.com
- qjfqvve.com
- betkhbcokn.net

- buvim.org
- tuwgresxff.net
- esfdrx.org
- gimbqwejt.org
- vqkgjg.net
- qfojwny.com
- jypmxggbe.net
- bopkt.com
- rcosdqvkc.net
- vpvuvi.org
- xchjuwapl.net
- kcgcly.org
- xhcmjwqukh.net
- tbwkdtvra.com
- unlkmoivsp.org
- buyqsohhho.net
- lmtmt.net
- a0621298.xsph.ru
- guadmgqcy.com
- aaxrubcof.net
- uswhy.com
- vqmqnwq.com
- ulfdnrx.net
- vyvnhyowq.net
- 185.215.113.35
- mpjbq.net
- smapchtl.com
- 185.163.204.22
- jeacjnamm.com
- awifxkoma.net

- 185.163.204.24
- aoummij.com
- omefw.net
- bgprljhr.com
- lptdnkjgh.net

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: tijXCZsbGe.exe PID: 6264 Parent PID: 5204

General

Start time:	09:24:18
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\tijXCZsbGe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\tijXCZsbGe.exe"
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	888928D26BD03678AFD9FED0D92F6FC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: tijXCZsbGe.exe PID: 864 Parent PID: 6264

General

Start time:	09:24:19
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\tijXCZsbGe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\tijXCZsbGe.exe"
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	888928D26BD03678AFD9FED0D92F6FC9
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.719913794.0000000000591000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.719885078.0000000000570000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 864

General

Start time:	09:24:26
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000000.708378047.0000000004DF1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 2192 Parent PID: 568

General

Start time:	09:24:27
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3848 Parent PID: 568

General

Start time:	09:24:46
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:	0x7ff732050000
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: rifsswe PID: 6952 Parent PID: 968

General

Start time:	09:24:58
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\rifsswe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rifsswe
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	888928D26BD03678AFD9FED0D92F6FC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: rifsswe PID: 7088 Parent PID: 6952

General

Start time:	09:24:59
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\rifsswe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rifsswe
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	888928D26BD03678AFD9FED0D92F6FC9
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: 0000000A.00000002.767900095.0000000000640000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000A.00000002.768056484.00000000022F1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 9334.exe PID: 7100 Parent PID: 3424

General

Start time:	09:25:02
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\9334.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\9334.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs
Reputation:	moderate

Analysis Process: svchost.exe PID: 7020 Parent PID: 568

General

Start time:	09:25:02
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 7128 Parent PID: 568

General

Start time:	09:25:05
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 4972 Parent PID: 7128

General

Start time:	09:25:05
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 7100 -ip 7100
Imagebase:	0xe90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6552 Parent PID: 7100

General

Start time:	09:25:06
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 264
Imagebase:	0xe90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: DB31.exe PID: 6560 Parent PID: 3424

General

Start time:	09:25:07
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\DB31.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DB31.exe
Imagebase:	0x400000

File size:	322560 bytes
MD5 hash:	6009BCB680BE6C0F656AA157E56423DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.780534031.0000000000712000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000010.00000002.780534031.0000000000712000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: E748.exe PID: 5476 Parent PID: 3424

General

Start time:	09:25:11
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E748.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E748.exe
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	7C64BD730B6C9565F287278834A33618
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000002.953428772.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000002.957118764.0000000000630000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000011.00000003.783551055.0000000000650000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: F65C.exe PID: 2980 Parent PID: 3424

General

Start time:	09:25:14
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\F65C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F65C.exe
Imagebase:	0xab0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000002.825741767.0000000003F01000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 6020 Parent PID: 5476

General

Start time:	09:25:16
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\xzxafeeu\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 4460 Parent PID: 6020

General

Start time:	09:25:16
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5984 Parent PID: 5476

General

Start time:	09:25:17
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\gecrjwsv.exe" C:\Windows\SysWOW64\xzxafeeu\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 4728 Parent PID: 5984

General

Start time:	09:25:17
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 2972 Parent PID: 5476

General

Start time:	09:25:17
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create xzxafeeu binPath= "C:\Windows\SysWOW64\xzxafeeu\gecrjwsv.exe /d\"C:\Users\user\AppData\Local\Temp\E748.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xd10000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5572 Parent PID: 2972

General

Start time:	09:25:18

Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6584 Parent PID: 5476

General

Start time:	09:25:19
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description xzxafeeu "wifi internet conection
Imagebase:	0xd10000
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: 7024 Parent PID: 6584

General

Start time:	09:25:19
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5016 Parent PID: 568

General

Start time:	09:25:19
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 2848 Parent PID: 5476

General

Start time:	09:25:20
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start xzxafeeu
Imagebase:	0xd10000
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: 1004 Parent PID: 2848

General

Start time:	09:25:20
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: gecrjwsv.exe PID: 2860 Parent PID: 568

General

Start time:	09:25:21
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\xzxafeeu\gecrjwsv.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\xzxafeeu\gecrjwsv.exe /d"C:\Users\user\AppData\Local\Temp\E748.exe"
Imagebase:	0x400000
File size:	11673600 bytes
MD5 hash:	6DD4312F6A305B72C1A1948F27068190
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000002.803587070.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000002.803962316.00000000005A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000003.801375609.00000000005A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000020.00000002.803904384.0000000000580000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: netsh.exe PID: 6720 Parent PID: 5476

General

Start time:	09:25:21
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x360000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6732 Parent PID: 2860

General

Start time:	09:25:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0x12f0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000022.00000002.949927934.00000000005D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: F65C.exe PID: 5348 Parent PID: 2980

General

Start time:	09:25:24
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\F65C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F65C.exe
Imagebase:	0x4d0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000023.00000000.820336133.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000023.00000000.821341997.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000023.00000000.819697566.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000023.00000000.820836278.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 5C89.exe PID: 5200 Parent PID: 3424

General

Start time:	09:25:41
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\5C89.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\5C89.exe
Imagebase:	0x400000
File size:	905216 bytes
MD5 hash:	852D86F5BC34BF4AF7FA89C60569DF13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000026.00000003.868438969.0000000004DE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000026.00000002.1024945743.0000000004D40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000026.00000002.953575570.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis