ID: 553170
Sample Name: sbxGIUIhRd.exe
Cookbook: default.jbs
Time: 12:27:37
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

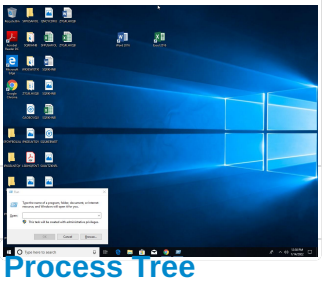
Windows Analysis Report sbxGIUlhRd.exe

Overview

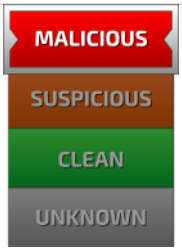
General Information

Sample Name:	sbxGIUlhRd.exe
Analysis ID:	553170
MD5:	f768f4a81e8b87d..
SHA1:	d0e5c1e975ec41..
SHA256:	164149035d4a3d..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



Amadey Raccoon RedLine SmokeLoader Tofsee Vidar

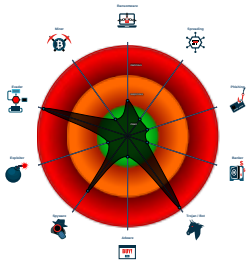
Score: 100
Range: 0 - 100

Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e.…
- 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**
- sbxGIUIhRd.exe (PID: 6964 cmdline: "C:\Users\user\Desktop\sbxGIUIhRd.exe" MD5: F768F4A81E8B87D6990895A35B8D7D6C)
  - sbxGIUIhRd.exe (PID: 6984 cmdline: "C:\Users\user\Desktop\sbxGIUIhRd.exe" MD5: F768F4A81E8B87D6990895A35B8D7D6C)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 8A6B.exe (PID: 6760 cmdline: C:\Users\user\AppData\Local\Temp\8A6B.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 6812 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6760 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 95C6.exe (PID: 6844 cmdline: C:\Users\user\AppData\Local\Temp\95C6.exe MD5: F768F4A81E8B87D6990895A35B8D7D6C)
        - 95C6.exe (PID: 6804 cmdline: C:\Users\user\AppData\Local\Temp\95C6.exe MD5: F768F4A81E8B87D6990895A35B8D7D6C)
      - CFE8.exe (PID: 4296 cmdline: C:\Users\user\AppData\Local\Temp\CFE8.exe MD5: E1AF41681888A847863EE17BD63450A0)
      - E2A6.exe (PID: 4752 cmdline: C:\Users\user\AppData\Local\Temp\E2A6.exe MD5: E4B33586BFDB5A9CD45F3038B8F4CCBD)
        - cmd.exe (PID: 5768 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\txlhcyih\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 4692 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\gaystiqf.exe" C:\Windows\SysWOW64\txlhcyih\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - extd.exe (PID: 5016 cmdline: C:\Users\user\AppData\Local\Temp\63DA.tmp\63DB.tmp\extd.exe "/hideself" "" "" "" "" "" "" "" "" "" MD5: 139B5CE627BC9EC1040A91EBE7830F7C)
        - sc.exe (PID: 4044 cmdline: C:\Windows\System32\sc.exe" create txlhcyih binPath= "C:\Windows\SysWOW64\txlhcyih\gaystiqf.exe /d\"C:\Users\user\AppData\Local\Temp\E2A6.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 2860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 240 cmdline: C:\Windows\System32\sc.exe" description txlhcyih "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 1740 cmdline: "C:\Windows\System32\sc.exe" start txlhcyih MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 2216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 6536 cmdline: "C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - conhost.exe (PID: 4620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - FA5C.exe (PID: 796 cmdline: C:\Users\user\AppData\Local\Temp\FA5C.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - FA5C.exe (PID: 1496 cmdline: C:\Users\user\AppData\Local\Temp\FA5C.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - 7D38.exe (PID: 6752 cmdline: C:\Users\user\AppData\Local\Temp\7D38.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - 96DB.exe (PID: 6404 cmdline: C:\Users\user\AppData\Local\Temp\96DB.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
        - mjlooy.exe (PID: 6804 cmdline: "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" MD5: 8B239554FE346656C8EEF9484CE8092F)
      - A15C.exe (PID: 5412 cmdline: C:\Users\user\AppData\Local\Temp\A15C.exe MD5: 6E7430832C1C24C2BF8BE746F2FE583C)
        - conhost.exe (PID: 4296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6316 cmdline: C:\Windows\sysnative\cmd" /c "C:\Users\user\AppData\Local\Temp\63DA.tmp\63DB.tmp\63DC.bat C:\Users\user\AppData\Local\Temp\A15C.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- svchost.exe (PID: 6228 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5420 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- adijaeg (PID: 6604 cmdline: C:\Users\user\AppData\Roaming\adijaeg MD5: F768F4A81E8B87D6990895A35B8D7D6C)
  - adijaeg (PID: 4204 cmdline: C:\Users\user\AppData\Roaming\adijaeg MD5: F768F4A81E8B87D6990895A35B8D7D6C)
- svchost.exe (PID: 6976 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6868 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6924 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6760 -ip 6760 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4800 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- gaystiqf.exe (PID: 4588 cmdline: C:\Windows\SysWOW64\txlhcyih\gaystiqf.exe /d"C:\Users\user\AppData\Local\Temp\E2A6.exe" MD5: 6D07EFE4270BD10431D8E32CADCFF4E7)
  - svchost.exe (PID: 5288 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- adijaeg (PID: 7148 cmdline: C:\Users\user\AppData\Roaming\adijaeg MD5: F768F4A81E8B87D6990895A35B8D7D6C)
  - adijaeg (PID: 6424 cmdline: C:\Users\user\AppData\Roaming\adijaeg MD5: F768F4A81E8B87D6990895A35B8D7D6C)
- **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
0000000A.00000002.767064606.000000000056 1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000030.00000002.933969192.000000000065 0000.00000040.00000001.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000001.00000002.719013921.000000000058 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000030.00000002.934394338.00000000007C 2000.00000004.00000001.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
0000002E.00000003.893800912.00000000026D 7000.00000004.00000040.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.95C6.exe.400000.0.unpack	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
1.0.sbxGIUIhRd.exe.400000.6.unpack	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
19.2.E2A6.exe.560e50.1.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
39.0.FA5C.exe.400000.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
39.0.FA5C.exe.400000.12.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 30 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Svchost Process

Sigma detected: Netsh Port or Application Allowed

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Raccoon Stealer

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for 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)

Yara detected BatToExe compiled binary

.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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

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

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

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Benign windows process drops PE files
- Maps a DLL or memory area into another process
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Contains functionality to inject code into remote processes
- Creates a thread in another existing process (thread injection)
- Writes to foreign memory regions
- .NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings
- 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
- Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality:

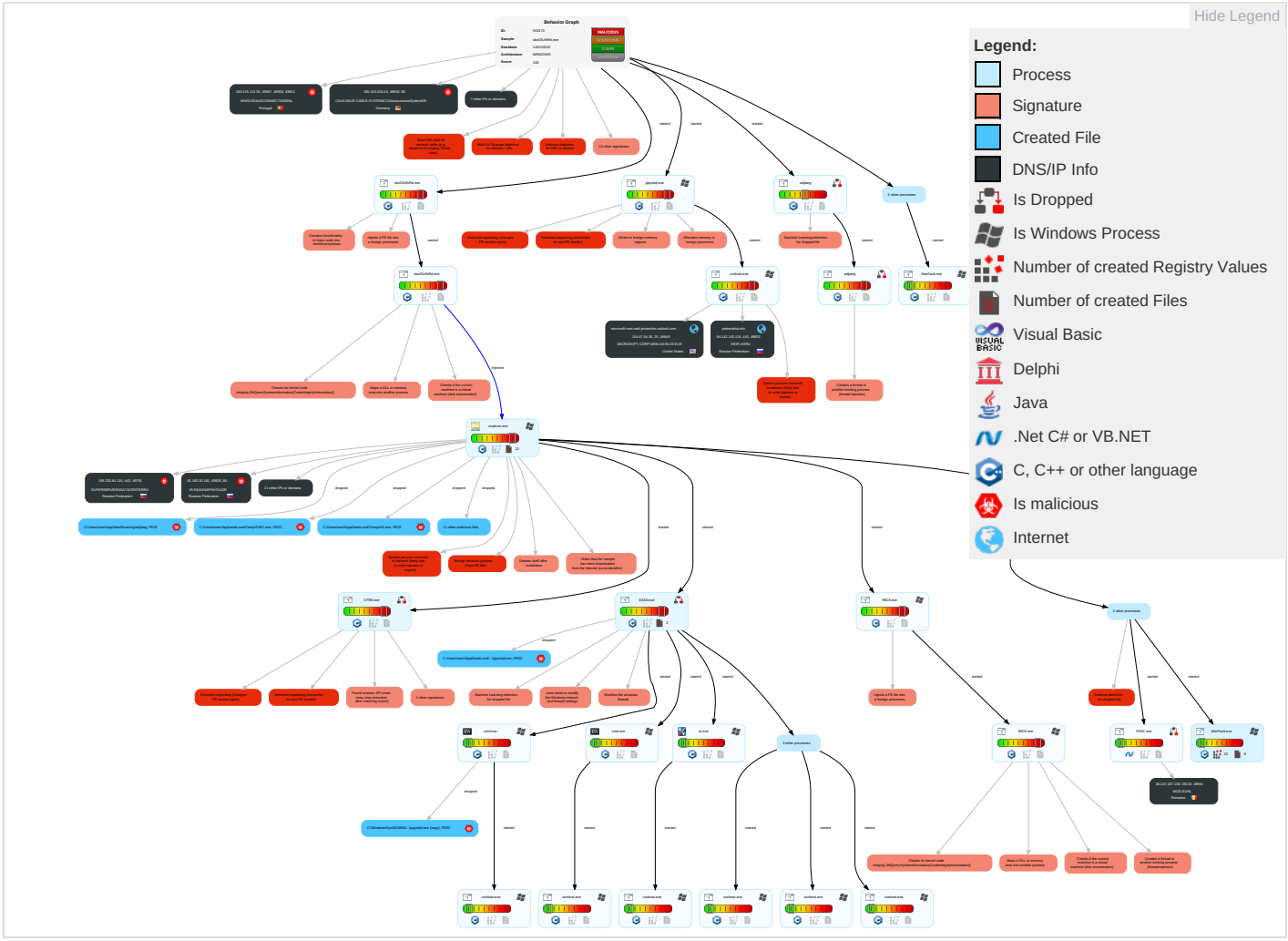
- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- Yara detected Raccoon Stealer
- Yara detected Vidar stealer
- Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts 1	Scripting 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Native API 5 3 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ingress To Transfer 2
Domain Accounts	Exploitation for Client Execution 1	Windows Service 1 4	Access Token Manipulation 1	Scripting 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Encrypted Channel 2
Local Accounts	Command and Scripting Interpreter 3	Logon Script (Mac)	Windows Service 1 4	Obfuscated Files or Information 3	NTDS	System Information Discovery 2 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Standard Port 1
Cloud Accounts	Service Execution 3	Network Logon Script	Process Injection 7 1 3	Software Packing 3 3	LSA Secrets	Security Software Discovery 5 5 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 5

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 3
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Virtualization/Sandbox Evasion 2 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading 1 3 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Valid Accounts 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Proto
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Virtualization/Sandbox Evasion 2 3 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Process Injection 7 1 3	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy
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	Internal Pr

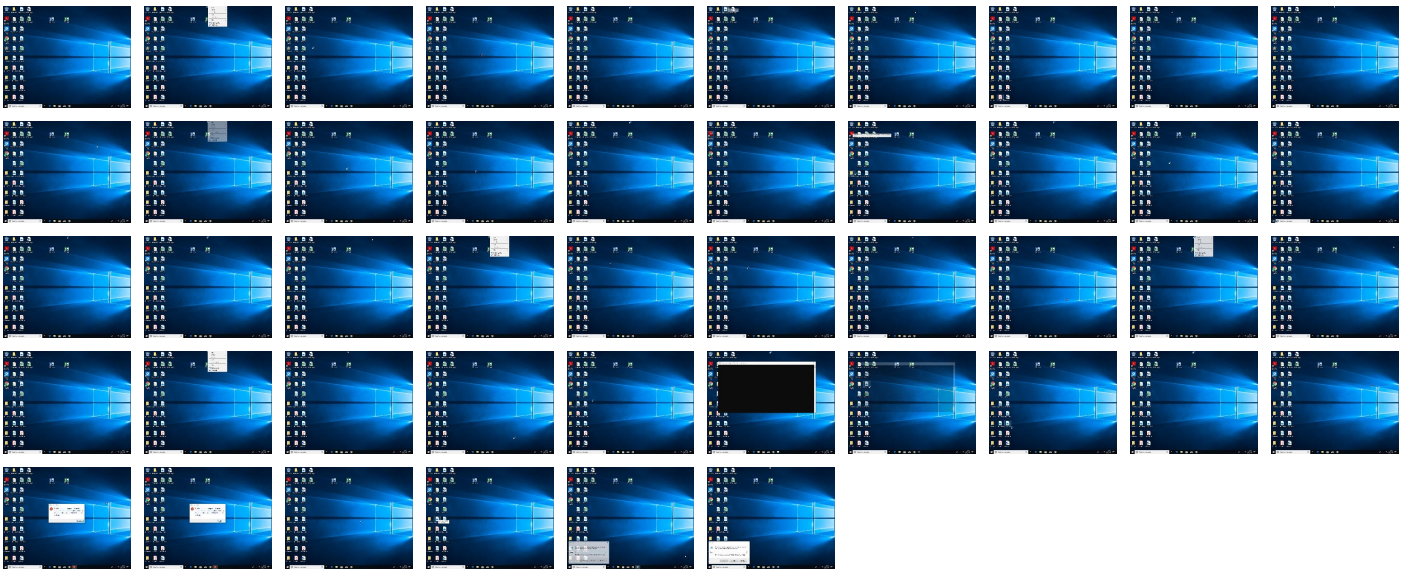
Behavior Graph



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
sbxGIUIhRd.exe	36%	Virustotal		Browse
sbxGIUIhRd.exe	49%	ReversingLabs	Win32.Trojan.Generic	
sbxGIUIhRd.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\gaystiqf.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\FA5C.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\8A6B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\adijaeg	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B3EB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\96DB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CF17.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CFE8.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A15C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\95C6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E2A6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BBBC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7D38.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C487.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\gaystiqf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FA5C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7D38.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7D38.exe	77%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.3.CFE8.exe.650000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
39.2.FA5C.exe.ab0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.2.E2A6.exe.560e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
39.0.FA5C.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
21.0.FA5C.exe.530000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
39.0.FA5C.exe.ab0000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
16.2.95C6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.CFE8.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.sbxGIUIhRd.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.8A6B.exe.590e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
39.0.FA5C.exe.ab0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.0.8A6B.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
39.0.FA5C.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
1.0.sbxGIUIhRd.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
9.2.adijaeg.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.3.svchost.exe.284d000.3.unpack	100%	Avira	TR/Patched.Gen		Download File
1.0.sbxGIUIhRd.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.FA5C.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
35.2.gaystiqf.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.95C6.exe.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.8A6B.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.ab0000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
35.3.gaystiqf.exe.650000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.95C6.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.3.E2A6.exe.580000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.95C6.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
39.0.FA5C.exe.ab0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
0.2.sbxGIUIhRd.exe.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.CFE8.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.8A6B.exe.590e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.FA5C.exe.530000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
10.1.adijaeg.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.sbxGIUIhRd.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.sbxGIUIhRd.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
1.0.sbxGIUIhRd.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
19.2.E2A6.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.2.sbxGIUIhRd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.gaystiqf.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
12.3.8A6B.exe.6f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.adijaeg.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.8A6B.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
16.0.95C6.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
10.0.adijaeg.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.sbxGIUIhRd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.ab0000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
21.0.FA5C.exe.530000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
16.0.95C6.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.ab0000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
38.2.svchost.exe.2360000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.0.sbxGIUIhRd.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
21.0.FA5C.exe.530000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File

Source	Detection	Scanner	Label	Link	Download
16.0.95C6.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
10.0.adijaeg.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.ab0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.2.8A6B.exe.590e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.FA5C.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
16.1.95C6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.gaystiqf.exe.850000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
21.0.FA5C.exe.530000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
39.0.FA5C.exe.ab0000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
38.3.svchost.exe.284d000.4.unpack	100%	Avira	TR/Patched.Gen		Download File
16.0.95C6.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.adijaeg.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.95C6.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/cae3f8ed633c3e67f112fa91bf9f9a15abbe2944	0%	Avira URL Cloud	safe	
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	13%	Virustotal		Browse
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	0%	Avira URL Cloud	safe	
http://185.163.204.24/	4%	Virustotal		Browse
http://185.163.204.24/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://81.163.30.181/1.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18Response	0%	URL Reputation	safe	
http://185.215.113.35/d2VxjasuwS/plugins/cred.dll	100%	Avira URL Cloud	malware	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id3Response	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://185.215.113.35/d2VxjasuwS/index.php	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pool-fr.supportxmr.com	149.202.83.171	true	false		high
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	8.209.70.0	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
patmushta.info	94.142.143.116	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high
privacy-tools-for-you-780.com	8.209.70.0	true	false		high
microsoft-com.mail.protection.outlook.com	104.47.54.36	true	false		high
goo.su	172.67.139.105	true	false		high
transfer.sh	144.76.136.153	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high
pool.supportxmr.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/cae3f8ed633c3e67f112fa91bf9f9a15abbe2944	true	• Avira URL Cloud: safe	unknown
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.163.204.24/	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://81.163.30.181/1.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://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://185.215.113.35/d2VxjasuwS/plugins/cred.dll	true	• Avira URL Cloud: malware	unknown
http://185.215.113.35/d2VxjasuwS/index.php	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.163.45.70	unknown	Moldova Republic of		39798	MIVOCLOUDMD	false
94.142.143.116	patmushta.info	Russian Federation		35196	IHOR-ASRU	false
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
104.47.54.36	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
81.163.30.181	unknown	Russian Federation		58303	IR-RASANAPISHTAZIR	true
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
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:	553170
Start date:	14.01.2022
Start time:	12:27:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sbxGIUIhRd.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@60/26@82/18
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.7% (good quality ratio 18.6%) • Quality average: 57.3% • Quality standard deviation: 40.8%
HCA Information:	• Successful, ratio: 57% • 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
12:29:12	Task Scheduler	Run new task: Firefox Default Browser Agent ADA74C3DB01BEC27 path: C:\Users\user\AppData\Roaming\adijaeg
12:29:26	API Interceptor	1x Sleep call for process: CFE8.exe modified
12:29:33	API Interceptor	8x Sleep call for process: svchost.exe modified
12:29:36	API Interceptor	1x Sleep call for process: WerFault.exe modified
12:30:12	API Interceptor	514x Sleep call for process: mjlooy.exe modified
12:30:12	API Interceptor	3x Sleep call for process: 7D38.exe modified
12:30:14	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
12:30:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe
12:30:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8A6B.exe_27f61c19393a91a6721bfcdfd39195a1563f_168ad717_1a666159\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):	0.814130699743922
Encrypted:	false
SSDEEP:	96:/NFAsohLcQfYOQoJ7R3V6tpXIQcQec6tycEfcw32+HbHg/8BRTf3o8Fa9iVfOyW9:1Ro9cQn8HQ0lLjIq/u7ssS274ltLV
MD5:	BCFAA4F0ABE224C129081104195B208D
SHA1:	7C74E7C498C804E32708117FED56F786144135DB
SHA-256:	571F668A0B47ABB3006EFA67DECA6BDEF2C7B1FEE84F1A834D4E96686EEF2719
SHA-512:	66803D4E9AC9824321022784AF827F1A91E057B2F43D903278798D5C50147FE4B4FB3F61A106B8853A0F60517142F1130A8B31A45FD2AD314DEE230A8F494C68
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.=.1.3.2.8.6.6.3.3.3.6.5.5.7.1.0.5.2.5.....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.=.1.3.2.8.6.6.3.3.3.7.4.9.1.4.8.1.8.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.d.5.3.8.4.4.d.-.6.e.2.3.-.4.8.6.4.-.b.c.9.9.-.8.6.8.6.e.4.7.9.c.c.6.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.f.9.d.5.9.b.3.-.7.a.3.d.-.4.7.a.0.-.8.9.8.a.-.4.a.1.4.a.b.4.9.1.5.b.b.....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.=.8.A.6.B...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.6.8.-.0.0.0.1.-.0.0.1.b.-.3.0.7.d.-.6.a.f.6.3.9.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.d.3.e.8.5.d.f.1.f.9.7.0.7.5.8.a.1.f.b.6.1.3.8.8.5.7.3.8.d.c.a.0.0.0.0.2.9.0.1.!.0.0.0.0.5.9.9.5.a.e.9.d.0.2.4.7.0.3.6.c.c.6.d.3.e.a.7.4.1.e.7.5.0.4.c.9.1.3.f.1.f.b.7.6.!.8.A.6.B...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\WER9E61.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	50272
Entropy (8bit):	3.0513863283023377
Encrypted:	false
SSDEEP:	1536:tTH80y1WUTcM/x/5pPrvVsEv1dGNOJOe72bAMS5p:tTH80y1WUTcM/x/5pPrvVsEv1dGNOJR3
MD5:	2C514D97A71C40AE306F14DC5FE4939D
SHA1:	D54DC9D0B97A9D80856B0B1A2B2B3958F6E93A07
SHA-256:	5EB64B0168ACE1914E6D15E9A486DC733228B3FF67C0A91BD29A64B5F7559E57
SHA-512:	AACBE3B2EF9E6119597E4FEC4DA7D690E6A66704D7E37B32F8E05D56537BAE0A6A0FA0D9C3775549F1BBEA82DD8843EC0C9E1FB4D3FD9E31D769EEC6C2F8A384
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA5A6.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6958459932531285
Encrypted:	false
SSDEEP:	96:9GiZYWqmbloY/YSW48H5YYEZDNt6iCqZSnwOLDaOzegIYzDvIoD3:9jZDqYrjO3a8XIYzMoD3
MD5:	A48C0C244A03917EB506BFC4589E49E6
SHA1:	46D79E4DFCD5E10A83A8D5C0570C8593083697AE
SHA-256:	D2AB6DF46DBA2B199382BAE371ED00789E343881376CCFE37614AE36A19E49CC
SHA-512:	07743E4D06DC669DFAE13CBC81A15E6777751FD33157BFF2551CCE986D5EE22F953586EB0D773F4ED529CF15EE165B28F08530A2D018025C5013A6F7FE0E3D2
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7C.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 11:29:26 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.119750978682941
Encrypted:	false
SSDEEP:	192:KulxjOs+oPOeh0kEHwyhZwqTm8TqsMRhhQRdZ1I/:vGeO9BEoZC/
MD5:	D605C4F70774958E2547E6414FD4A784
SHA1:	4EC2D2615AF2F97C7E6D177B1A415166360DD43C
SHA-256:	5C38CA968F16D2BC4C57EC90E0B3D4563435E21F1ABB8A4C55D8A6943BAB491D
SHA-512:	DE0D5112C7CC04651309A6406040955F27ADA781CB80157935E35E8579FC12AD48B9F7045B7705DB89ED06A4F037A7B83B6965D8D9CFEF9FDF127F8D3DB081A
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....^.a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIn telW.....T.....h....^.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\WERC559.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):	3.70325701546705
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7g6is06Yr8SUp8gmfyRSvpU+pDV89bqlsfYOm:RrlsNiM6y6YQSUygmfyRSvpyq+f4
MD5:	32D09D1ABD420B614246EBA61BA9CFE8
SHA1:	C5F78339CE65139BB7DF356B40A8AF1E9366D46F
SHA-256:	142D5B3FAC8B1F050783F59D8971529DD62F71CC792194CFE041678238A2AD3D
SHA-512:	EB46878449E623A991383FBA000D603EC444E71DFBA0F01BD3A53AEFC529C122C8A234EBEB27AB357C74E692A54118DB7E179ECC651210B83C08AF944989D99
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.6.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC913.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):	4.480601083768932

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC913.tmp.xml	
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9TLWSC8Bg8fm8M4Jt8qFFh+q8vx8ZZ1T/W2d:uITfJo6SN7JLhKQZ1T/W2d
MD5:	A1F7CC4965649E691E2187A3A528262D
SHA1:	90CDD28B76330D7F49F90456526597690D2E8BF2
SHA-256:	F1086A6B524BC2AEBE8AB605F40C7A4EEACF3B94BC3EA1211B955A0B6CCEE28F
SHA-512:	89AEB5281D2AAF618C254F27A34C9CED7A50E8617FB1A880DF30CDA538CF5A700D0BB8D4D7B263D9C86282883203AC77A66C7A0F4B3C9528A714A48344B3C3B
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="1341880" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FA5C.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\FA5C.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\7D38.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....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._.....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text.....`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\8A6B.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

C:\Users\user\AppData\Local\Temp\8A6B.exe

Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i.hG..w.i.Richv.i.....PE..L....b_.....-.....0....@..... .....e..P.....2..... Y..@.....0.....text..... ..`.rdata..D?...0...@..."..... @..@.data...X....p...$...b.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\95C6.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.68963832251392
Encrypted:	false
SSDEEP:	6144:03Oruhy9+2efARaYhqUc9xm1IQgUS1u2NG03OF:aOrm0JRzp0x/QgUp2N6
MD5:	F768F4A81E8B87D6990895A35B8D7D6C
SHA1:	D0E5C1E975EC41E222F99F7A235D85317A1BE3A7
SHA-256:	164149035D4A3D2EDBA76C0601F6F83E04D45D7C057D221130C57FC9B13FD5B5
SHA-512:	004DFFBFCF0F36E6C4A411D3D499F25D8441F98F465D1B8A704CE9E9004D2785604C15F96E33A9761DEFE4AE1454E84BD76DD5CAE1A3658EF14D301FE0B6972
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.....`..... .....@.....'.....T...(.....@.....D..... .text..... ..`.data.....@....zas.....@....give.....@....riyevol.....@....rsrc.....@..@.reloc..XF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\96DB.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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\A15C.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.848593493266229

C:\Users\user\AppData\Local\Temp\A15C.exe

Encrypted:	false
SSDEEP:	6144:v5aWbksiNTBiNg5/dEQECtD2YajndnU4aomwStqUJE0ra7yswH:v5atNTMNg5eQX2BdUcDStq+J4bwH
MD5:	6E7430832C1C24C2BF8BE746F2FE583C
SHA1:	158936951114B6A76D665935AD34F6581556FCDF
SHA-256:	972D533E4DF0786799C0E7C914AA6C04870753C10757C5D58CD874B92A7F4739
SHA-512:	79289323C1104F7483FAC9BF2BCAB5B3804C8F2315C8EDEA9D7C83C8B68B64473122F9B38627169D64A35A960A5F74A3364159CA9CB37B0A2B1BA1B41607A8C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....\.....0....@..... .....lq.....pt..<.....code...~8.....:..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... ....

C:\Users\user\AppData\Local\Temp\B3EB.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3576320
Entropy (8bit):	**7.9976863291960605**
Encrypted:	**true**
SSDEEP:	49152:Y+RSFqeQKgdJee+ntOkgd+TuRCg+687ZEYNFvKfDIcK8nAONaGGh:Yb8eQKg+tOV0T0z875NFKfDPK8nASA
MD5:	5800952B83AECEFC3AA06CCB5B29A4C2
SHA1:	DB51DDBDF8B5B1ABECD6CFAB36514985F357F7A8
SHA-256:	B8BED0211974F32DB2C385350FB62954F0B0F335BC592B51144027956524D674
SHA-512:	2A490708A2C5B742CEB14DE6E2180C4CB606FCCEB5F17DE69249CF532EDC37B984686B534A88AE861CC38471C5892785C26DA68C4F662959542458C583E77E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....!7. .....|.N. .... M..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....x+...P.....@.....1.....@....rsrc..... M.....L0.....@....28gybOo.....N.....1.....@....ada ta.....pS.....6.....@..... .....

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

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

C:\Users\user\AppData\Local\Temp\C487.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

C:\Users\user\AppData\Local\Temp\C487.exe	
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\CF17.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.8500958922173165
Encrypted:	false
SSDEEP:	6144:P5aWbksiNTBQlCuchwPuVbIn97yYUdL6TVrp/LbU7LY6TzeWJwN:P5atNTqlCl84wJyYUpUrLbU9SWJwN
MD5:	FEB8ADD569247306CB0271C907607238
SHA1:	BB9353D602A82FF174AFE7574F4AFD6009E2A8B0
SHA-256:	E7587776ADECF859E137E7AF3DA4B9B6FD9428E6F89CC48D3A63886D490BAACA
SHA-512:	6F650A1D44A11B2205E59DC915E244AC43988C7AC32972280CC5C5CA1ED668B683C2B06F61AEF8D2E91CE1C83FC4E0788207023B6CA81372ACDB4935F040268
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....\.....0....@..... .....lq.....pt..<.....code...~8.....`..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... .....

C:\Users\user\AppData\Local\Temp\CFE8.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	323072
Entropy (8bit):	6.715654310492716
Encrypted:	false
SSDEEP:	6144:LDKNqNHeJZentJavqabB5guxMOgOC9nfpL6P9KJ:LDRNHWsJdKDgXOgOYfpQU
MD5:	E1AF41681888A847863EE17BD63450A0
SHA1:	E03508E1D39121DD0263C5A734C1C6ED0E266AC1
SHA-256:	AEED1BF32DF36AD3CCC929987DBD30E2B1836C267223614D3648B3027E23E1FE
SHA-512:	1E4F8699884B43B06020469AE6BBE94F3744075595DE9EFAF868DD7AB5FB40DE89CF5CADA3E9EA6033F3316D09EA4B9B79837E6C9AD8742436C07FF1B86E65B 1
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....V._.....@.....@.....t...(.....@.....D..... .text..... ..`.data.....@....sutala.....@....buve.....@....bobe.....@....rsrc....."..... .....@..@.reloc..bF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\E2A6.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.689874466366023
Encrypted:	false
SSDEEP:	6144:rwbDZlpg+MKH0e+F4a3TCkh4hXfcAg4SzqHeBcgKl:rUZfgTKH014UBqhEAg4fHe
MD5:	E4B33586BFDB5A9CD45F3038B8F4CCBD

C:\Users\user\AppData\Local\Temp\E2A6.exe	
SHA1:	D9E825FCAB71C80BA1515BEDB40030840837D1B4
SHA-256:	3BB8EF6EAEC03C54C6C517000575EF943577CA0A71E61FD29257786991306133
SHA-512:	3A648A9F056588502191E531AF5BC19E57B802C5B6DB71DA9F6C9CACD4715726E0058D04C5597329338E930AED6B2A5FFD736C779F36CABCB8CAF6D509AEBE B
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.....R.Rich.R..... ..PE..L...-..`.....@.....:=.....(.....@.....D..... text...~..... ..`.data.....@....tojid.....@....vese.....@....fikazap.....@....rsrc..... .....@..@.reloc..XF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\FA5C.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\gaystiqf.exe	
Process:	C:\Users\user\AppData\Local\Temp\E2A6.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12005888
Entropy (8bit):	3.8030917940266584
Encrypted:	false
SSDEEP:	6144:pwbDZlpg+MKH0e+F4a3TCkh4hXfcAg4SzqHeBcgKlClClClClClClClClClClCl8:pUZfgTKH014UBqhEAg4fHe
MD5:	6D07EFE4270BD10431D8E32CADCFF4E7
SHA1:	AD08F50151D2F7587196092F97BB24BB696C3084
SHA-256:	24762737036178 70AE392F166BC07D346596D23A159BF762FD5468844B70E33F
SHA-512:	03E36F3E9821FB681436A6ED381FB0E03B0EE1DEC5E7EDD27A5A3A3289A9D6EA896CD61F7E7BC355D4E2D34B200F50BC5CEDB36BE02BBDF5C781CC49B77C D38
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.....R.Rich.R..... ..PE..L...-..`.....@.....:=.....(.....@.....D..... text...~..... ..`.data.....@....tojid.....@....vese.....@....fikazap.....@....rsrc..... .....@..@.reloc..XF.....@..B..... .....

C:\Users\user\AppData\Roaming\adijaeg	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.68963832251392
Encrypted:	false
SSDEEP:	6144:03Oruhy9+2efARaYhqUc9xm1IQgUS1u2NG03OF:aOrm0JRzp0x/QgUp2N6

C:\Users\user\AppData\Roaming\adijaeg	
MD5:	F768F4A81E8B87D6990895A35B8D7D6C
SHA1:	D0E5C1E975EC41E222F99F7A235D85317A1BE3A7
SHA-256:	164149035D4A3D2EDBA76C0601F6F83E04D45D7C057D221130C57FC9B13FD5B5
SHA-512:	004DFFBFCF0F36E6C4A411D3D499F25D8441F98F465D1B8A704CE9E9004D2785604C15F96E33A9761DEFE4AE1454E84BD76DD5CAE1A3658EF14D301FE0B6972
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.....R.Rich.R..... ..PE..L.....`..... .....@.....'.....T...(.....@.....D..... .text..... ..`.data.....@....zas.....@....give.....@....riyevol.....@....rsrc.....@..@ .reloc..XF.....H.....@..B..... .....

C:\Users\user\AppData\Roaming\adijaeg: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\txlhcyih\gaystiqf.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12005888
Entropy (8bit):	3.8030917940266584
Encrypted:	false
SSDEEP:	6144:pwbDZlpg+MKH0e+F4a3TCkh4hXfcAg4SzqHeBcgKlClClClClClClClClClClCl8:pUZfgTKH014UBqhEAg4fHe
MD5:	6D07EFE4270BD10431D8E32CADCFF4E7
SHA1:	AD08F50151D2F7587196092F97BB24BB696C3084
SHA-256:	2476273703617870AE392F166BC07D346596D23A159BF762FD5468844B70E33F
SHA-512:	03E36F3E9821FB681436A6ED381FB0E03B0EE1DEC5E7EDD27A5A3A3289A9D6EA896CD61F7E7BC355D4E2D34B200F50BC5CEDB36BE02BBDF5C781CC49B77C D38
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.....R.Rich.R..... ..PE..L...-..`.....@.....:=.....(.....@.....D..... text...~..... ..`.data.....@....tojid.....@....vese.....@....fikazap.....@....rsrc..... .....@..@.reloc..XF.....@..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):	4.23827032270778
Encrypted:	false
SSDEEP:	12288:VH9yhjdQZT0wNxPwkQ9LLFQQvolLhLg0/+8K7vGneigAgc8O:V9yhjdQZT0CxPwJJv
MD5:	B057F97299DBE5E945EEF8754F5D4597
SHA1:	C6230D218779F120F9911265D4D3BE4C8D753618
SHA-256:	286C246A52C29E67BA99172CCB226A45CF05253EE28354730FE94FCB6F8D203A
SHA-512:	74ACDC737EFB2B39C740F422202E9392F956790398E9C3EC35B00A8BCCE0021D75F834C029D88DA82E13F6983BFB50E8850DA397CBF7E6889C48738CBE047F8
Malicious:	false
Reputation:	unknown

C:\Windows\appcompat\Programs\Amcache.hve	
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./..9..... ....

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):	3.3475884053493443
Encrypted:	false
SSDEEP:	384:hLz5K5vRv4KgnVVeeDze31NKZtjfT8GRwU3AsPzM8i:9NKPg/eeDzelNYtjoGRwURM8
MD5:	A5E06A1D69185A2B857B67E5B04572E8
SHA1:	85572781BB9F1FCF67A9FCC48147B01F9D022CF9
SHA-256:	361D01FAB30CC588055ACC3204B221A57029A22C9E796F38FB98A2EF7FAAB011
SHA-512:	249EE970D19B9CFDEF7BFD65A660C187723B3E6B5813542B33D8A8B18757B4169F5E1918F24A5D83B8D1E1839481AF7A3F1E46D65CB60A582F88A87CFC2CC1A
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./..9..... ....HvLE.N.....G.....x...'.,.~..... ..hbin.....p.\..,.....nk,....9.....x..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ....9..... ....Z.....Root.....lf.....Root....nk ....9..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBIlydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8
SHA-512:	48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090F
Malicious:	false
Reputation:	unknown
Preview:	..A specified value is not valid.....Usage: add rule name=<string>.. dir=in|out.. action=allow|block|bypass.. [program=<program path>].. [service=<service short name>|any].. [description=<string>].. [enable=yes|no (default=yes)].. [profile=public|private|domain|any[,...]].. [localip=any|<IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [localport=0-65535|<port range>[,...]|RPC|RPC-EPMap|IPHTTPS|any (default=any)].. [remoteport=0-65535|<port range>[,...]|any (default=any)].. [protocol=0-255|icmpv4|icmpv6|icmpv4:type,code|icmpv6:type,code|.. tcp|udp|any (default=any)].. [interfacetype=wireless|lan|ras|any].. [rmtcomputergrp=<SDDL string>].. [rmtusrgrp=<SDDL string>].. [edge=yes|deferapp|deferuser|no (default=no)].. [security=authenticate|authenc|authdynenc|authnoencap|

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.68963832251392
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:	sbxGIUIhRd.exe
File size:	320000
MD5:	f768f4a81e8b87d6990895a35b8d7d6c
SHA1:	d0e5c1e975ec41e222f99f7a235d85317a1be3a7
SHA256:	164149035d4a3d2edba76c0601f6f83e04d45d7c057d221 130c57fc9b13fd5b5

General

SHA512:	004dffbfcf0f36e6c4a411d3d499f25d8441f98f465d1b8a704ce9e9004d2785604c15f96e33a9761defe4ae1454e84bd76dd5cae1a3658ef14d301fe0b69720
SSDEEP:	6144:03Oruhy9+2efARaYhqUc9xm1lQgUS1u2NG03OF:aOrm0JRzp0x/QgUp2N6
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.....`.....

File Icon

Icon Hash:	c8d0d8e0f8e0f0e8

Static PE Info

General

Entrypoint:	0x41b620
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x60CC14F0 [Fri Jun 18 03:37:20 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:	64f7fef844b1e4fdfabf9d9b629075a0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e6ce	0x3e800	False	0.582125	data	6.96344242356	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.340657552083	data	3.46395750767	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.zas	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.give	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.riyevol	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	0.597271543561	data	5.82672582834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x4658	0x4800	False	0.346462673611	data	3.68432452042	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 12:29:11.782485008 CET	192.168.2.4	8.8.8.8	0x67b5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:11.963017941 CET	192.168.2.4	8.8.8.8	0xe986	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:12.430608034 CET	192.168.2.4	8.8.8.8	0x5bf4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:12.606929064 CET	192.168.2.4	8.8.8.8	0x4112	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:13.093177080 CET	192.168.2.4	8.8.8.8	0xc21b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:13.564027071 CET	192.168.2.4	8.8.8.8	0x8bf6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:14.948347092 CET	192.168.2.4	8.8.8.8	0xa91d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:15.427823067 CET	192.168.2.4	8.8.8.8	0xc66a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:15.594754934 CET	192.168.2.4	8.8.8.8	0xad10	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:17.681981087 CET	192.168.2.4	8.8.8.8	0xd6ae	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:17.868205070 CET	192.168.2.4	8.8.8.8	0xd89a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:18.034226894 CET	192.168.2.4	8.8.8.8	0x5ee7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:18.336664915 CET	192.168.2.4	8.8.8.8	0x54cb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:18.505330086 CET	192.168.2.4	8.8.8.8	0x89d2	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:20.346779108 CET	192.168.2.4	8.8.8.8	0x6d1f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:20.801031113 CET	192.168.2.4	8.8.8.8	0x68bb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:20.967899084 CET	192.168.2.4	8.8.8.8	0x3931	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.120146990 CET	192.168.2.4	8.8.8.8	0x1d8b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.315474033 CET	192.168.2.4	8.8.8.8	0x44e5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.504046917 CET	192.168.2.4	8.8.8.8	0x25c0	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 12:29:21.694421053 CET	192.168.2.4	8.8.8.8	0x639b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:22.180890083 CET	192.168.2.4	8.8.8.8	0x33a6	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:25.771519899 CET	192.168.2.4	8.8.8.8	0xed2c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:25.937843084 CET	192.168.2.4	8.8.8.8	0x2715	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:26.102307081 CET	192.168.2.4	8.8.8.8	0x143d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:26.315789938 CET	192.168.2.4	8.8.8.8	0x734e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.117929935 CET	192.168.2.4	8.8.8.8	0x33ca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.293498993 CET	192.168.2.4	8.8.8.8	0xdcf4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.473170996 CET	192.168.2.4	8.8.8.8	0xd6f7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.656965017 CET	192.168.2.4	8.8.8.8	0xb971	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:31.224777937 CET	192.168.2.4	8.8.8.8	0x521d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:31.394221067 CET	192.168.2.4	8.8.8.8	0x49bf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:31.562335968 CET	192.168.2.4	8.8.8.8	0x2eb3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.890839100 CET	192.168.2.4	8.8.8.8	0x87cb	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:44.528678894 CET	192.168.2.4	8.8.8.8	0x1a68	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.201407909 CET	192.168.2.4	8.8.8.8	0xdaf0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.367465973 CET	192.168.2.4	8.8.8.8	0x5b4c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.557280064 CET	192.168.2.4	8.8.8.8	0x4a7c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.736764908 CET	192.168.2.4	8.8.8.8	0x9d7e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.901665926 CET	192.168.2.4	8.8.8.8	0x17ca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.067249060 CET	192.168.2.4	8.8.8.8	0xb79f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.283118010 CET	192.168.2.4	8.8.8.8	0x5c2f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.452543020 CET	192.168.2.4	8.8.8.8	0x3d2f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.619712114 CET	192.168.2.4	8.8.8.8	0x4f2b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.798546076 CET	192.168.2.4	8.8.8.8	0x4e70	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.966861963 CET	192.168.2.4	8.8.8.8	0x25a4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:55.145189047 CET	192.168.2.4	8.8.8.8	0x8dcc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:55.398905993 CET	192.168.2.4	8.8.8.8	0xff6a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:55.566248894 CET	192.168.2.4	8.8.8.8	0xa5df	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.441070080 CET	192.168.2.4	8.8.8.8	0x648d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.609729052 CET	192.168.2.4	8.8.8.8	0xd308	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.783494949 CET	192.168.2.4	8.8.8.8	0x8226	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:59.128232002 CET	192.168.2.4	8.8.8.8	0x8d36	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:59.305922985 CET	192.168.2.4	8.8.8.8	0xb0	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:59.700192928 CET	192.168.2.4	8.8.8.8	0xf035	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:00.035913944 CET	192.168.2.4	8.8.8.8	0xb9a8	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 12:30:00.674380064 CET	192.168.2.4	8.8.8.8	0x336	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:00.959358931 CET	192.168.2.4	8.8.8.8	0x61e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:01.321439981 CET	192.168.2.4	8.8.8.8	0xf3f6	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:04.139807940 CET	192.168.2.4	8.8.8.8	0x82ed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:04.312947989 CET	192.168.2.4	8.8.8.8	0x43d2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:04.526979923 CET	192.168.2.4	8.8.8.8	0x4cb4	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.377934933 CET	192.168.2.4	8.8.8.8	0x7c19	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.559844971 CET	192.168.2.4	8.8.8.8	0x3d62	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.735255957 CET	192.168.2.4	8.8.8.8	0x7946	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.912570953 CET	192.168.2.4	8.8.8.8	0x5623	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:08.140345097 CET	192.168.2.4	8.8.8.8	0x598	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:11.223495007 CET	192.168.2.4	8.8.8.8	0xfd8c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:11.397445917 CET	192.168.2.4	8.8.8.8	0x30ac	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:11.563966036 CET	192.168.2.4	8.8.8.8	0x5efb	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:13.492192030 CET	192.168.2.4	8.8.8.8	0xf3c6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:13.665873051 CET	192.168.2.4	8.8.8.8	0xbbfe	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:13.852792025 CET	192.168.2.4	8.8.8.8	0xfa1f	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:15.926599026 CET	192.168.2.4	8.8.8.8	0xe24a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:16.141427994 CET	192.168.2.4	8.8.8.8	0xa604	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:21.652688026 CET	192.168.2.4	8.8.8.8	0x8116	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:21.847970009 CET	192.168.2.4	8.8.8.8	0x6d9b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:22.201057911 CET	192.168.2.4	8.8.8.8	0x510	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:25.474335909 CET	192.168.2.4	8.8.8.8	0xb7b6	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:48.699079037 CET	192.168.2.4	8.8.8.8	0xab12	Standard query (0)	pool.supportxmr.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:16.120827913 CET	192.168.2.4	8.8.8.8	0x58e1	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.487710953 CET	192.168.2.4	8.8.8.8	0xdeb8	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:29:11.800079107 CET	8.8.8.8	192.168.2.4	0x67b5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:12.274777889 CET	8.8.8.8	192.168.2.4	0xe986	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:12.450135946 CET	8.8.8.8	192.168.2.4	0x5bf4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:12.944006920 CET	8.8.8.8	192.168.2.4	0x4112	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:13.409914970 CET	8.8.8.8	192.168.2.4	0xc21b	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 12:29:13.583471060 CET	8.8.8.8	192.168.2.4	0x8bf6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:15.262034893 CET	8.8.8.8	192.168.2.4	0xa91d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:15.447199106 CET	8.8.8.8	192.168.2.4	0xc66a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:15.881325006 CET	8.8.8.8	192.168.2.4	0xad10	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:17.699449062 CET	8.8.8.8	192.168.2.4	0xd6ae	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:17.887447119 CET	8.8.8.8	192.168.2.4	0xd89a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:18.053019047 CET	8.8.8.8	192.168.2.4	0x5ee7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:18.355922937 CET	8.8.8.8	192.168.2.4	0x54cb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:18.790898085 CET	8.8.8.8	192.168.2.4	0x89d2	No error (0)	privacy-tools-for-you-780.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:20.656292915 CET	8.8.8.8	192.168.2.4	0x6d1f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:20.820332050 CET	8.8.8.8	192.168.2.4	0x68bb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.072279930 CET	8.8.8.8	192.168.2.4	0x3931	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.139534950 CET	8.8.8.8	192.168.2.4	0x1d8b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.334872007 CET	8.8.8.8	192.168.2.4	0x44e5	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.523125887 CET	8.8.8.8	192.168.2.4	0x25c0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:21.983006954 CET	8.8.8.8	192.168.2.4	0x639b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:22.472062111 CET	8.8.8.8	192.168.2.4	0x33a6	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:25.790760994 CET	8.8.8.8	192.168.2.4	0xed2c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:25.954900026 CET	8.8.8.8	192.168.2.4	0x2715	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:26.121053934 CET	8.8.8.8	192.168.2.4	0x143d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:26.332964897 CET	8.8.8.8	192.168.2.4	0x734e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.135415077 CET	8.8.8.8	192.168.2.4	0x33ca	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.312202930 CET	8.8.8.8	192.168.2.4	0xdcf4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.490415096 CET	8.8.8.8	192.168.2.4	0xd6f7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.678015947 CET	8.8.8.8	192.168.2.4	0xb971	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.678015947 CET	8.8.8.8	192.168.2.4	0xb971	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:29:29.678015947 CET	8.8.8.8	192.168.2.4	0xb971	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.678015947 CET	8.8.8.8	192.168.2.4	0xb971	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:29.678015947 CET	8.8.8.8	192.168.2.4	0xb971	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:31.244934082 CET	8.8.8.8	192.168.2.4	0x521d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:31.414046049 CET	8.8.8.8	192.168.2.4	0x49bf	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:31.582149982 CET	8.8.8.8	192.168.2.4	0x2eb3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.910156012 CET	8.8.8.8	192.168.2.4	0x87cb	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.910156012 CET	8.8.8.8	192.168.2.4	0x87cb	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.910156012 CET	8.8.8.8	192.168.2.4	0x87cb	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.910156012 CET	8.8.8.8	192.168.2.4	0x87cb	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.910156012 CET	8.8.8.8	192.168.2.4	0x87cb	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:41.910156012 CET	8.8.8.8	192.168.2.4	0x87cb	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:44.645194054 CET	8.8.8.8	192.168.2.4	0x1a68	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.220798969 CET	8.8.8.8	192.168.2.4	0xdaf0	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.386814117 CET	8.8.8.8	192.168.2.4	0x5b4c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.576463938 CET	8.8.8.8	192.168.2.4	0x4a7c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.755656958 CET	8.8.8.8	192.168.2.4	0x9d7e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:53.921154976 CET	8.8.8.8	192.168.2.4	0x17ca	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.085957050 CET	8.8.8.8	192.168.2.4	0xb79f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.302371979 CET	8.8.8.8	192.168.2.4	0x5c2f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.472028971 CET	8.8.8.8	192.168.2.4	0x3d2f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.636883974 CET	8.8.8.8	192.168.2.4	0x4f2b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.817362070 CET	8.8.8.8	192.168.2.4	0x4e70	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:54.985551119 CET	8.8.8.8	192.168.2.4	0x25a4	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 12:29:55.164411068 CET	8.8.8.8	192.168.2.4	0x8dcc	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:55.418090105 CET	8.8.8.8	192.168.2.4	0xff6a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:55.585751057 CET	8.8.8.8	192.168.2.4	0xa5df	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.460091114 CET	8.8.8.8	192.168.2.4	0x648d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.626797915 CET	8.8.8.8	192.168.2.4	0xd308	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.808177948 CET	8.8.8.8	192.168.2.4	0x8226	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:58.808177948 CET	8.8.8.8	192.168.2.4	0x8226	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:59.145658016 CET	8.8.8.8	192.168.2.4	0x8d36	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:59.324620008 CET	8.8.8.8	192.168.2.4	0xb0	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 12:29:59.719247103 CET	8.8.8.8	192.168.2.4	0xf035	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:00.052918911 CET	8.8.8.8	192.168.2.4	0xb9a8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:00.694416046 CET	8.8.8.8	192.168.2.4	0x336	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:00.978961945 CET	8.8.8.8	192.168.2.4	0x61e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:01.340497971 CET	8.8.8.8	192.168.2.4	0xf3f6	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:04.158957005 CET	8.8.8.8	192.168.2.4	0x82ed	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:04.332336903 CET	8.8.8.8	192.168.2.4	0x43d2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:04.546641111 CET	8.8.8.8	192.168.2.4	0x4cb4	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.397336960 CET	8.8.8.8	192.168.2.4	0x7c19	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.579046965 CET	8.8.8.8	192.168.2.4	0x3d62	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.752860069 CET	8.8.8.8	192.168.2.4	0x7946	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:07.931826115 CET	8.8.8.8	192.168.2.4	0x5623	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:08.159605980 CET	8.8.8.8	192.168.2.4	0x598	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:11.243046999 CET	8.8.8.8	192.168.2.4	0xfd8c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:11.420278072 CET	8.8.8.8	192.168.2.4	0x30ac	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:11.583112955 CET	8.8.8.8	192.168.2.4	0x5efb	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:13.512223959 CET	8.8.8.8	192.168.2.4	0xf3c6	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 12:30:13.683284044 CET	8.8.8.8	192.168.2.4	0xbbfe	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:13.870006084 CET	8.8.8.8	192.168.2.4	0xfa1f	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:15.946022034 CET	8.8.8.8	192.168.2.4	0xe24a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:16.161323071 CET	8.8.8.8	192.168.2.4	0xa604	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:21.675123930 CET	8.8.8.8	192.168.2.4	0x8116	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:21.865549088 CET	8.8.8.8	192.168.2.4	0x6d9b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:22.220680952 CET	8.8.8.8	192.168.2.4	0x510	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:25.792366028 CET	8.8.8.8	192.168.2.4	0xb7b6	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:48.718033075 CET	8.8.8.8	192.168.2.4	0xab12	No error (0)	pool.supportxmr.com	pool-fr.supportxmr.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:30:48.718033075 CET	8.8.8.8	192.168.2.4	0xab12	No error (0)	pool-fr.supportxmr.com		149.202.83.171	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:48.718033075 CET	8.8.8.8	192.168.2.4	0xab12	No error (0)	pool-fr.supportxmr.com		91.121.140.167	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:48.718033075 CET	8.8.8.8	192.168.2.4	0xab12	No error (0)	pool-fr.supportxmr.com		37.187.95.110	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:48.718033075 CET	8.8.8.8	192.168.2.4	0xab12	No error (0)	pool-fr.supportxmr.com		94.23.23.52	A (IP address)	IN (0x0001)
Jan 14, 2022 12:30:48.718033075 CET	8.8.8.8	192.168.2.4	0xab12	No error (0)	pool-fr.supportxmr.com		94.23.247.226	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:16.139516115 CET	8.8.8.8	192.168.2.4	0x58e1	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.621751070 CET	8.8.8.8	192.168.2.4	0xdeb8	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.621751070 CET	8.8.8.8	192.168.2.4	0xdeb8	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.621751070 CET	8.8.8.8	192.168.2.4	0xdeb8	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.621751070 CET	8.8.8.8	192.168.2.4	0xdeb8	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.621751070 CET	8.8.8.8	192.168.2.4	0xdeb8	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 12:31:38.621751070 CET	8.8.8.8	192.168.2.4	0xdeb8	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- rrooukv.org
  - host-data-coin-11.com
- rxyqqf.net

- dutgomfkc.net
- qwfulsm.net
- rxkloxn.com
- hopcq.com
- ocnbwlevej.org
- gdffxf.org
- data-host-coin-8.com
- psgcnvvm.org
- vxjxd.org
- mpabshq.org
- ubyvpwxipt.net
- privacy-tools-for-you-780.com
- pxnotaacu.org
- lnpyohcdyx.com
- unicupload.top
- byfupx.org
- iijrpdo.org
- ntsddipn.org
- vkaflekmve.net
- seaed.com
- obclg.net
- pgydqikexd.org
- gminomh.net
- 185.7.214.171:8080
- tgajiadc.net
- xvuvc.org
- tdosgx.net
- npqwstsduq.net
- ouyysee.net
- rtqpowrk.org

- hhpljg.org
- ipycpcfbe.com
- sdstpsloir.org
- tfxyjpgh.net
- ycdbyxqt.net
- gcfxlgitg.org
- afdvsashlg.com
- kapjpsnnjq.org
- kcsjausffk.com
- djmmsjo.net
- ipjoaoftf.net
- sdkmuxkbh.org
- vomuxg.org
- fjenisnthl.net
- pixmwg.net
- mwbuboe.net
- pylkam.org
- fdhqx.net
- pslqekdvh.org
- ecicwppql.net
- tlwsaw.net
- krrkfa.com
- gfydmobm.net
- uhdak.net
- assuf.net
- rblisqqaii.com
- xnvwvqck.com
- vltihla.com
- qnqlcbx.com
- 185.215.113.35

- flqhri.com
- poqgfb.net
- oycnsawak.org
- 81.163.30.181
- 185.163.204.22
- 185.163.204.24
- ylanbcfwv.net
- yxorycdxma.net
- tcqdnx.net

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: sbxGIUIhRd.exe PID: 6964 Parent PID: 5836

General

Start time:	12:28:30
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\sbxGIUIhRd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\sbxGIUIhRd.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	F768F4A81E8B87D6990895A35B8D7D6C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: sbxGIUIhRd.exe PID: 6984 Parent PID: 6964

General

Start time:	12:28:31
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\sbxGIUIhRd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\sbxGIUIhRd.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	F768F4A81E8B87D6990895A35B8D7D6C
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: 00000001.00000002.719013921.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.719027443.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 6984

General

Start time:	12:28:38
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: 00000005.00000000.706607181.0000000004DC1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6228 Parent PID: 568

General

Start time:	12:28:40
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: 5420 Parent PID: 568

General

Start time:	12:29:00
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: adijaeg PID: 6604 Parent PID: 968

General

Start time:	12:29:12
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\adijaeg
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\adijaeg
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	F768F4A81E8B87D6990895A35B8D7D6C
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: adijaeg PID: 4204 Parent PID: 6604

General

Start time:	12:29:14
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\adijaeg
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\adijaeg
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	F768F4A81E8B87D6990895A35B8D7D6C
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.00000002.767064606.0000000000561000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000A.00000002.766964771.0000000000420000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 6976 Parent PID: 568

General

Start time:	12:29:15
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: 8A6B.exe PID: 6760 Parent PID: 3424

General

Start time:	12:29:16
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8A6B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8A6B.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	moderate

Analysis Process: 95C6.exe PID: 6844 Parent PID: 3424

General

Start time:	12:29:18
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\95C6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\95C6.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	F768F4A81E8B87D6990895A35B8D7D6C
Has elevated privileges:	true
Has administrator privileges:	true

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

Analysis Process: svchost.exe PID: 6868 Parent PID: 568

General

Start time:	12:29:19
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: 6924 Parent PID: 6868

General

Start time:	12:29:19
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 6760 -ip 6760
Imagebase:	0x1160000
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: 95C6.exe PID: 6804 Parent PID: 6844

General

Start time:	12:29:20
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\95C6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\95C6.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	F768F4A81E8B87D6990895A35B8D7D6C
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: 00000010.00000002.787707490.0000000002051000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000010.00000002.787566424.0000000002030000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 6812 Parent PID: 6760

General

Start time:	12:29:21
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6760 -s 520
Imagebase:	0x1160000
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: CFE8.exe PID: 4296 Parent PID: 3424

General

Start time:	12:29:22
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\CFE8.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CFE8.exe
Imagebase:	0x400000
File size:	323072 bytes
MD5 hash:	E1AF41681888A847863EE17BD63450A0
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: 00000012.00000002.778871372.0000000000873000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000012.00000002.778871372.0000000000873000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Reputation:	low

Analysis Process: E2A6.exe PID: 4752 Parent PID: 3424

General

Start time:	12:29:27
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E2A6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E2A6.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	E4B33586BFDB5A9CD45F3038B8F4CCBD
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: 00000013.00000002.803426452.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000013.00000003.785124178.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000013.00000002.803137475.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: FA5C.exe PID: 796 Parent PID: 3424

General

Start time:	12:29:29
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\FA5C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\FA5C.exe
Imagebase:	0x530000
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: 00000015.00000002.833273258.0000000003971000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: svchost.exe PID: 4800 Parent PID: 568

General

Start time:	12:29:30
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5768 Parent PID: 4752

General

Start time:	12:29:32
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\txlhcyih\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5152 Parent PID: 5768

General

Start time:	12:29:32
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: 4692 Parent PID: 4752

General

Start time:	12:29:33
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\gaystiqf.exe" C:\Windows\SysWOW64\txlhcyih\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6316 Parent PID: 4692

General

Start time:	12:29:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	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: 4044 Parent PID: 4752

General

Start time:	12:29:34
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create txlhcyih binPath= "C:\Windows\SysWOW64\txlhcyih\gaystiqf.exe /d\"C:\Users\user\AppData\Local\Temp\E2A6.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x20000
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: 2860 Parent PID: 4044

General

Start time:	12:29:34
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: 240 Parent PID: 4752

General

Start time:	12:29:35
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description txlhcyih "wifi internet conection
Imagebase:	0x20000
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: 6480 Parent PID: 240

General

Start time:	12:29:36
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: 1740 Parent PID: 4752

General

Start time:	12:29:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start txlhcyih
Imagebase:	0x20000
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: 2216 Parent PID: 1740

General

Start time:	12:29:37
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: netsh.exe PID: 6536 Parent PID: 4752

General

Start time:	12:29:37
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:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: gaystiqf.exe PID: 4588 Parent PID: 568

General

Start time:	12:29:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\txlhcyih\gaystiqf.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\txlhcyih\gaystiqf.exe /d"C:\Users\user\AppData\Local\Temp\E2A6.exe"
Imagebase:	0x400000
File size:	12005888 bytes
MD5 hash:	6D07EFE4270BD10431D8E32CADCFF4E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000023.00000002.809196350.0000000000630000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000023.00000003.805779040.0000000000650000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000023.00000002.808208197.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000023.00000002.809631719.0000000000850000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4620 Parent PID: 6536

General

Start time:	12:29:38
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: 5288 Parent PID: 4588

General

Start time:	12:29:39
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0x110000
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: 00000026.00000002.979557466.0000000002360000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: FA5C.exe PID: 1496 Parent PID: 796

General

Start time:	12:29:43
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\FA5C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\FA5C.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: 00000027.00000002.933081162.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.824314083.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.824767570.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.823843288.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.825252840.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis