ID: 552870
Sample Name:
emPJndhuvA.exe
Cookbook: default.jbs
Time: 20:48:33
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

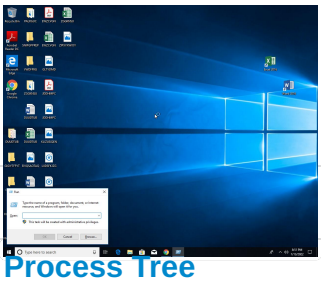
Windows Analysis Report emPJndhuvA.exe

Overview

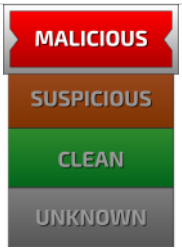
General Information

Sample Name:	emPJndhuvA.exe
Analysis ID:	552870
MD5:	a7444553f8a8fe2..
SHA1:	f6d3d6ccf728ae7..
SHA256:	ba5303301925a8..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



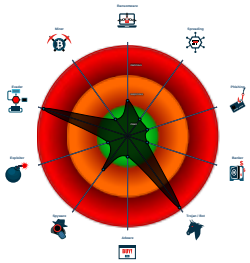
Amadey RedLine SmokeLoader Tofsee Vidar

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- emPJndhuvA.exe (PID: 3352 cmdline: "C:\Users\user\Desktop\emPJndhuvA.exe" MD5: A7444553F8A8FE2702B6FD48008D6605)
  - emPJndhuvA.exe (PID: 4160 cmdline: "C:\Users\user\Desktop\emPJndhuvA.exe" MD5: A7444553F8A8FE2702B6FD48008D6605)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 2819.exe (PID: 3104 cmdline: C:\Users\user\AppData\Local\Temp\2819.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 5956 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3104 -s 540 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 3D67.exe (PID: 5276 cmdline: C:\Users\user\AppData\Local\Temp\3D67.exe MD5: BB0BA8D31F37E6B9F683EBD9044F1A85)
        - 3D67.exe (PID: 4968 cmdline: C:\Users\user\AppData\Local\Temp\3D67.exe MD5: BB0BA8D31F37E6B9F683EBD9044F1A85)
      - FD2B.exe (PID: 468 cmdline: C:\Users\user\AppData\Local\Temp\FD2B.exe MD5: CEBAF005081C730D4AC7A87E46B440D0)
      - 952.exe (PID: 1068 cmdline: C:\Users\user\AppData\Local\Temp\952.exe MD5: 4C29CFD658E015FA4DB5A2454F103D4A)
        - cmd.exe (PID: 4356 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\bhlprady\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6248 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\vodibdaj.exe" C:\Windows\SysWOW64\bhlprady\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6304 cmdline: C:\Windows\System32\sc.exe" create bhlprady binPath= "C:\Windows\SysWOW64\bhlprady\vodibdaj.exe /d\"C:\Users\user\AppData\Local\Temp\952.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6372 cmdline: C:\Windows\System32\sc.exe" description bhlprady "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6412 cmdline: "C:\Windows\System32\sc.exe" start bhlprady MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 6460 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: 6492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 13E2.exe (PID: 2316 cmdline: C:\Users\user\AppData\Local\Temp\13E2.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 13E2.exe (PID: 6652 cmdline: C:\Users\user\AppData\Local\Temp\13E2.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 4372 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4596 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4400 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5784 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5400 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5056 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 2872 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5796 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3540 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6628 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 1280 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- tiftjuh (PID: 4892 cmdline: C:\Users\user\AppData\Roaming\tiftjuh MD5: A7444553F8A8FE2702B6FD48008D6605)
  - tiftjuh (PID: 5816 cmdline: C:\Users\user\AppData\Roaming\tiftjuh MD5: A7444553F8A8FE2702B6FD48008D6605)
- svchost.exe (PID: 5208 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5736 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 3104 -ip 3104 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- vodibdaj.exe (PID: 6484 cmdline: C:\Windows\SysWOW64\bhlprady\vodibdaj.exe /d"C:\Users\user\AppData\Local\Temp\952.exe" MD5: E331BE085840751FF0AC8DCBCDC5F5E3)
  - svchost.exe (PID: 6580 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **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
00000001.00000002.310069625.0000000001F51000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
0000001C.00000002.386280466.0000000001F30000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000020.00000002.447751764.000000000402000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000001C.00000002.386498287.000000000243000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000001E.00000002.412229320.000000000058000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.emPJndhuvA.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
21.0.tiftjuh.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
21.0.tiftjuh.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
21.2.tiftjuh.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
32.2.13E2.exe.413f910.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 19 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:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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

Persistence and Installation Behavior:

Yara detected Amadey bot

Creates files in the system32 config directory

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)

Query firmware table information (likely to detect VMs)

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

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

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

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

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Vidar stealer

Yara detected Tofsee

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

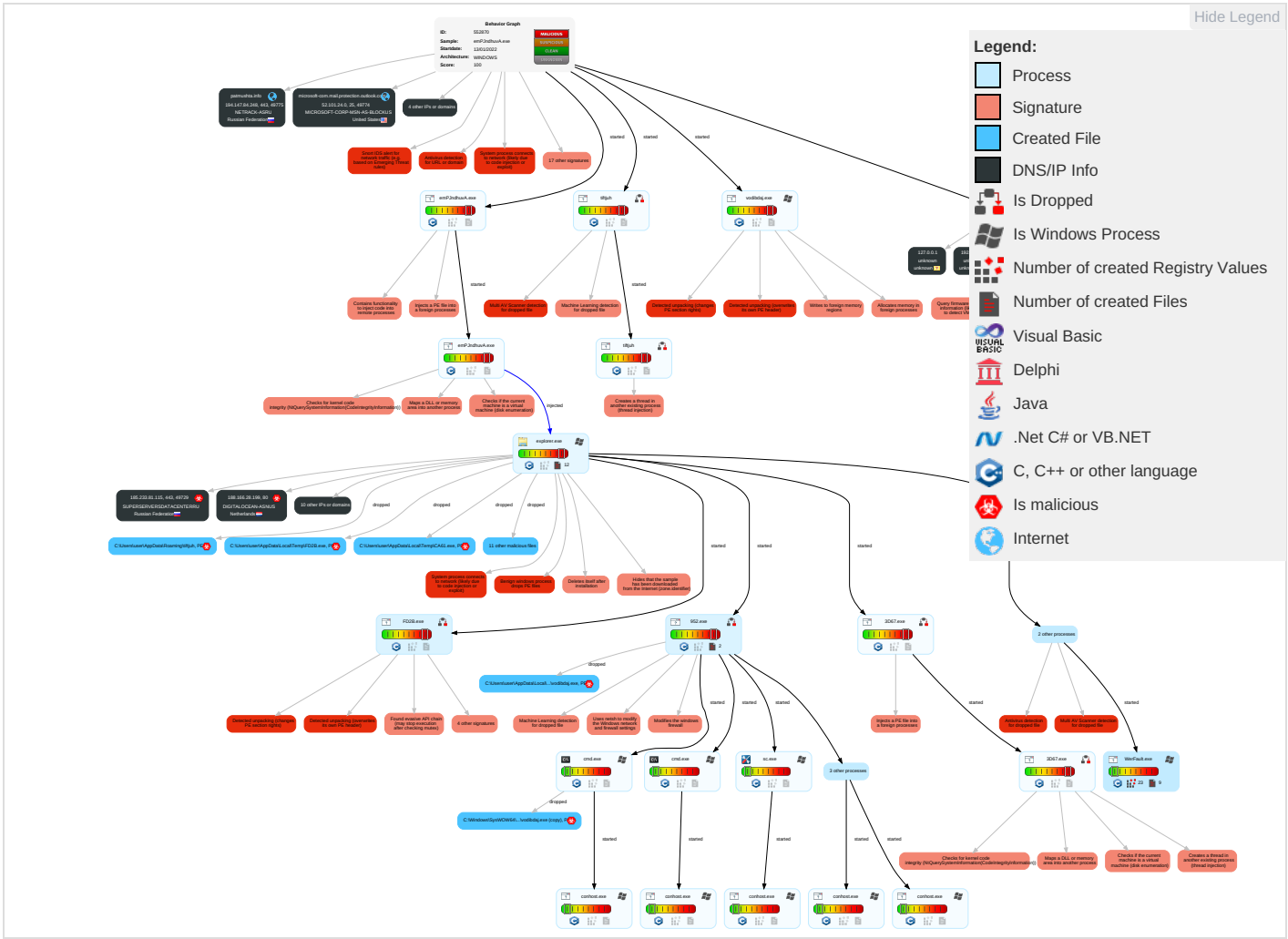
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 3 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingres Transf
Default Accounts	Native API 5 4	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Exploitation for Client Execution 1	Windows Service 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-S Port 2
Local Accounts	Service Execution 3	Logon Script (Mac)	Windows Service 4	Software Packing 3 3	NTDS	System Information Discovery 2 3 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Process Injection 7 1 3	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Applic Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 6 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 2 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 3 4 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web F
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 3 4 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail P
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

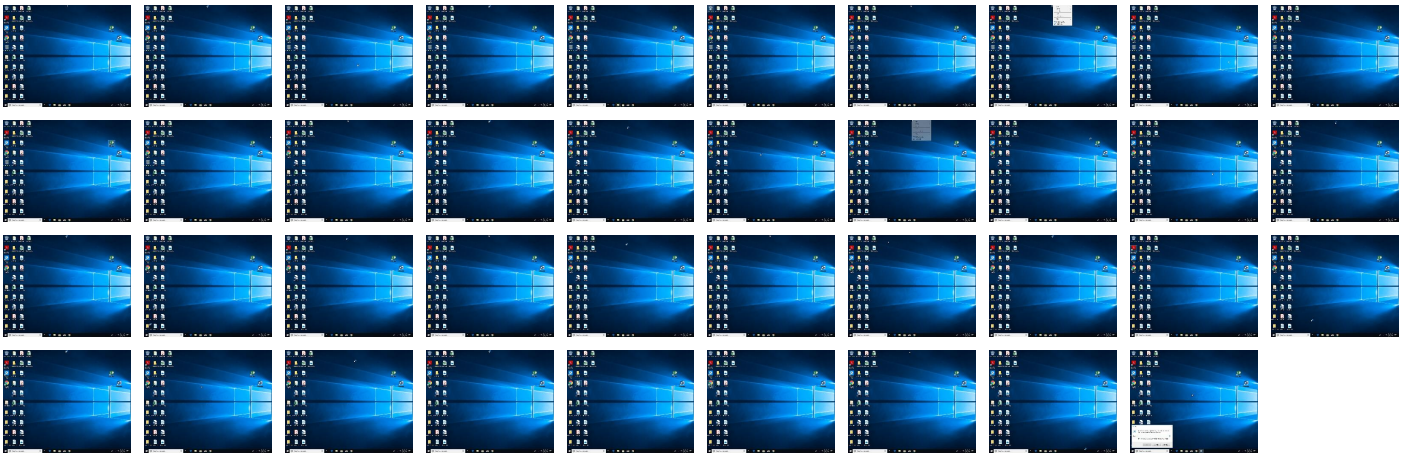
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
emPJndhuvA.exe	40%	Virustotal		Browse
emPJndhuvA.exe	66%	ReversingLabs	Win32.Trojan.Raccrypt	
emPJndhuvA.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\13E2.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\7E61.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FD2B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\13E2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2819.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\952.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6B74.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\tiftjuh	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5F8C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\45F8.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vodibdaj.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B1F6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9054.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CA61.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3D67.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\13E2.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\13E2.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\2819.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2819.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\5F8C.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5F8C.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Roaming\tiftjuh	66%	ReversingLabs	Win32.Trojan.Raccrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.0.tiftjuh.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.2819.exe.2080e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.0.13E2.exe.c80000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.1.emPJndhuvA.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.tiftjuh.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.3.952.exe.5a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.2819.exe.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.2819.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3D67.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.tiftjuh.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.emPJndhuvA.exe.5315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.0.13E2.exe.c80000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.emPJndhuvA.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.1.3D67.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.13E2.exe.c80000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.2.2819.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
44.2.vodibdaj.exe.610000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.0.emPJndhuvA.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.952.exe.580e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.2.2819.exe.2080e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.3.FD2B.exe.5a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.0.3D67.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.0.13E2.exe.c80000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.2.emPJndhuvA.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.tiftjuh.4615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.3D67.exe.4615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.FD2B.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.1.tiftjuh.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.emPJndhuvA.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
44.2.vodibdaj.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
29.2.FD2B.exe.580e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.2.3D67.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3D67.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
44.3.vodibdaj.exe.560000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
30.2.952.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
22.0.2819.exe.2080e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.2819.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
44.2.vodibdaj.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
21.0.tiftjuh.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.0.13E2.exe.c80000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://data-host-coin-8.com/files/4918_1642080252_3360.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://Passport.NET/tbpose	0%	Avira URL Cloud	safe	
http://Passport.NET/tb_jz	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	100%	Avira URL Cloud	malware	
http://docs.oasi	0%	Avira URL Cloud	safe	
http://docs.sis-op	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/9006_1642091568_3496.exe	100%	Avira URL Cloud	malware	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://www.w3.or	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://passport.net/tb	0%	Avira URL Cloud	safe	
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://Passport.NET/STS%3C/ds:KeyName%3E%3C/ds:KeyInfo%3E%3CCipherData%3E%3CCipherValue%3ECSImQ81IxG	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://Passport.NET/STS09/xmldsig#ripledes-cbc90995-327840285-2659745135-2630312742	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://Passport.NET/STS09/xmldsig#ripledes-cbc48496-2624191407-3283318427-1255436723	0%	Avira URL Cloud	safe	
http://Passport.NET/tbusi	0%	Avira URL Cloud	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://Passport.NET/STS	0%	Avira URL Cloud	safe	
http://schemas.microso	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://Passport.NET/STS09/xmldsig#ripledes-cbcices/SOAPF	0%	Avira URL Cloud	safe	
http://Passport.NET/STS09/xmldsig#ripledes-cbcices/SOAPFaultcurity-utility-1.0.xsd	0%	Avira URL Cloud	safe	
http://dhttp://Passport.NET/STS09/xmldsig#ripledes-cbcices/SOAPFaultcurity-utility-1.0.xsd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	45.135.233.182	true	false		high
patmushta.info	194.147.84.248	true	false		high
cdn.discordapp.com	162.159.129.233	true	false		high
privacy-tools-for-you-780.com	45.135.233.182	true	false		high
microsoft-com.mail.protection.outlook.com	52.101.24.0	true	false		high
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high
data-host-coin-8.com	45.135.233.182	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://a0621298.xsph.ru/7.exe	false		high
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://data-host-coin-8.com/files/4918_1642080252_3360.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	true	• Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/c_setup.exe	false		high
http://a0621298.xsph.ru/3.exe	false		high
http://data-host-coin-8.com/files/9006_1642091568_3496.exe	true	• Avira URL Cloud: malware	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://a0621298.xsph.ru/442.exe	false		high
http://privacy-tools-for-you-780.com/downloads/toolspab3.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://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://a0621298.xsph.ru/RMR.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.135.233.182	host-data-coin-11.com	Russian Federation		49392	ASBAXETNRU	false
194.147.84.248	patmushta.info	Russian Federation		61400	NETRACK-ASRU	false
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
54.38.220.85	unicupload.top	France		16276	OVHFR	false
52.101.24.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.21.38.221	goo.su	United States		13335	CLOUDFLARENETUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552870
Start date:	13.01.2022
Start time:	20:48:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	emPJndhuvA.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:	49

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@61/41@91/14
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 47.1% (good quality ratio 38%) • Quality average: 64.9% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:49:38	API Interceptor	2x Sleep call for process: svchost.exe modified
20:50:15	Task Scheduler	Run new task: Firefox Default Browser Agent BF39D970AE7F435F path: C:\Users\user\AppData\Roaming\tiftjuh
20:50:34	API Interceptor	1x Sleep call for process: FD2B.exe modified
20:50:54	API Interceptor	1x Sleep call for process: WerFault.exe modified
20:50:55	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
20:51:22	API Interceptor	1x Sleep call for process: explorer.exe modified
20:51:23	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
20:51:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe
20:51:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
20:52:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_s.exe
20:52:17	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\IdentityCRL\production\wlidsvcconfig.xml	
Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12703
Entropy (8bit):	5.664727316652114
Encrypted:	false
SSDEEP:	192:Tu8vk5/2HBw1tY3LZC7URIwKZ1bSvHSm5128Zil7Or5QwhJlAi:Tu8+2xZJRIwKZzm5yKFX
MD5:	0516512FF97C0F1DF67ED56A848B02A9
SHA1:	F50B8012260B8085EE1F350F78D8F3D24FB4F5EF
SHA-256:	41BE64D933BE2102AB9651C6478959EDB3763A7AA7B32E4E086150F7F13CE7A0
SHA-512:	CE06CA9414EF56987D45D43253DA96B53074BFED48DC4383AAF8EFC78CC3EEF2B982738CC7AEF9E3F750A2F55EF14EEED3F077026ADDC07C4D01D36BFB3A77C
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="us-ascii"?><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><cfg:Configuration version="1.1" xmlns:cfg="http://schemas.microsoft.com/Passport/PPCRL"> .. When a certificate is rev'd, a line like the following should be .. added to the cfg:Settings section:.. <cfg:Certificate expired="true">SLCA_BACKUP.CER</cfg:Certificate>.. --><cfg:Settings><cfg:DeviceDNSSuffix>.devicedns.live.com</cfg:DeviceDNSSuffix><cfg:ResolveTimeout>120000</cfg:ResolveTimeout><cfg:ConnectTimeout>60000</cfg:ConnectTimeout><cfg:SendTimeout>30000</cfg:SendTimeout><cfg:ReceiveTimeout>30000</cfg:ReceiveTimeout><cfg:MinMinutesBetweenMetaConfigCheck>1440</cfg:MinMinutesBetweenMetaConfigCheck><cfg:ConfigServerSslURI>https://go.microsoft.com/fwlink/?LinkId=859524</cfg:ConfigServerSslURI><cfg:DIDCOMMetaData><cfg:DIDWithAuth>1</cfg:DIDWithAuth><cfg:AssocPDIDToLDID>1</cfg:AssocPDIDToLDID><cfg:Protocol><cfg:CLSID>{1C109E4C-2F30-4EA3-A57A-A290877A2303}</cfg:CLSID><cfg:DATA

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24860541449255014
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4X:BJiRdwfu2SRU4X
MD5:	AA6BB71586A207C1805C93957AA30AD9
SHA1:	4DFEE4DC837378A57D1CDD209B6B65A1CEE6695F
SHA-256:	442E88CC083C574C0BC33DAAD27CBEC794D2BBCD6E9389807B3BDA866ADAE862
SHA-512:	2F0DF0E36BAD852287F4E96669D6E6BCFF71EACD912F2D05096DCFC7754D8EBF4EBA481216552068BFDA8453CD7A221EFA3E36877DA7C697AA8489F0D364933
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xa30397f4, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507428048063614
Encrypted:	false
SSDEEP:	384:s+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:zSB2nSB2RSjlK/+mLesOj1J2
MD5:	7D10996D49DA5170622F111A8DB3B34C
SHA1:	0C045A3F8BA0C37DC286E381377A6D043864301E
SHA-256:	6182B373F28CCD8B703A8CD8E6E05EBF41DADE4901523196E0678272D1560E93
SHA-512:	15DD1652FC6408931EB4B2463D5C7976D430F1E05A150778BA40B91C56BE28701ADA03400D0300C048495C47CD543CDF6F99737C065B05693313E1649F96B30B
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Reputation:	unknown
Preview:	....e.f.3...w.....&.....w..&1...z..h.(.....3...w.....B.....@..... .....3...w..... .....<&1...z.....T..&1...z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07693191266980651
Encrypted:	false
SSDEEP:	3:C/7EvD47p+/tc8l/bJdAtiS9WAplllAll3VkttlmlnI:Sif/i8t4pWMA3
MD5:	72AACDA5BA34A1204B0E1761FB516F25
SHA1:	1770B3792BD62164797B8463286B18D7ECA1D5CA
SHA-256:	FF7F15C485345CD656ED4496922F6EB2D137C044D1BC8CC242FF12383B127712
SHA-512:	04332DA807E7F6956F9C3C1E2373235D002F6741CEE8D030D9703FBCA08A9703548512D871F95BC2C75F242EA9A5F520789C152C571ECE838EAE7D8DD94DAC2
Malicious:	false
Reputation:	unknown
Preview:	rW.N.....3...w..&1...z.....w.....w.....w....:O....w.....T..&1...z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_2819.exe_886dfb69803377da97d7c95cea5f58e4d54dd88_79c6d167_161f0920\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):	0.813185051222203
Encrypted:	false
SSDEEP:	96:gJFibve1tLzH6/OQoJ7R3V6tpXIQcQec6tycEfcw3e+HbHg/8BRTf3o8Fa9iVfO5:kavazHN8HQ0lTjIq/u7sOS274ltn
MD5:	5DF816B307E5ED55ACEAE1818BF188C9
SHA1:	A2ECBBBDDEE5600524BF87EB68FF5599B32ED568
SHA-256:	E1659F9E3DBA19433F8BF949C621B590C6CFEC74710E63F2397FFF35F30EECAC
SHA-512:	6A171D4BE7C64A891ABD201851D68112132FEA330990FF28B8C7C5F7CE10BD5CE8A988DE9EC1E37D405E8E9470C911274DD0538FF0169E666EE0310DA78B1BE8
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.=.1.3.2.8.6.6.0.9.4.3.2.3.6.2.8.2.8.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.0.9.4.5.1.3.1.5.9.1.2.7.....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.=.7.a.7.e.f.b.f.c.-.8.e.6.7.-.4.f.3.c.-.9.e.0.3.-.2.c.3.0.4.d.a.5.8.b.b.d.....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.=.b.c.4.d.7.4.a.9.-.5.4.6.3.-.4.d.1.8.-.a.c.1.d.-.d.3.b.7.1.3.1.9.e.5.3.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.2.8.1.9...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.c.2.0.-.0.0.0.1.-.0.0.1.6.-.b.b.0.c.-.b.2.3.b.0.2.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.b.0.f.c.3.5.0.f.c.0.2.c.2.e.a.2.2.b.0.8.4.8.e.c.d.c.6.6.3.5.0.0.0.0.0.2.9.0.1.!.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.!.2.8.1.9...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\WER3D44.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 04:50:35 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.120563142372381
Encrypted:	false
SSDEEP:	192:DaATNpst2Oeh0GHpTvML8S9JYzF7YBJPhfO1Fopz:CjeJh0LLo2BFhjz
MD5:	79EB4C3C1720452CFE290A77CC582C28
SHA1:	C9C73BE51B4919D7009C4AD29237379F508878D2
SHA-256:	A284AC58B9B88A70B6A7A0B3FE4B428E664E59E039F2BE9DEACF9D4C8333EFC0
SHA-512:	061894FDBFAC7FD90291909E767D191B28F6BFCF9158EEA604B6503CEBA18644EEC09CE7DF693D5080CC4CB0F2E4C04DD1CC9EADE62C38A9A5A75B3243B9C6B
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D44.tmp.dmp	
Preview:	MDMP..... .....a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T..... .....a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D14.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.700961067644554
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiQSd6tRsQ6YIDSUUzgmfzRSiAzCpDL89bY8sf7vZIm:RrlsNiX6tRsQ6YcSUigmfzRSiAfYPf77
MD5:	FCA0AA267BB33A0A3C78DD00C7E53FB2
SHA1:	F4F2EFF771E4C3D5DD85CA69F32C61F958DCEE41
SHA-256:	F38C651573C980EA18F20245643CA2D7B980FCEEADE83743C38F737F3BE70247
SHA-512:	409D12B28966F71B1E4E2A2A298AEDFE2DF489879F27CB2882D246EC1BEC7139B2C8BF691D84E3D7B471C54C79F91638B5A38EE0597067C54D9DC99881E51DD
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.>.3.1.0.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5487.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):	4.4709404462914755
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9DrWSC8Bqs8fm8M4J98qFE+q8vs8p3fgtYd:uITfiAaSNsRJOKffgtYd
MD5:	3F3A356F56D6A4533FAE911FD1906421
SHA1:	03AE9A922F06A240D9DF2F55307883508317AD08
SHA-256:	6885066DFF181A511EB79B1E7932E547CB4A0539677422F5EF41B6DA93805D04
SHA-512:	87920C710F33B65101A1A9FCFDE875D147D30EAAC545C3D1DA990446EDE7F4FFEB25E5F687AE1EBACD32045220D2E452FED6571338055ABCB0FFE748EA35BF54
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="1341481" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C60.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	55410
Entropy (8bit):	3.051722069493437
Encrypted:	false
SSDEEP:	1536:0fHLHUn24ZROzw2qZvCdqQoLbFrIKv4FnEFiaqvMiZIYPTL0:0fHLHUn24ZROzw2qZvCdqQoPFrIKv4FA
MD5:	F0398FDA44063007178B1E5A94776196
SHA1:	37CAF4B9C45DEFB483495C539A515EAD03AA87CF
SHA-256:	7A4E4081A72A8BCD8968C217133BD66B7E5E88E8B457D8CD10391EE938632AE9
SHA-512:	AC19D75FEC3926FDA5C623F6D4F98E1ED8C292E1955C72143031E52D06ECF52E2CBF378AC8943DA463BA02442F9D093CCAF9BCD93BC4B7CB45965A97FA75876
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C60.tmp.csv	
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E93.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696246008462747
Encrypted:	false
SSDEEP:	96:9GiZYWBubhddalYiYADWroHKUYEZzkstrigkOLzwRyC97aNk9At8l4/3:9jZDXlFvkz/97aNk9At74/3
MD5:	2F634B54C8BD66B1F1A55B4EC51F7840
SHA1:	32D8023A10E64A0DD194D6F504466B5F6BCB9ACE
SHA-256:	3E34045BF40114946DF5EE6435F4DDFDE287F8ADB05E84011CC41372BA48C0D1
SHA-512:	5F8D6CF992088D0F53D2458FC8357623F6D902BB983AA5A603EF3CC44D4BFB3CCEB4933CB618D5D44806BB75C5F477A4397FECDFDA786C91C39F8179FBF44D1
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\WERA6E2.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51100
Entropy (8bit):	3.065536061021575
Encrypted:	false
SSDEEP:	768:sAH+OF+Et0rWE/230frj2FZOTo/sBw9fm5vjcbgX8:sAHRB0l230Tj2FZMo/sBw9fm5vjcbgX8
MD5:	9A6560221109CF6DC6D1181532311280
SHA1:	7C675FD2498E5A94B827C3500776ADDF85AC3B29
SHA-256:	33B139EE36667DE6A30D7A03DA377B6165A71107CC625C963C1D53220292E892
SHA-512:	44D00625A305F47AECA9B14F09B3FF63F3DA5FA61A71872B99A0C65689F2E40F901E9A956E28176DE3C984AC82135E129899B51AFF0B066DB25377E3DD7DECA
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\WERADC7.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53558
Entropy (8bit):	3.0577445365050546
Encrypted:	false
SSDEEP:	1536:FqHffSe2EPOVE2qZGCVqQbLbu1xkbOBn9LvT+XtigB:FqHffSe2EPOVE2qZGCVqQbPu1xkbOBn4
MD5:	44F909722F6881ACB5E0D38DC5049285
SHA1:	5706A9B1E113AD28B7F0A03C23225FE40EB5BF25
SHA-256:	6B768330BA798FE5485A054DE417DAB859FD699FAB81D8FF1436BA6D9BAE829A
SHA-512:	F160455B750A640B658B45FDDD572919A5CE60764AFAC07C3CD71D6D888915F16C6C1F43EE17F0935661B4957DA9C352F2D00EEC31D40C17F62E1564FF46088
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WERADC7.tmp.csv	
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.69513043446906
Encrypted:	false
SSDEEP:	96:9GiZYWxvo/arYLYFBWDazHNUYEZgztFipFKFowbGAnsaS0BM4aIt33:9jZDJMIkaf52aS0BM4Nt33
MD5:	50D28775D5999ACE46C22C7DCCBA883D
SHA1:	7528888E8F506DE3C8896E00F06DF8C97B688CA8
SHA-256:	836333D49E9F1E2F3295F85CC601AB6246D9744FDA09B9970543C61BBE6FE340
SHA-512:	75277E3CF2C41086D1DE67026708AD8BC6F87031F300215B9E5834C9B60833AA82F89C80D0131B4F5173ECCD9FF49D251213891332BC2AF08A914BEDCEC1EE4
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\WERB673.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696427295032779
Encrypted:	false
SSDEEP:	96:9GiZYWdKw9aHYtYItW8HGUYEZuGtriKjkJLCw9JPmkaBoxP6rZaEWIGZ2a3:9jZDIHqHk1JukauJ6rZaERGZ2a3
MD5:	4AB02C3931E0B05AB492267DDEDB81FC
SHA1:	028F4AD9FBCF725953A84B21F89C3C55F3A43DA0
SHA-256:	948238F9A7DAFD6B69DA99D0430F09F44D9E9B30C0C853BE18E8345A10D7676D
SHA-512:	0E9DC0351D7531B3C557A0C6C69E9E54A8F32EE5A7C3CA1DA642BB412AE443CB43B1E4C8C37D534E2BEEE1B9C2820B16568034A3167CF32786E0A32DF9173AC
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\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	5.229161033546255
Encrypted:	false
SSDEEP:	24:2dS48pX4y/DvKWDkQpydX8ICDKbnTiTBMuT52YGP8EqXpWfKFghR4p/BzceFYMQc:cAn/TLtpuQ6Zhip/B4VDSkC9+TiL+s
MD5:	745BFA39C73F634F5383C83A69A11AD0
SHA1:	D946292D52770ADBBEAC4A4D4E5A18407D1A80D9
SHA-256:	E2B998E9EC2D0C2FE171C06C98A6BE56D0CB1C00D8D0D007B526F782EBDAF763
SHA-512:	B775FD26BAD7E17250738E7CE7489CC34207B295D54EE21079D62C7485A8315A5DF7CDA7607B4001B5133EE7A297ACDDCE059127D9876420A648A66E1205B7D
Malicious:	false
Reputation:	unknown

C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)	
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService d ataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataTyp e="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399985333469120</FirstScanAttempt Time><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399985333781637</LastMeteredScanTime><LastScanAttemptTime dataType ="21">132399985333469120</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType ="21">132459503442223904</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml	
Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	5.229161033546255
Encrypted:	false
SSDEEP:	24:2dS48pX4y/DvKWDkQpydX8ICDKbnTiTBMuT52YGP8EqXpWfKFghR4p/BzceFYMQc:cAn/TLtpuQ6Zhip/B4VDSkC9+TiL+s
MD5:	745BFA39C73F634F5383C83A69A11AD0
SHA1:	D946292D52770ADBBEAC4A4D4E5A18407D1A80D9
SHA-256:	E2B998E9EC2D0C2FE171C06C98A6BE56D0CB1C00D8D0D007B526F782EBDAF763
SHA-512:	B775FD26BAD7E17250738E7CE7489CC34207B295D54EE21079D62C7485A8315A5DF7CDA7607B4001B5133EE7A297ACDDCE059127D9876420A648A66E1205B7D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService d ataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataTyp e="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399985333469120</FirstScanAttempt Time><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399985333781637</LastMeteredScanTime><LastScanAttemptTime dataType ="21">132399985333469120</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType ="21">132459503442223904</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.001.etl (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.7649970978747143
Encrypted:	false
SSDEEP:	192:xii8i/EV0E+Nn9MC++6U6yuI6LpYL87LWdCLWMa:wZR6oa
MD5:	16A89235CAAF9B886829EF4DA5C9B3B3
SHA1:	2E33823F067339232CE23D5C4DB6763B690DDCCA
SHA-256:	D502642BE4B16C9D616952661BBB7F754A1F8200F078AE67CD230541C4FB51AF
SHA-512:	A7140CEAAEBCC4B1D0B6310440495692DF21616D29B38FB0FC8F3452115F2CD82169063F27FB70A3A9038564E99AD4F4948193F9F8EB4950AC89CD4B4E56CB67
Malicious:	false
Reputation:	unknown
Preview:	.....l.0+.....B.....Zb..K...(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....~.C+..... .....l.0+.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U. S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.....l.0+..... ....

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.7649970978747143
Encrypted:	false
SSDEEP:	192:xii8i/EV0E+Nn9MC++6U6yuI6LpYL87LWdCLWMa:wZR6oa
MD5:	16A89235CAAF9B886829EF4DA5C9B3B3
SHA1:	2E33823F067339232CE23D5C4DB6763B690DDCCA
SHA-256:	D502642BE4B16C9D616952661BBB7F754A1F8200F078AE67CD230541C4FB51AF
SHA-512:	A7140CEAAEBCC4B1D0B6310440495692DF21616D29B38FB0FC8F3452115F2CD82169063F27FB70A3A9038564E99AD4F4948193F9F8EB4950AC89CD4B4E56CB67
Malicious:	false
Reputation:	unknown

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl	
Preview:	.....l.0+.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....~.C+..... .....l.0+.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.....l.0+..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\13E2.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\13E2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\13E2.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....l... ...`....@.. ..... ..@.....`l..K...`.....  .....  ..H.....text....)... ...*.....  ..`.rsrc.....`.....@....reloc..... .....0.....@..B.....l.....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\2819.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:lls8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\2819.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i.hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@..... .....e..P.....2..... Y..@.....0.....text..... ..`.rdata..D?...0...@..."....@..@.data...X....p...$...b.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\3D67.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	294400
Entropy (8bit):	5.161700003924834
Encrypted:	false
SSDEEP:	3072:jeZ5ZOixQx3X3QR6+lnj2D+bLiVsJEarkCVggjcGkNIVqI:jeZ74nAt1MEi1arR7ITsq
MD5:	BB0BA8D31F37E6B9F683EBD9044F1A85
SHA1:	4809E4E2D68DFBAB64E8D0C78DEBCCAB3AFEB219
SHA-256:	5C84D1C4DE9E3BCCD37EA7B64B4EC7551A1D50FA38F70217F0D9B1D79C496F9C
SHA-512:	25E240D39FF1508F9B294F202F81DA68D9F26848A85A698059E004022732AB3D744033D69BD3617C663D5C3FF2EC01D07A10A6E3D13C0EB84A6791F06AA000AA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,?a.Bla.Bla.Bl._.l|.Bl._.l..Bl._.lO.BlF.9lb.Bla.Cl..Bl._.l`.Bl._.l`.Bl._.l`.BlRicha.Bl.....PE..L.....`..... .....2.....0....@.....(... .....1.....r..@.....0.....text..... ....`.rdata...X...0...Z...$.....@..@.data.....".-~.....@....rsrc..... .....@..@.....

C:\Users\user\AppData\Local\Temp\45F8.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%
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\5F8C.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**

C:\Users\user\AppData\Local\Temp\5F8C.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..U(...(...(...6.).1...6.?.W....l..+...(.....6.8....6.(.)...6.-.)...Rich(.....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8.....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|.....@..@.reloc..4F...0...H...l.....@..B.....

C:\Users\user\AppData\Local\Temp\6B74.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	357376
Entropy (8bit):	7.848837612305308
Encrypted:	false
SSDEEP:	6144:L5aWbksiNTBCxw++TiSUOTtF08P3A6rZluu2PocRzBcByMFkBrBXwNmQp9Un:L5atNTAduU0tFDdlD2PVRzBeyiuFbAGn
MD5:	98E5E0F15766F21E9DCBEEF7DFB6EBB2
SHA1:	921E1B410528FF10A2C3980E35A8F036FF5E40B3
SHA-256:	5C7BF1968002CFFE455B5651C6D650323EA800AD03FA996A9F96CC01028AB093
SHA-512:	E425628E1A6311EBF57F73213DF8CDA9C8B5E888A6054188485614D1910F9E1CD879D5DE1D284CA9754D6405809FBDCC9FEFB72852ACE8E7357A71099800CC4
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.....L.....pt..<.....code...~8.....:..... ..`.text...B....P.....>..... ..`.rdata...3...0...4.....@..@.data.....p.....J.....@....rsrc...L.....\.....@..@.....

C:\Users\user\AppData\Local\Temp\7E61.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	357376
Entropy (8bit):	7.84824059044154
Encrypted:	false
SSDEEP:	6144:b5aWbksiNTBcMOxjwlPHtnAA8R0O+eNpEj9JE/emtUfMtK+e:b5atNTKpxkIPNnT8f+WEj9JETmUKP
MD5:	56610CBDB784A4F8517C5DE4FF92D85E
SHA1:	9A7DC5A26040DC775C1B3854E6909DFD0ADF84FC
SHA-256:	3B6CBB6FDE5051E6EC3AD23789968670C68F3EF82D8FEBE258E223C1487F42C4
SHA-512:	2CA0753458611C7DC5BFAAE0BA2947E001E6D2E3BD8A4FB447B075D755BFA0566AEA4FCCCC5C97FAE4149CF1A439922B4B14EE4D39B7DF0B26F775FD3F6C8C92
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.....D.....pt..<.....code...~8.....:..... ..`.text...B....P.....>..... ..`.rdata...3...0...4.....@..@.data.....p.....J.....@....rsrc...D.....\.....@..@.....

C:\Users\user\AppData\Local\Temp\9054.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3570176
Entropy (8bit):	**7.997630766149595**
Encrypted:	**true**
SSDEEP:	98304:Eyu1PF0IdV1/b4gfya9kofb/4rosp08oUPQH:EjtFp/tfyOTQrosGrUP0
MD5:	DDC599DB99362A7D8642FC19ABE03871
SHA1:	11199134356D8DE145D2EE22AAC37CA8AABA8A0B
SHA-256:	5D94F66FD3315E847213E16E19DFEB008B020798CFFF1334D48AC3344B711F22
SHA-512:	E35DBE56828E804AA78FE436E1717C3A09C416DBE2873FFFC9B44393E7EC2336CE9C544E4D6011C58E7E706819AEABC027AF9A85AA2A2509BDFC39699560ABD

C:\Users\user\AppData\Local\Temp\9054.exe

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... T.....b.6.....|IO. .....M..... ....&....@.....@.....0.....@.....1...P.....@.....02...../.....@....rsrc.....M.....40.....@....T3QbYgM.....`O.....1..... ..@....adata.....T.....z6.....@..... .....

C:\Users\user\AppData\Local\Temp\952.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	313344
Entropy (8bit):	5.385503417493937
Encrypted:	false
SSDEEP:	3072:ODhRp6LR3B/X3Q36+cErZGXrVfAEiphvXRltMMkNkVggjcGkNIVqI:ODhRMRvAzjZGXhfAEivBV7ITsq
MD5:	4C29CFD658E015FA4DB5A2454F103D4A
SHA1:	8F6446343C0EEC5AD7F78F359BFE3CB1774974E6
SHA-256:	52E5252201061F6D1FF2EA00B5DC59A8B0F85FBA7E5F3EF7B3187717431E2DC5
SHA-512:	F611459A65EF60B4FDFE82BFD30EADC53F3122DE0EF00377C7208441C9B9DC001DAD9F5C16E0F12578EF4D2695433F93D4921254F425FE9F52B64F79E6A139A0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,?a.Bla.Bla.Bl._.l\|.Bl._.l..Bl._.lO.BlF.9lb.Bla.Cl..Bl._.l`.Bl._.l`.Bl ._.l`.BlRicha.Bl.....PE..L...(6._..... ..."......2.....0....@.....@.....r7.....(....`.....1..... .r..@.....0.....text..... ....`.rdata...X...0...Z...$.....@..@.data.....l..~.....@....rsrc.....`.....@..@..... ....

C:\Users\user\AppData\Local\Temp\B1F6.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3558912
Entropy (8bit):	**7.997469140425603**
Encrypted:	**true**
SSDEEP:	98304:yzzKY1eh2yDYShw4LnKd4yYcr8tEY8fhV1T:yzW52yw4rZy3rOEvhv
MD5:	DB3711D2DE8511E1192E6E38988E6989
SHA1:	D33A20FDC9D6E08BB66E355DA3B9B9219E459DDB
SHA-256:	0D5636B8B6C3F9876A0CA4741F8FA704366DDABA6FA65C5BB5740616F8985927
SHA-512:	32ADE75117319A5CB139BA83277F3F5007289A6559BDDC78D1417C7F20219D11F0668AE3743A7B8142562C43170D22CD85C8440D88F1C8509A414234DEFEB76F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... S.....G6.....|.N. ....@M..... ....&....@.....@.....0.....@.....~....P.....@.....1..p.....@....rsrc.....@M.....MYBFBZj.....N.....1..... ..@....adata.....S.....N6.....@..... .....

C:\Users\user\AppData\Local\Temp\CA61.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**

C:\Users\user\AppData\Local\Temp\CA61.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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\FD2B.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	327168
Entropy (8bit):	5.544004911166714
Encrypted:	false
SSDEEP:	3072:kApM+Wvghk1X3Qvg6+3lpIWnTPCl1Jw62s1pILewTywVggjcGkNIVqI:kApE4kxAvU3lpIWql3Ewkewv7ITsq
MD5:	CEBAF005081C730D4AC7A87E46B440D0
SHA1:	70C9FDA14D6F9B578E795B6FCD015629BA6FBFF5
SHA-256:	4F5A438F45CD46F639F813063DCA15C0D7A6F77BCB5DF788AE8B761A96AE25F5
SHA-512:	E398988945BC2D75D53A822FD482B16C9E780E64620F2663B85F6D9F4076A9397FFBA7EFA7A205A13CD33B77356002BA34F88FA30175241E98F05E7582598410
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,?a.Bla.Bla.Bl._.l\|.Bl._.l..Bl._.lO.BlF.9lb.Bla.Cl..Bl._.l`.Bl._.l`.Bl ._.l`.BlRicha.Bl.....PE..L....._..... ...Z.....2.....0....@.....i.....(.....1.....r..@..... .....0.....text..... ..... ..`.rdata..xX...0...Z...$.....@..@.data...x.....~.....@....rsrc..... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\vodibdaj.exe	
Process:	C:\Users\user\AppData\Local\Temp\952.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13043712
Entropy (8bit):	6.366947693071425
Encrypted:	false
SSDEEP:	12288:lDhWRvAkYLv7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7QD:loRvA7
MD5:	E331BE085840751FF0AC8DCBCDC5F5E3
SHA1:	131F8E057EB9476CC73080E76BB845A06EDC0964
SHA-256:	520F8BC540C90AF4B21118E2DAFC63878C84C685B2CF8682B94D52E7FA492796
SHA-512:	D33ACFD2E4859615CC2AA383E598B58426940AFD0795AB8B14A34F4C7EE3BCD154E5975D294397D30AB588228F5C04348F53362F3CA51D0FB6CBB7A717CFE29
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,?a.Bla.Bla.Bl._.l\|.Bl._.l..Bl._.lO.BlF.9lb.Bla.Cl..Bl._.l`.Bl._.l`.Bl ._.l`.BlRicha.Bl.....PE..L...(6._..... ...".....2.....0....@.....@.....r7.....(....`.....1..... .r..@.....0.....text..... ....`.rdata...X...0...Z...$.....@..@.data.....l...~.....@....rsrc.....`.....@..@..... ....

C:\Users\user\AppData\Roaming\tiftjuh	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	283648
Entropy (8bit):	5.09190119944441
Encrypted:	false
SSDEEP:	3072:AQAT6lATyGd4pXqYMER3QLSeuYerXcyGmofWrxpzbgqru:AQppHZQLSeNcbG/fuzbgwu
MD5:	A7444553F8A8FE2702B6FD48008D6605
SHA1:	F6D3D6CCF728AE7AB39B7E29F21AE5BCC7FCE98B
SHA-256:	BA5303301925A877689B30EFC36F872564F06906B2A61D7C3A7C955B0587D4F8
SHA-512:	28A1EDB043AE30AF213CBFE93745F2D94A4F9F5B76668CBED0889780DC7031E4A6D1CAA839D78035A42769BC13D2D0A376E13E50779807EDBCD3189D44F070E F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 66%

C:\Users\user\AppData\Roaming\tiftjuh	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L.....?_..... .....0.....0....@.....,Q.....hf..(..... .....1.....@Y..@.....0.....text..... .. ..`.rdata..2?...0...@...$.....@..@.data.....p..."...d.....@....rsrc... .....@..@..... .....

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

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

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220114_044950_709.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.386072904720816
Encrypted:	false
SSDEEP:	96:3TCA2po+EP5IT9s2Y7FCHSI2lQJvkzM4zOT2AYFz/UMCprJRpl5N:WZ5rjh2WZOCrh
MD5:	36C1E8F3408F5AB482AB271BEA1CE1FD
SHA1:	383C14C76CA0057C0CD4CFF0E2C5F373D2D7E6D5
SHA-256:	34E2ACEBF493AB5EF65D665DFF258A649B57FACEAAF558017A11DDCD8A5BA935
SHA-512:	70DA15A77F2C3F1AD7BE7EDAD3197FE5D38D5D7BD1EBF8763ED2EEBEA3D29F7B1FF9423B8A79BA2E1DD679506CE69BA2536AD8E4D2B715C1E72A446812551 663
Malicious:	false
Reputation:	unknown
Preview:	....!.....8.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1...../_8..... ....%(.*.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.2.0.1.1.4._.0.4.4.9.5.0._.7.0.9...e.t.l.....P.P.8.....

C:\Windows\SysWOW64\bhlprady\vodibdaj.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Windows\SysWOW64\bhlprady\vodibdaj.exe (copy)	
Size (bytes):	13043712
Entropy (8bit):	6.366947693071425
Encrypted:	false
SSDEEP:	12288:lDhWRvAkYLv7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7Q7QD:loRvA7
MD5:	E331BE085840751FF0AC8DCBCDC5F5E3
SHA1:	131F8E057EB9476CC73080E76BB845A06EDC0964
SHA-256:	520F8BC540C90AF4B21118E2DAFC63878C84C685B2CF8682B94D52E7FA492796
SHA-512:	D33ACFD2E4859615CC2AA383E598B58426940AFD0795AB8B14A34F4C7EE3BCD154E5975D294397D30AB588228F5C04348F53362F3CA51D0FB6CBB7A717CFE29
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,?a.Bla.Bla.Bl._.l|.Bl._.l..Bl._.lO.BlF.9lb.Bla.Cl..Bl._.l`.Bl._.l`.Bl ._.l`.BlRicha.Bl.....PE..L...(6._..... ..."......2.....0....@.....@.....r7.....(....`.....1..... .r..@.....0.....text..... ....`.rdata...X...0...Z...$.....@..@.data.....l...~.....@....rsrc.....`.....@..@..... ....

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\IdentityCRL\production\tmpconfig.xml	
Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12703
Entropy (8bit):	5.664727316652114
Encrypted:	false
SSDEEP:	192:Tu8vk5/2HBw1tY3LZC7URIwKZ1bSvHSm5128Zil7Or5QwhJlAi:Tu8+2xZJRIwKZzm5yKFX
MD5:	0516512FF97C0F1DF67ED56A848B02A9
SHA1:	F50B8012260B8085EE1F350F78D8F3D24FB4F5EF
SHA-256:	41BE64D933BE2102AB9651C6478959EDB3763A7AA7B32E4E086150F7F13CE7A0
SHA-512:	CE06CA9414EF56987D45D43253DA96B53074BFED48DC4383AAF8EFC78CC3EEF2B982738CC7AEF9E3F750A2F55EF14EEED3F077026ADDC07C4D01D36BFB3A77C
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="us-ascii"?><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><cfg:Configuration version="1.1" xmlns:cfg="http://schemas.microsoft.com/Passport/PPCRL"> .. When a certificate is rev'd, a line like the following should be .. added to the cfg:Settings section:.. <cfg:Certificate expired="true" >SLCA_BACKUP.CER</cfg:Certificate>.. --><cfg:Settings><cfg:DeviceDNSSuffix>.devicedns.live.com</cfg:DeviceDNSSuffix><cfg:ResolveTimeout>120000</cfg:ResolveTimeout><cfg:ConnectTimeout>60000</cfg:ConnectTimeout><cfg:SendTimeout>30000</cfg:SendTimeout><cfg:ReceiveTimeout>30000</cfg:ReceiveTimeout><cfg:MinMinutesBetweenMetaConfigCheck>1440</cfg:MinMinutesBetweenMetaConfigCheck><cfg:ConfigServerSslURI>https://go.microsoft.com/fwlink/?LinkId=859524</cfg:ConfigServerSslURI><cfg:DIDCOMMetaData><cfg:DIDWithAuth>1</cfg:DIDWithAuth><cfg:AssocPDIDToLDID>1</cfg:AssocPDIDToLDID><cfg:Protocol><cfg:CLSID>{1C109E4C-2F30-4EA3-A57A-A290877A2303}</cfg:CLSID><cfg:DATA

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):	4.261542646947877
Encrypted:	false
SSDEEP:	12288:WDry9CsWH6WqxQJKo3pscOBnAykoTjuWKSZ/J4F2U5+DWu4UTKDFmkM9:Wry9CsWH6WqxQJKV5DZ9
MD5:	9DD1B2C13E54BFBDDC233A2107B3AFA1
SHA1:	19F44BC959620448A9E8E45198902EB667D3F0FF
SHA-256:	D91CC5B510FF718D8CED59A261914ABEB72B96FB40418949E6B1DF993BB949BE
SHA-512:	91B5CDDA3FF1363663AB4B897869EF1C39FD8F722048887CEB7AA513C05AB6DD7183EDC72E4B3FE63B0C4140C4D2AEE0B2C9DC5CBA3EAC9C40E6913FF2394AD
Malicious:	false
Reputation:	unknown
Preview:	regfQ...Q...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm"."A..... ....`')..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.7809311639586114
Encrypted:	false

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
SSDEEP:	384:co65rZrdFdXp5xQp8JXQnxOf2oLPmxwpe5GjZmGudDTTVv5N5/sTCef:vk1rFXp4pHgf2oqxwpCWmGutTVRN5gCe
MD5:	28554A0C6B33D9BF5BA5149FFD57ED28
SHA1:	D61C244F3A5C9FF4891DF70831A455ADE9ADFF6C
SHA-256:	2933C4D27D58B26EA5F4662F16E54A62CC44CD39CBC0D40B86168E97E35345B7
SHA-512:	E7A739F019DC7EADCD94676324AB1B9FE76D75EDAABFE6785A97F23FA35DA8653103C2E77D20EE0FC07DE38668EE291A3DBB6C50412804F5F16F70B6F3C29EA
Malicious:	false
Reputation:	unknown
Preview:	regfP...P...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm"."A..... ....f').HvLE.^.....P.....~h>....L+..... ..hbin.....p.\.,.....nk,...$A..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...$A..... .....P..... .....Z.....Root.....lf.....Root....nk ...$A.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBIydWALLt2w
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):	5.09190119944441
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	emPJndhuvA.exe
File size:	283648
MD5:	a7444553f8a8fe2702b6fd48008d6605
SHA1:	f6d3d6ccf728ae7ab39b7e29f21ae5bcc7fce98b
SHA256:	ba5303301925a877689b30efc36f872564f06906b2a61d7c3a7c955b0587d4f8
SHA512:	28a1edb043ae30af213cbfe93745f2d94a4f9f5b76668cbed0889780dc7031e4a6d1caa839d78035a42769bc13d2d0a376e13e50779807edbcd3189d44f070bf
SSDEEP:	3072:AQAT6lATyGd4pXqYMER3QLSeuYerXcyGmofWrxpzbgqru:AQppHZQLSeNcbG/fuzbgwu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I.....v.....h.....E.....x.....f.....c.....Rich.....PE..L.....?_.....

File Icon

Icon Hash:	acfc36b6b69cc6e2

Static PE Info

General

Entrypoint:	0x403000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F3F8DFF [Fri Aug 21 09:03:59 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6d4af36ccbaddaffd179ef41d42df9cf

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11e13	0x12000	False	0.607245551215	data	6.66808697674	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x13000	0x3f32	0x4000	False	0.365783691406	data	5.41084156967	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x17000	0x281b8	0x22200	False	0.252797332875	data	2.7964138755	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x40000	0xcd20	0xce00	False	0.660421723301	data	6.34041238895	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Bulgarian	Bulgaria	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 20:50:14.577049971 CET	192.168.2.5	8.8.8.8	0xfd21	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:15.097651005 CET	192.168.2.5	8.8.8.8	0x67b8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:15.604837894 CET	192.168.2.5	8.8.8.8	0x5b2a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:16.368606091 CET	192.168.2.5	8.8.8.8	0x2fbe	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:16.568407059 CET	192.168.2.5	8.8.8.8	0x425a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:17.347769976 CET	192.168.2.5	8.8.8.8	0x2663	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:18.771472931 CET	192.168.2.5	8.8.8.8	0x3e82	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:18.969288111 CET	192.168.2.5	8.8.8.8	0x6d91	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:19.171705961 CET	192.168.2.5	8.8.8.8	0x407c	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:21.509632111 CET	192.168.2.5	8.8.8.8	0x5049	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:21.724939108 CET	192.168.2.5	8.8.8.8	0x561d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:22.292650938 CET	192.168.2.5	8.8.8.8	0x87be	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:23.315615892 CET	192.168.2.5	8.8.8.8	0x60cc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:23.627414942 CET	192.168.2.5	8.8.8.8	0x1fba	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.195837021 CET	192.168.2.5	8.8.8.8	0xba95	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.386401892 CET	192.168.2.5	8.8.8.8	0x88f3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.631541967 CET	192.168.2.5	8.8.8.8	0x8aa	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.707587957 CET	192.168.2.5	8.8.8.8	0xe57a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.926979065 CET	192.168.2.5	8.8.8.8	0x407f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:28.139836073 CET	192.168.2.5	8.8.8.8	0x2822	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:28.369760990 CET	192.168.2.5	8.8.8.8	0xd5c8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:28.567552090 CET	192.168.2.5	8.8.8.8	0xf69b	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:31.556504011 CET	192.168.2.5	8.8.8.8	0xdbc5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:31.757889986 CET	192.168.2.5	8.8.8.8	0x3417	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:31.960659981 CET	192.168.2.5	8.8.8.8	0xde5c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:32.173810959 CET	192.168.2.5	8.8.8.8	0xb0e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:34.603390932 CET	192.168.2.5	8.8.8.8	0x2046	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:34.810184956 CET	192.168.2.5	8.8.8.8	0x8348	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.096636057 CET	192.168.2.5	8.8.8.8	0xac98	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.335197926 CET	192.168.2.5	8.8.8.8	0xcf3	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:37.140340090 CET	192.168.2.5	8.8.8.8	0xd895	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:37.333856106 CET	192.168.2.5	8.8.8.8	0xcd87	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:37.548629045 CET	192.168.2.5	8.8.8.8	0x69e3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:54.076708078 CET	192.168.2.5	8.8.8.8	0x2d8f	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 20:50:56.620975971 CET	192.168.2.5	8.8.8.8	0x3455	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.217998028 CET	192.168.2.5	8.8.8.8	0xb09d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.440074921 CET	192.168.2.5	8.8.8.8	0x552	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.692543030 CET	192.168.2.5	8.8.8.8	0xc02b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.898191929 CET	192.168.2.5	8.8.8.8	0x7c6e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:00.107970953 CET	192.168.2.5	8.8.8.8	0x89a6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:01.453991890 CET	192.168.2.5	8.8.8.8	0xf67f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:02.568372011 CET	192.168.2.5	8.8.8.8	0x1521	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.060121059 CET	192.168.2.5	8.8.8.8	0x419	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.279849052 CET	192.168.2.5	8.8.8.8	0xe98	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.501588106 CET	192.168.2.5	8.8.8.8	0xc12	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.713627100 CET	192.168.2.5	8.8.8.8	0xd038	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.943644047 CET	192.168.2.5	8.8.8.8	0x8f25	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:04.459856033 CET	192.168.2.5	8.8.8.8	0xace9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:04.658813953 CET	192.168.2.5	8.8.8.8	0x92b4	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:10.049961090 CET	192.168.2.5	8.8.8.8	0xed9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:10.255024910 CET	192.168.2.5	8.8.8.8	0x3059	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:10.499171019 CET	192.168.2.5	8.8.8.8	0x69ab	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:11.517026901 CET	192.168.2.5	8.8.8.8	0xd592	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:11.716371059 CET	192.168.2.5	8.8.8.8	0x5e38	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:11.886979103 CET	192.168.2.5	8.8.8.8	0xcf9b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:12.179253101 CET	192.168.2.5	8.8.8.8	0xc75c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:12.409200907 CET	192.168.2.5	8.8.8.8	0xf592	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:12.605907917 CET	192.168.2.5	8.8.8.8	0xd851	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:13.098541021 CET	192.168.2.5	8.8.8.8	0x380a	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:17.349642992 CET	192.168.2.5	8.8.8.8	0x850e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:17.560170889 CET	192.168.2.5	8.8.8.8	0x82bc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:17.806190968 CET	192.168.2.5	8.8.8.8	0x76d1	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:21.828104019 CET	192.168.2.5	8.8.8.8	0x97ec	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:22.121568918 CET	192.168.2.5	8.8.8.8	0x4f71	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:22.377249956 CET	192.168.2.5	8.8.8.8	0x21c0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:23.009521008 CET	192.168.2.5	8.8.8.8	0x3bcd	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.063586950 CET	192.168.2.5	8.8.8.8	0x82c7	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.479244947 CET	192.168.2.5	8.8.8.8	0xf177	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.672830105 CET	192.168.2.5	8.8.8.8	0xa949	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.874068022 CET	192.168.2.5	8.8.8.8	0x5da8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.073750973 CET	192.168.2.5	8.8.8.8	0x5f8c	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 20:51:25.267398119 CET	192.168.2.5	8.8.8.8	0x72f6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.460829020 CET	192.168.2.5	8.8.8.8	0xad22	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.517657995 CET	192.168.2.5	8.8.8.8	0x59eb	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.664927006 CET	192.168.2.5	8.8.8.8	0x2c80	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.866749048 CET	192.168.2.5	8.8.8.8	0x3812	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.920264006 CET	192.168.2.5	8.8.8.8	0xf11	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:28.638899088 CET	192.168.2.5	8.8.8.8	0x23bb	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:29.410271883 CET	192.168.2.5	8.8.8.8	0xfb88	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:29.672091961 CET	192.168.2.5	8.8.8.8	0xdb83	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:29.923193932 CET	192.168.2.5	8.8.8.8	0xc153	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:31.026422977 CET	192.168.2.5	8.8.8.8	0x9964	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:33.084913015 CET	192.168.2.5	8.8.8.8	0xe25a	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:39.198669910 CET	192.168.2.5	8.8.8.8	0x60e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:39.451325893 CET	192.168.2.5	8.8.8.8	0xb836	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:39.708311081 CET	192.168.2.5	8.8.8.8	0xa8ef	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:43.278525114 CET	192.168.2.5	8.8.8.8	0x7de9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:43.868870974 CET	192.168.2.5	8.8.8.8	0xffbd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:44.177290916 CET	192.168.2.5	8.8.8.8	0x5096	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:46.916022062 CET	192.168.2.5	8.8.8.8	0x9c6c	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:51.415652037 CET	192.168.2.5	8.8.8.8	0xd24b	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 13, 2022 20:49:49.973989010 CET	8.8.8.8	192.168.2.5	0x753f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 20:49:51.230057955 CET	8.8.8.8	192.168.2.5	0xc461	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 20:50:14.901438951 CET	8.8.8.8	192.168.2.5	0xfd21	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:15.412342072 CET	8.8.8.8	192.168.2.5	0x67b8	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:15.915755987 CET	8.8.8.8	192.168.2.5	0x5b2a	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:16.388226032 CET	8.8.8.8	192.168.2.5	0x2fbe	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:16.887778044 CET	8.8.8.8	192.168.2.5	0x425a	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:17.367253065 CET	8.8.8.8	192.168.2.5	0x2663	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:18.790960073 CET	8.8.8.8	192.168.2.5	0x3e82	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:18.988770008 CET	8.8.8.8	192.168.2.5	0x6d91	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 20:50:19.189316988 CET	8.8.8.8	192.168.2.5	0x407c	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:21.528119087 CET	8.8.8.8	192.168.2.5	0x5049	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:22.031879902 CET	8.8.8.8	192.168.2.5	0x561d	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:22.578578949 CET	8.8.8.8	192.168.2.5	0x87be	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:23.333172083 CET	8.8.8.8	192.168.2.5	0x60cc	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:23.913242102 CET	8.8.8.8	192.168.2.5	0x1fba	No error (0)	privacy-tools-for-you-780.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.213608027 CET	8.8.8.8	192.168.2.5	0xba95	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.405731916 CET	8.8.8.8	192.168.2.5	0x88f3	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.652326107 CET	8.8.8.8	192.168.2.5	0x8aa	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.727003098 CET	8.8.8.8	192.168.2.5	0xe57a	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:27.944425106 CET	8.8.8.8	192.168.2.5	0x407f	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:28.157407045 CET	8.8.8.8	192.168.2.5	0x2822	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:28.389689922 CET	8.8.8.8	192.168.2.5	0xd5c8	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:28.585131884 CET	8.8.8.8	192.168.2.5	0xf69b	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:31.579428911 CET	8.8.8.8	192.168.2.5	0xdbc5	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:31.777633905 CET	8.8.8.8	192.168.2.5	0x3417	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:31.980295897 CET	8.8.8.8	192.168.2.5	0xde5c	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:32.195322990 CET	8.8.8.8	192.168.2.5	0xb0e	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:34.620995045 CET	8.8.8.8	192.168.2.5	0x2046	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:34.829580069 CET	8.8.8.8	192.168.2.5	0x8348	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.114659071 CET	8.8.8.8	192.168.2.5	0xac98	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.356386900 CET	8.8.8.8	192.168.2.5	0xcf3	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.356386900 CET	8.8.8.8	192.168.2.5	0xcf3	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.356386900 CET	8.8.8.8	192.168.2.5	0xcf3	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.356386900 CET	8.8.8.8	192.168.2.5	0xcf3	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:35.356386900 CET	8.8.8.8	192.168.2.5	0xcf3	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 13, 2022 20:50:37.159130096 CET	8.8.8.8	192.168.2.5	0xd895	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:37.352848053 CET	8.8.8.8	192.168.2.5	0xcd87	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:37.567598104 CET	8.8.8.8	192.168.2.5	0x69e3	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:54.104259014 CET	8.8.8.8	192.168.2.5	0x2d8f	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:54.104259014 CET	8.8.8.8	192.168.2.5	0x2d8f	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:54.104259014 CET	8.8.8.8	192.168.2.5	0x2d8f	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:54.104259014 CET	8.8.8.8	192.168.2.5	0x2d8f	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:54.104259014 CET	8.8.8.8	192.168.2.5	0x2d8f	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:56.640268087 CET	8.8.8.8	192.168.2.5	0x3455	No error (0)	patmushta.info		194.147.84.248	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.240576982 CET	8.8.8.8	192.168.2.5	0xb09d	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.462568998 CET	8.8.8.8	192.168.2.5	0x552	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.711718082 CET	8.8.8.8	192.168.2.5	0xc02b	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:50:59.917193890 CET	8.8.8.8	192.168.2.5	0x7c6e	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:00.127841949 CET	8.8.8.8	192.168.2.5	0x89a6	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:01.473987103 CET	8.8.8.8	192.168.2.5	0xf67f	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:02.854114056 CET	8.8.8.8	192.168.2.5	0x1521	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.077233076 CET	8.8.8.8	192.168.2.5	0x419	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.299500942 CET	8.8.8.8	192.168.2.5	0xe98	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.521477938 CET	8.8.8.8	192.168.2.5	0xc12	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:03.733238935 CET	8.8.8.8	192.168.2.5	0xd038	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:04.255460978 CET	8.8.8.8	192.168.2.5	0x8f25	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:04.479167938 CET	8.8.8.8	192.168.2.5	0xace9	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:04.675826073 CET	8.8.8.8	192.168.2.5	0x92b4	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:10.068919897 CET	8.8.8.8	192.168.2.5	0xed9	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 20:51:10.274704933 CET	8.8.8.8	192.168.2.5	0x3059	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:10.521966934 CET	8.8.8.8	192.168.2.5	0x69ab	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:10.521966934 CET	8.8.8.8	192.168.2.5	0x69ab	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:11.536814928 CET	8.8.8.8	192.168.2.5	0xd592	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:11.735837936 CET	8.8.8.8	192.168.2.5	0x5e38	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:11.904275894 CET	8.8.8.8	192.168.2.5	0xcf9b	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:12.199425936 CET	8.8.8.8	192.168.2.5	0xc75c	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:12.429064035 CET	8.8.8.8	192.168.2.5	0xf592	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:12.892231941 CET	8.8.8.8	192.168.2.5	0xd851	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:13.118015051 CET	8.8.8.8	192.168.2.5	0x380a	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:17.369241953 CET	8.8.8.8	192.168.2.5	0x850e	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:17.577545881 CET	8.8.8.8	192.168.2.5	0x82bc	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:17.825061083 CET	8.8.8.8	192.168.2.5	0x76d1	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:21.847376108 CET	8.8.8.8	192.168.2.5	0x97ec	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:22.140321970 CET	8.8.8.8	192.168.2.5	0x4f71	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:22.698045015 CET	8.8.8.8	192.168.2.5	0x21c0	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:23.031286001 CET	8.8.8.8	192.168.2.5	0x3bcd	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.175137997 CET	8.8.8.8	192.168.2.5	0x82c7	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.498091936 CET	8.8.8.8	192.168.2.5	0xf177	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.692013979 CET	8.8.8.8	192.168.2.5	0xa949	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:24.891491890 CET	8.8.8.8	192.168.2.5	0x5da8	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.090441942 CET	8.8.8.8	192.168.2.5	0x5f8c	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.284733057 CET	8.8.8.8	192.168.2.5	0x72f6	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.480112076 CET	8.8.8.8	192.168.2.5	0xad22	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.540070057 CET	8.8.8.8	192.168.2.5	0x59eb	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.683645010 CET	8.8.8.8	192.168.2.5	0x2c80	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 20:51:25.888603926 CET	8.8.8.8	192.168.2.5	0x3812	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:25.939457893 CET	8.8.8.8	192.168.2.5	0xf11	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:28.658353090 CET	8.8.8.8	192.168.2.5	0x23bb	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:29.429544926 CET	8.8.8.8	192.168.2.5	0xfb88	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:29.689757109 CET	8.8.8.8	192.168.2.5	0xdb83	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:29.940614939 CET	8.8.8.8	192.168.2.5	0xc153	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:31.048644066 CET	8.8.8.8	192.168.2.5	0x9964	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:31.048644066 CET	8.8.8.8	192.168.2.5	0x9964	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:31.048644066 CET	8.8.8.8	192.168.2.5	0x9964	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:31.048644066 CET	8.8.8.8	192.168.2.5	0x9964	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:31.048644066 CET	8.8.8.8	192.168.2.5	0x9964	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:33.104171038 CET	8.8.8.8	192.168.2.5	0xe25a	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:39.223459959 CET	8.8.8.8	192.168.2.5	0x60e	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:39.470139027 CET	8.8.8.8	192.168.2.5	0xb836	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:40.018325090 CET	8.8.8.8	192.168.2.5	0xa8ef	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:43.627818108 CET	8.8.8.8	192.168.2.5	0x7de9	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:43.888562918 CET	8.8.8.8	192.168.2.5	0xffbd	No error (0)	host-data-coin-11.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:44.195440054 CET	8.8.8.8	192.168.2.5	0x5096	No error (0)	data-host-coin-8.com		45.135.233.182	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:47.260868073 CET	8.8.8.8	192.168.2.5	0x9c6c	No error (0)	patmushta.info		194.147.84.248	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:51.442142963 CET	8.8.8.8	192.168.2.5	0xd24b	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:51.442142963 CET	8.8.8.8	192.168.2.5	0xd24b	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:51.442142963 CET	8.8.8.8	192.168.2.5	0xd24b	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:51.442142963 CET	8.8.8.8	192.168.2.5	0xd24b	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 13, 2022 20:51:51.442142963 CET	8.8.8.8	192.168.2.5	0xd24b	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hudnwo.net
  - host-data-coin-11.com
- imfaq.com
- jjxcvqdtu.com
- fbpbiuf.net
- ubqgnsref.net
- dencntiwom.org
- facsdjlrhe.org
- nbopqwwil.org
- data-host-coin-8.com
- bksuhny.net
- ncekou.com
- mlrqq.org
- mkylelnvhx.org
- privacy-tools-for-you-780.com
- uasbnlg.com
- djtirwiie.net
- unicupload.top
- ruexdakex.net
- obxaeg.net
- ocenwxcoy.net
- cbnhk.net
- qqkskcahhd.com
- crthr.com
- kjtyikafjr.org
- gcluxyujw.net
- 185.7.214.171:8080
- bsyjr.com
- uvbrfosd.org
- phljuvuic.com

- mtege.com
- hsqeovy.org
- ffohm.org
- uwxadets.net
- owkwjgjx.org
- ujflcd.org
- wwwrwr.net
- rffjdwq.org
- hwjxdg.com
- hrknr.net
- ffqdri.net
- rsnegictry.org
- jeltu.com
- kdpxgri.net
- fisxwlhs.org
- hfldhq.org
- ontfrhif.com
- bbrscm.org
- rsccxqyvj.org
- jhmgibx.org
- xcyxdpo.com
- bmitrqru.com
- yomhbwinpp.net
- jowhwjm.org
- pedgrinq.com
- a0621298.xsph.ru
- pfdipnd.com
- bhcnfrdygt.net
- lepwe.net
- wlbpl.net

- ebglpbq.net
- ldoxvunj.com
- arxpt.com
- wajww.org
- bitqeg.net
- rqhabfnn.net
- hjilsxiyi.com
- lvexyr.org
- rfqgywpmj.net
- nkjumxwsc.org
- wnfuahwrra.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: emPJndhuvA.exe PID: 3352 Parent PID: 5996

General

Start time:	20:49:29
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\emPJndhuvA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\emPJndhuvA.exe"
Imagebase:	0x400000
File size:	283648 bytes
MD5 hash:	A7444553F8A8FE2702B6FD48008D6605
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: emPJndhuvA.exe PID: 4160 Parent PID: 3352

General

Start time:	20:49:32
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\emPJndhuvA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\emPJndhuvA.exe"
Imagebase:	0x400000
File size:	283648 bytes
MD5 hash:	A7444553F8A8FE2702B6FD48008D6605
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: 00000001.00000002.310069625.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.309813053.0000000000530000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 4372 Parent PID: 556

General

Start time:	20:49:38
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 3472 Parent PID: 4160

General

Start time:	20:49:39
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000000.295057363.0000000003A61000.00000020.00020000.sdmp, Author: Joe Security

Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 4596 Parent PID: 556

General

Start time:	20:49:48
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 4400 Parent PID: 556

General

Start time:	20:49:48
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5784 Parent PID: 556

General

Start time:	20:49:49
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

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

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5400 Parent PID: 556

General

Start time:	20:49:50
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5056 Parent PID: 556

General

Start time:	20:49:50
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 2872 Parent PID: 556

General

Start time:	20:49:51
Start date:	13/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7d4480000

File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5796 Parent PID: 556

General

Start time:	20:49:52
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3540 Parent PID: 556

General

Start time:	20:49:53
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 1280 Parent PID: 556

General

Start time:	20:50:07
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: tiftjuh PID: 4892 Parent PID: 904

General

Start time:	20:50:16
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\tiftjuh
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tiftjuh
Imagebase:	0x400000
File size:	283648 bytes
MD5 hash:	A7444553F8A8FE2702B6FD48008D6605
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 66%, ReversingLabs

Analysis Process: tiftjuh PID: 5816 Parent PID: 4892

General

Start time:	20:50:18
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\tiftjuh
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tiftjuh
Imagebase:	0x400000
File size:	283648 bytes
MD5 hash:	A7444553F8A8FE2702B6FD48008D6605
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: 00000015.00000002.360645909.00000000004D1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000015.00000002.360518485.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: 2819.exe PID: 3104 Parent PID: 3472

General

Start time:	20:50:20
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2819.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2819.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs

Analysis Process: svchost.exe PID: 5208 Parent PID: 556

General

Start time:	20:50:25
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: 3D67.exe PID: 5276 Parent PID: 3472

General

Start time:	20:50:25
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3D67.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3D67.exe
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	BB0BA8D31F37E6B9F683EBD9044F1A85
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: WerFault.exe PID: 5736 Parent PID: 5208

General

Start time:	20:50:26
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 3104 -ip 3104
Imagebase:	0x1e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5956 Parent PID: 3104

General

Start time:	20:50:28
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3104 -s 540
Imagebase:	0x1e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: 3D67.exe PID: 4968 Parent PID: 5276

General

Start time:	20:50:29
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3D67.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3D67.exe
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	BB0BA8D31F37E6B9F683EBD9044F1A85
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: 0000001C.00000002.386280466.0000000001F30000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001C.00000002.386498287.0000000002431000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: FD2B.exe PID: 468 Parent PID: 3472

General

Start time:	20:50:30
Start date:	13/01/2022

Path:	C:\Users\user\AppData\Local\Temp\FD2B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\FD2B.exe
Imagebase:	0x400000
File size:	327168 bytes
MD5 hash:	CEBAF005081C730D4AC7A87E46B440D0
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: 0000001D.00000002.379514532.0000000000482000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000001D.00000002.379514532.0000000000482000.00000004.00000020.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: 952.exe PID: 1068 Parent PID: 3472

General

Start time:	20:50:33
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\952.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\952.exe
Imagebase:	0x400000
File size:	313344 bytes
MD5 hash:	4C29CFD658E015FA4DB5A2454F103D4A
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: 0000001E.00000002.412229320.0000000000580000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001E.00000003.383697292.00000000005A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001E.00000002.410807233.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 13E2.exe PID: 2316 Parent PID: 3472

General

Start time:	20:50:35
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\13E2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\13E2.exe
Imagebase:	0xc80000
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: 00000020.00000002.447751764.0000000004021000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 89%, ReversingLabs

Analysis Process: cmd.exe PID: 4356 Parent PID: 1068

General

Start time:	20:50:41
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\bhlprady\
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6168 Parent PID: 4356

General

Start time:	20:50:42
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6248 Parent PID: 1068

General

Start time:	20:50:43
Start date:	13/01/2022
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\vodibdaj.exe" C:\Windows\SysWOW64\bhlprady\
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6260 Parent PID: 6248

General

Start time:	20:50:44
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6304 Parent PID: 1068

General

Start time:	20:50:44
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create bhlprady binPath= "C:\Windows\SysWOW64\bhlprady\vodibdaj.exe /d\"C:\Users\user\AppData\Local\Temp\952.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xfd0000
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: 6332 Parent PID: 6304

General

Start time:	20:50:45
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6372 Parent PID: 1068

General

Start time:	20:50:46

Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description bhlprady "wifi internet conection
Imagebase:	0xfd0000
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: 6384 Parent PID: 6372

General

Start time:	20:50:46
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6412 Parent PID: 1068

General

Start time:	20:50:47
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start bhlprady
Imagebase:	0xfd0000
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: 6436 Parent PID: 6412

General

Start time:	20:50:48
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 6460 Parent PID: 1068

General

Start time:	20:50:48
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x11f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vodibdaj.exe PID: 6484 Parent PID: 556

General

Start time:	20:50:49
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\bhlprady\vodibdaj.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\bhlprady\vodibdaj.exe /d"C:\Users\user\AppData\Local\Temp\952.exe"
Imagebase:	0x400000
File size:	13043712 bytes
MD5 hash:	E331BE085840751FF0AC8DCBCDC5F5E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002C.00000002.417710033.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002C.00000002.417504443.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002C.00000002.417841182.0000000000610000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000002C.00000003.415295647.0000000000560000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis