ID: 553117
Sample Name:
zmbGUZTICp.exe
Cookbook: default.jbs
Time: 10:42:04
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

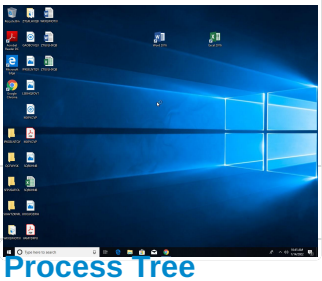
Windows Analysis Report zmbGUZTICp.exe

Overview

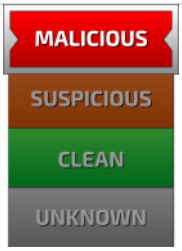
General Information

Sample Name:	zmbGUZTICp.exe
Analysis ID:	553117
MD5:	9af4d2022dc05c2..
SHA1:	f87c7511d2c4ea4..
SHA256:	c8fe81088b2caa9..
Tags:	exe RaccoonStealer
Infos:	

Most interesting Screenshot:



Detection



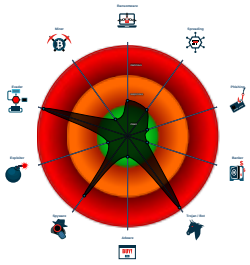
Amadey Raccoon RedLine SmokeLoader Tofsee Vidar

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- zmbGUZTICp.exe (PID: 4404 cmdline: "C:\Users\user\Desktop\zmbGUZTICp.exe" MD5: 9AF4D2022DC05C2DBBC4D218A8F0974C)
  - zmbGUZTICp.exe (PID: 3416 cmdline: "C:\Users\user\Desktop\zmbGUZTICp.exe" MD5: 9AF4D2022DC05C2DBBC4D218A8F0974C)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 1E7F.exe (PID: 5200 cmdline: C:\Users\user\AppData\Local\Temp\1E7F.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 5648 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5200 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 2DB3.exe (PID: 5640 cmdline: C:\Users\user\AppData\Local\Temp\2DB3.exe MD5: 6009BCB680BE6C0F656AA157E56423DC)
      - 309C.exe (PID: 5132 cmdline: C:\Users\user\AppData\Local\Temp\309C.exe MD5: 8B25D9317E18654C3F83EF8630D1DE16)
        - cmd.exe (PID: 852 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\ozuqupbe\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5820 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\tejjnepq.exe" C:\Windows\SysWOW64\ozuqupbe\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 4636 cmdline: C:\Windows\System32\sc.exe" create ozuqupbe binPath= "C:\Windows\SysWOW64\ozuqupbe\tejjnepq.exe /d\"C:\Users\user\AppData\Local\Temp\309C.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 3500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5360 cmdline: C:\Windows\System32\sc.exe" description ozuqupbe "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 1148 cmdline: "C:\Windows\System32\sc.exe" start ozuqupbe MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 5308 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: 3532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 3F71.exe (PID: 5196 cmdline: C:\Users\user\AppData\Local\Temp\3F71.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 3F71.exe (PID: 1508 cmdline: C:\Users\user\AppData\Local\Temp\3F71.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - A7F0.exe (PID: 2200 cmdline: C:\Users\user\AppData\Local\Temp\A7F0.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - BC16.exe (PID: 2576 cmdline: C:\Users\user\AppData\Local\Temp\BC16.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
        - mjlooy.exe (PID: 4660 cmdline: "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" MD5: 8B239554FE346656C8EEF9484CE8092F)
          - cmd.exe (PID: 5416 cmdline: "C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\82aa4a6c48\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 4864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - reg.exe (PID: 3168 cmdline: REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\82aa4a6c48\ MD5: CEE2A7E57DF2A159A065A34913A055C2)
          - schtasks.exe (PID: 4000 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN mjlooy.exe /TR "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 4636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - D452.exe (PID: 5572 cmdline: C:\Users\user\AppData\Local\Temp\D452.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
        - AppLaunch.exe (PID: 5588 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - 239.exe (PID: 5632 cmdline: C:\Users\user\AppData\Local\Temp\239.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
        - AppLaunch.exe (PID: 2152 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - 1D34.exe (PID: 2696 cmdline: C:\Users\user\AppData\Local\Temp\1D34.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - 2D04.exe (PID: 2896 cmdline: C:\Users\user\AppData\Local\Temp\2D04.exe MD5: 6ADB5470086099B9169109333FADAB86)
- gdrgbdj (PID: 2468 cmdline: C:\Users\user\AppData\Roaming\gdrgbdj MD5: 9AF4D2022DC05C2DBBC4D218A8F0974C)
  - gdrgbdj (PID: 3492 cmdline: C:\Users\user\AppData\Roaming\gdrgbdj MD5: 9AF4D2022DC05C2DBBC4D218A8F0974C)
- svchost.exe (PID: 5636 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5668 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 5200 -ip 5200 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- tejjnepq.exe (PID: 2320 cmdline: C:\Windows\SysWOW64\ozuqupbe\tejjnepq.exe /d"C:\Users\user\AppData\Local\Temp\309C.exe" MD5: 310337FA2432C256984AA89486B74D95)
  - svchost.exe (PID: 4692 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 5368 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5728 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- mjlooy.exe (PID: 2988 cmdline: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
- mjlooy.exe (PID: 3916 cmdline: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
0000002E.00000002.664274182.00000000076A6000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000022.00000002.583256444.00000000000C2000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.408517834.00000000005C1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000018.00000003.484958252.0000000000650000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0000002E.00000002.636412165.0000000000402000.00000020.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.3F71.exe.370f910.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
28.0.3F71.exe.400000.12.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.0.zmbGUZTICp.exe.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.3.309C.exe.660000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
24.2.tejjnepq.exe.400000.0.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 29 entries				

Sigma Overview

System Summary:

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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Raccoon Stealer
Antivirus detection for URL or domain
Antivirus detection for dropped file
Multi AV Scanner detection for submitted file
Multi AV Scanner detection for domain / URL
Machine Learning detection for sample
Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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

Persistence and Installation Behavior:

Yara detected Amadey bot

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

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

Tries to evade analysis by execution special instruction which cause usermode exception

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)

Tries to detect virtualization through RDTSC time measurements

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Raccoon Stealer

Yara detected Vidar stealer

Yara detected Tofsee

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

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

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Raccoon Stealer

Yara detected Vidar stealer

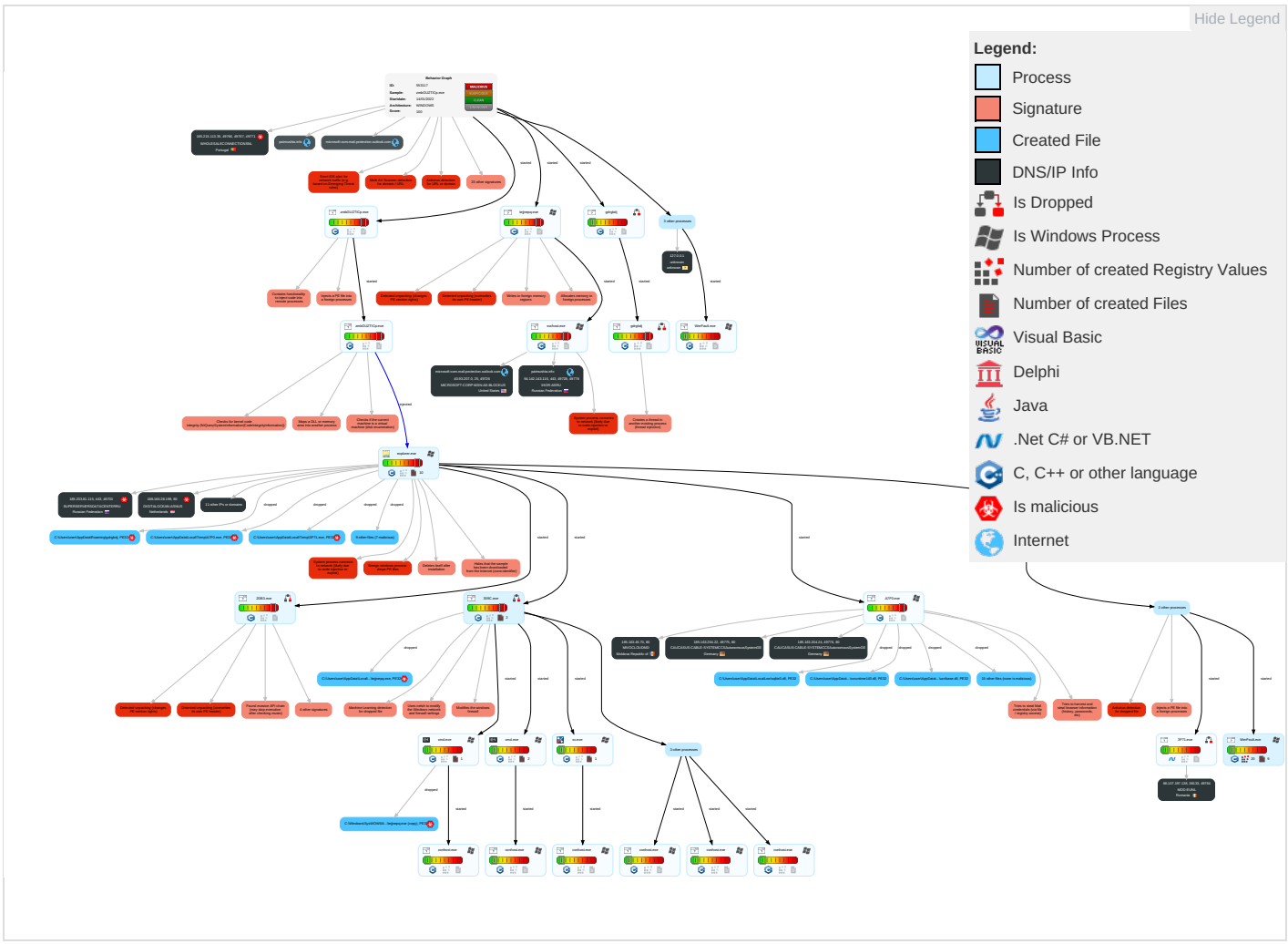
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Native API 5 3 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Default Accounts	Exploitation for Client Execution 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	Command and Scripting Interpreter 3	Windows Service 1 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Sta Port 1
Local Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Windows Service 1 4	Software Packing 3 3	NTDS	System Information Discovery 4 3 8	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Non-Applicat Layer Protocol
Cloud Accounts	Service Execution 3	Network Logon Script	Process Injection 7 1 3	Timestomp 1	LSA Secrets	Security Software Discovery 6 6 1	SSH	Keylogging	Data Transfer Size Limits	Applicat Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Scheduled Task/Job 1	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multibar Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Virtualization/Sandbox Evasion 2 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Modify Registry 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Virtualization/Sandbox Evasion 2 4 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Process Injection 7 1 3	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy
Trusted Relationship	Python	Hypervisor	Process Injection	Hidden Files and Directories 1	Web Portal Capture	Cloud Groups	Attack PC via USB Connection	Local Email Collection	Standard Application Layer Protocol	Internal

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
zmbGUZTICp.exe	35%	Virustotal		Browse
zmbGUZTICp.exe	42%	ReversingLabs	Win32.Trojan.Casdet	
zmbGUZTICp.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\3F71.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\239.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2D04.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\309C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1E7F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2DB3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1D34.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3F71.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy_InUse.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy_InUse.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	2%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
28.0.3F71.exe.fa0000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.zmbGUZTICp.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
28.0.3F71.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
28.0.3F71.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
13.2.3F71.exe.130000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.3.tejjnepq.exe.650000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.3F71.exe.130000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
7.0.1E7F.exe.2080e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.2DB3.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.zmbGUZTICp.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.gdrgbdj.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3F71.exe.fa0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
28.0.3F71.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
24.2.tejjnepq.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
28.0.3F71.exe.fa0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
28.0.3F71.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
7.2.1E7F.exe.2080e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.309C.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.0.3F71.exe.fa0000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
0.2.zmbGUZTICp.exe.6415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3F71.exe.fa0000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
6.0.gdrgbdj.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.zmbGUZTICp.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.3.A7F0.exe.4d10000.2.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
6.1.gdrgbdj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.zmbGUZTICp.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
8.2.2DB3.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.3.2DB3.exe.650000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
27.2.svchost.exe.4d0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
11.3.309C.exe.660000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.2.gdrgbdj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.zmbGUZTICp.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.gdrgbdj.6515a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.zmbGUZTICp.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
31.2.A7F0.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1127993		Download File
28.0.3F71.exe.fa0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.2.tejjnepq.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.3F71.exe.130000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
6.0.gdrgbdj.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.tejjnepq.exe.ed0000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.0.1E7F.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.1E7F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.1E7F.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3F71.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
7.0.1E7F.exe.2080e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3F71.exe.fa0000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
11.2.309C.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
13.0.3F71.exe.130000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
28.0.3F71.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.zmbGUZTICp.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
1.2.zmbGUZTICp.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.3F71.exe.130000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.zmbGUZTICp.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.3F71.exe.fa0000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
7.3.1E7F.exe.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.163.45.70/capibar	12%	Virustotal		Browse
http://185.163.45.70/capibar	100%	Avira URL Cloud	phishing	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/74acab80c259fbd3afe9b19dbd62861e1ddfe5b8	0%	Avira URL Cloud	safe	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/53d4f78085a60d100b5580840cacffadb56a356d	0%	Avira URL Cloud	safe	
http://185.163.204.24/r	0%	Avira URL Cloud	safe	
http://185.215.113.35/d2VxjasuwS/index.php	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://185.163.204.24/a	0%	Avira URL Cloud	safe	
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	0%	Avira URL Cloud	safe	
http://185.163.204.24/	0%	Avira URL Cloud	safe	
http://https://login.liUTF-8/p	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/74acab80c259fbd3afe9b19dbd62861e1ddfe5b8v	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	100%	Avira URL Cloud	malware	
http://Passport.NET/tb	0%	Avira URL Cloud	safe	
http://https://login.liUTF-16p	0%	Avira URL Cloud	safe	
http://https://login.live	0%	Avira URL Cloud	safe	
http://185.163.204.24/F	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://185.163.204.24/B	0%	Avira URL Cloud	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://https://login.live.c	0%	Avira URL Cloud	safe	
http://185.163.204.24/0	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://185.163.204.22/capibar	100%	Avira URL Cloud	malware	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/74acab80c259fbd3afe9b19dbd62861e1ddfe5b841	0%	Avira URL Cloud	safe	
http://185.163.204.24/as	0%	Avira URL Cloud	safe	
http://https://185.163.204.22/capibar	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://185.215.113.35/d2VxjasuwS/plugins/cred.dll	100%	Avira URL Cloud	malware	
http://https://logilive.c	0%	Avira URL Cloud	safe	
http://178.62.113.205/capibar	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	8.209.70.0	true	false		high
patmushta.info	94.142.143.116	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high
microsoft-com.mail.protection.outlook.com	40.93.207.0	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://a0621298.xsph.ru/7.exe	false		high
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/74acab80c259fbd3afe9b19dbd62861e1ddfe5b8	false	• Avira URL Cloud: safe	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/53d4f78085a60d100b5580840cacffadb56a356d	false	• Avira URL Cloud: safe	unknown
http://185.215.113.35/d2VxjasuwS/index.php	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• Avira URL Cloud: malware	unknown
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	true	• Avira URL Cloud: safe	unknown
http://185.163.204.24/	false	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	true	• Avira URL Cloud: malware	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://185.163.204.22/capibar	true	• Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/9.exe	false		high
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://185.215.113.35/d2VxjasuwS/plugins/cred.dll	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.163.45.70	unknown	Moldova Republic of		39798	MIVOCLOUDMD	false
40.93.207.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
94.142.143.116	patmushta.info	Russian Federation		35196	IHOR-ASRU	false
185.215.113.35	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
8.209.70.0	host-data-coin-11.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
104.21.38.221	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
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false
185.163.204.22	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false
185.163.204.24	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false

Private

IP
192.168.2.1

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553117
Start date:	14.01.2022
Start time:	10:42:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zmbGUZTICp.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:	48
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@61/51@81/19
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 19.1% (good quality ratio 13.1%) • Quality average: 51.7% • Quality standard deviation: 40.5%
HCA Information:	• Successful, ratio: 56% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:43:45	Task Scheduler	Run new task: Firefox Default Browser Agent EA345A35CCA4E184 path: C:\Users\user\AppData\Roaming\gdrgbdj
10:43:55	API Interceptor	1x Sleep call for process: 2DB3.exe modified
10:44:13	API Interceptor	1x Sleep call for process: WerFault.exe modified
10:44:22	API Interceptor	3x Sleep call for process: svchost.exe modified
10:44:44	API Interceptor	4x Sleep call for process: A7F0.exe modified
10:44:46	API Interceptor	464x Sleep call for process: mjlooy.exe modified
10:44:48	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2485928694932566
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU45:BJiRdwfu2SRU45
MD5:	46301C913F59052C24F89BB61C076A86
SHA1:	280D65E7DD5758F8E3A6C48C41E32B6D0AA4C53F
SHA-256:	8A752E2055C6F60317E892892F41DF560209FE83C82A8EBE85AD5A82FB3F15B7
SHA-512:	2DEA2312E30258ABD94606A4BBB1C5CBF0819C4CF4AA2AE98225AFD924E64406923D915ECED6F62BDD08499A1F8EA479432EE8D0FA243F2ECF9162E658910D3
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 user DataBase, version 0x620, checksum 0x2d162e1b, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506815554351528
Encrypted:	false
SSDEEP:	384:lbW+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:lbZSB2nSB2RSjlK/+mLesOj1J2
MD5:	5E8CDCD58254AD3AA7C14A73154B3277
SHA1:	9E9C44202300E3B618537D4D692360D57052A478
SHA-256:	6D19EF4AD21115659FEB89AB15A4CC3C26E5DBE468A568B2908A2B95AB552345
SHA-512:	6B45638E58215FDBF208547170B3DE276BCA26C78415874AAAEA5BEA56507B18529515AD47D36A876B12149FFC9BD5F9154A671BAD5A4C252C1B15DC29703B7
Malicious:	false
Reputation:	unknown
Preview:	-..... .....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... .....3...w..... .....S.3.,...z.q.....8.`.,..z.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07555221228914681
Encrypted:	false
SSDEEP:	3:sX1EvyJAq+l/bJdAtiXn6kqyll3VkttlmlnI:sAyuq+t4Lkq23
MD5:	C7CCFBC9E369C73F4A1268BEC8B124FA
SHA1:	F665B2B40E0561EE864D90A3D4F80E86324B5D6A
SHA-256:	64230019D1737CAFA29C4DF8DFCF1EFB8FE98851FEBEE83F490EF18F9E5FAF2D
SHA-512:	EF37F0AB3ABD2CF8DF0F66F4FDE4C0F729044CDD7E0829F0BA42FCD409365A7CE6F17A77CB5F90AFD33F70C612EA82D3DD7374D0E5603F5F766D07D487110EA
Malicious:	false
Reputation:	unknown
Preview:	...R.....3...w.....z.....w.....w.....w....:O....w.....8.`..,..z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_1E7F.exe_56ef6c3f939a5c31c54ae423594576eccb36d7e_39743ca4_173f7c90\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):	0.8147334084221176
Encrypted:	false
SSDEEP:	96:j+F+XLkopwOQoJ7R3V6tpXIQcQec6tycEfcw3m+HbHg/8BRTf3o8Fa9iVfOyWYmp:qckoJ8HQ0lbjIq/u7srS274ItvS
MD5:	0649ECAD777C02E54262EF3EB90CCED8
SHA1:	5E75E6699F03B849535D31A1A09A0F3497C86D7B
SHA-256:	85BA251E129D34788335425E83C40F0B5008954FAFF5A28F0E4CEA178D0737BF
SHA-512:	79B833B2EFB512A790883AF7B7F5DEEC4029A1D3FDBD099FC6FD8E4E51D3584DA139E4633BA69FEFCFA8076C88AE31177E06AF9B5F3D4360772BFF716705CDF
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.=.1.3.2.8.6.6.5.9.4.4.1.4.4.7.7.0.1.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.5.9.4.5.0.5.8.8.2.7.8.7.....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.=.3.d.b.a.8.7.6.a.-.b.e.b.4.-.4.f.0.c.-.b.3.f.0.-.b.a.1.e.3.9.a.c.0.0.3.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.a.2.c.d.2.1.-.2.4.f.3.-.4.b.b.a.-.8.f.6.c.-.2.9.5.2.1.f.e.9.2.d.0.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.1.E.7.F...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.5.0.-.0.0.0.1.-.0.0.1.7.-.6.8.0.9.-.2.5.a.b.7.6.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.b.8.a.6.9.7.9.3.a.e.a.f.d.6.b.7.1.9.f.f.0.5.f.0.c.b.d.a.b.c.6.0.0.0.0.2.9.0.1.!.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.!.1.E.7.F...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\WER4E1E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 18:44:02 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	42152
Entropy (8bit):	2.0070556637522814
Encrypted:	false
SSDEEP:	192:9+01WMNuYFYdOeh0k1ZU/z3gtgcoegRtT2t9sL2ChH1X:pNh6QefOjwzAx1X
MD5:	316DB5CFD39AB644814F89500F3C9906
SHA1:	66A84F4A0D70C0DB0D93DC88D01CB7DB183612F7
SHA-256:	B89B7C2A0A6ECF23AFA9F25E045FF95F078F13F8581664FB63FAB4ABB2F1FCA6
SHA-512:	5D786B587A11E11BFD7D4538D0C815664BF8136E06C9F411C9F563CB31EDED963757FBDCFD54A003C6CC8DCA2C5EBE964207AD6788D2C2E2ABC8213B909F56
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....r..a.....4...v(.....T.....8.....T.....x.....d.....U.....B.....GenuineIntelW.....T.....P...d..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\WER5581.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5581.tmp.WERInternalMetadata.xml	
Size (bytes):	8390
Entropy (8bit):	3.702157392275921
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNire6F6YJfSUjgmfqRSUCpDi89b23sfdym:RrlsNiC6F6YhSUjgmfqRSf28fZ
MD5:	68B45BFA81BD5DDCCE22105ACE357023
SHA1:	F8518BF4AC336C8189438B8FF8DFACAD2867A272
SHA-256:	7A3BDCE83450471DAADB0BE59262D65E518AC8B3A31C6289846522CCBBB0C300
SHA-512:	30C650628A38511C711E5DA5C1979A31325B52F6E478AFE0D574874561A63DC7C217615B62255B7D00A55D38227A24468164D0113BC04D02E55BE825E264E21A
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.>.5.2.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER59A9.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):	4.480309088097584
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9oaEYWSC8BQ8fm8M4JN8qFthlco+q8v981juLiAd:uITfifaERSNnJfnKAuLiAd
MD5:	FF921EB2F3095E2BB781CB4894F054C4
SHA1:	53BB32657077BCC58DBA8B5554DE9558041C2110
SHA-256:	DD601D81852C59F193A8E0FD702813BD11727BB49E38C1DE94CF94BF80C4BA56
SHA-512:	DB05E9D5B1E65C9FD7CDA725F54F48AD57B35799325CEE9BA8DC852256AC2C802AA2C853EF0E7E327DBC414F8C3FDDBFD2D52305532E3AD69AA62AC4EA343E5C
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="1342314" />.. <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\WER6219.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	48344
Entropy (8bit):	3.066109567350114
Encrypted:	false
SSDEEP:	768:/fHX382gE2hsUrLYKARAkNkiUQIyzU9XMPvw0:/fHX382CsUrLYKARAskihNU9XMPvw0
MD5:	54C5FA9810320E84420B5B29103D744D
SHA1:	6CE46C334A0FCB0C036BCD6C987CA01674896471
SHA-256:	07C0E1227916720162035 22FCF355B2D35C74777E35EB16B8C09A117A6010B28
SHA-512:	3F50E4D84BE8DF612BBA7F15DBFB2658ACB83A20547A0BAB93D5F7476769E4008C320E994C297487AD49F896A2129E6F9F2759CE4C3CEDB4A12657FB6C16343
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\WER66CE.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.69536143503136
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66CE.tmp.txt	
SSDEEP:	96:9GiZYWK5aBkdY1Y6W/5H6YEZ7FtBt8i0Tj0/w6UA1kaObMaz8IOq3:9jZDKxiVtZUmkaObMaz7Oq3
MD5:	E5DAA55DFDF64E4FD828D86A427F34A8
SHA1:	A1743376D125D03351D754B114121A79696341EC
SHA-256:	DDFB1CDEA7F63C7808AA474F23F299F6CD0189E80695D0C0F7D0B87BE293C3A5
SHA-512:	FBB6388AAE297315408093BC303D0A87ED52FBBE20F8911FEAA7DE77AD6ADC39CF65D28A534DB34DA4D4D3F70B0F60E3D4C03AF58E2C3D5D6A2206FF559A65 50
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.. ..../{...../{...../{b...../{.....Rich.....PE..L...C@.\.....''!.....b.....0.....~p....@.....p.....h.....0...T..... .....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T.. .U..T...U...U...U..T...URich...U.....PE..L...<@.\....."!.....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T..... .....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....* .....@..@.reloc..<.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5 A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&|.J...K&|.J...K&|uK...K&|.J...KRich...K.....PE..L...J@.\....."!.....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD 3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\....."!.....@.....0.....@.....0:.....:..d....`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy_InUse.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD 3D
Malicious:	false

C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy_InUse.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...;...X...;&..X...;...X..Rich.X.....PE..L....=.\.....".....!.....@.....0.....@.....0:.....:..d....`..p.....0.....p.....5..T.....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc...p....`.....(.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+l.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A.{*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....".....t.....0.....S....@.....P...P.....(.....`...T.....@.....0..D.....text..... ..`.rdata...l...0...n.. .....@..@.data.....@....rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\dI3hX2r.zip	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Reputation:	unknown
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o.....[.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`.M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\.../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.|k.5...XF.Y..lVVW..C..|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..|!.....O....M....>.>.$\.%..L.zF.I...3

C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false

C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....@.\....."!.....f.....p.....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\....."!.....f..... .....0.....@..... x..... .....p...T.....@.....\.....text...`..... ..`.rdata...@.....B.....@..@.data...l.....@....rsrc...x.... .....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich..j.....PE..L....<.\....."!.....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@.....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\lgpllibs.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F90313272081760 59CD03F53C8C5934C1050897F
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E676 5A

C:\Users\user\AppData\LocalLow\sG8rM8v\lgpllibs.dll	
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l..l..l.....l..~...l..9...l..~....l..~....l..~....l.....l..l....l..l..l..l..l..l..l..l..l..l..l..l..l..l..l..l..Rich.l.....PE..L...z@.\.....".....2.....t....@.....x.....T.....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\libEGL.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T-~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....".....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. ....."..@..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\nssdbm3.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwl41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E5E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4..5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L....@.\.....".....0.....0.....*q....@..... ?.....(@.....`..x. .....L.....p.....:.T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsr c...x....`.....@.....@..@.reloc.....p.....D.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[ .$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\....."!..... ... .....%.....0.....p...../...@.....5.....p7..x....P..x... .....@.....`..$...`1..T.....1..@.....0.,.....text...2..... ..... ..`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc. ..x....P.....8.....@..@.reloc..$....`.....<.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\qipcap.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91 A9E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W. .7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\....."!..... ..... `.....r....@.....$..P....@..x....."....P.. .... ..T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\softokn3.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C 6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@.\.....!.....b.....P.....|....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\ucrtbase.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2IleaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....I.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\ucrtbase.dll	

C:\Users\user\AppData\LocalLow\sG8rM8v\vcruntime140.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\A7F0.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a.....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata.....|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsrc..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@.....@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3F71.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\3F71.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3F71.exe.log	
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\1D34.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....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0...@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata.."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\1E7F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8lA0ZU3D80T840yWrxpzbgqruJnfed:lls8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i.hG..w.i.Richv.i.....PE..L....b_.....-.....0....@..... .....e..P.....2..... Y..@..... .0.....text..... ..`.rdata..D?...0...@..."....@..@.data...X....p...$...b.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\239.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3576320
Entropy (8bit):	**7.9976863291960605**
Encrypted:	**true**
SSDEEP:	49152:Y+RSFqeQKgdJee+ntOkgd+TuRCg+687ZEYNFvKfDIcK8nAONaGGh:Yb8eQKg+tOV0T0z875NFKfDPK8nASA
MD5:	5800952B83AECEFC3AA06CCB5B29A4C2
SHA1:	DB51DDBDF8B5B1ABECD6CFAB36514985F357F7A8
SHA-256:	B8BED0211974F32DB2C385350FB62954F0B0F335BC592B51144027956524D674
SHA-512:	2A490708A2C5B742CEB14DE6E2180C4CB606FCCEB5F17DE69249CF532EDC37B984686B534A88AE861CC38471C5892785C26DA68C4F662959542458C583E77E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\239.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....!7. .....|.N. .... M.....@.....0.....@.....@ ...z.....@..... ...0.....@.....x+...P.....@.....1.....@....rsrc..... M.....L0.....@....28gybOo.....N.....1.....@....ada ta.....pS.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\2D04.exe

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

C:\Users\user\AppData\Local\Temp\2DB3.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	322560
Entropy (8bit):	6.7095586688781985
Encrypted:	false
SSDEEP:	6144:nOOJ91Tu9Vc1ye3MKfa+zqKnvDfsxa6hkZC15O5Pdz:nRJ91TYWym1ffzvD36YC15E
MD5:	6009BCB680BE6C0F656AA157E56423DC
SHA1:	FA9BA68D6B2026683BD392259BA26D7D468AEA7E
SHA-256:	5C037C7C1338CF54A9D1E81B74BB4AD003E1A254069A03499426EC1600A748D9
SHA-512:	5ECE7D9531051C951DFA0CF9533AB778B468EBE3EBE5D7B8A934D408E69BE910F244C59810A5FB41376B1CA7E5EB78DBF514032354EF047D00F043E2A17795E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...9.-`.....@.....$...(.....0...@.....D..... .text..... ..`.data.....@....gave.....@....noduf.....@....gafal.....@....rsrc..... ....@..@.reloc..dF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\309C.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.693203776268283
Encrypted:	false
SSDEEP:	6144:ea1ijIN+Aee6+saxCBxHoM3sDKOd4xncb3wQ:eag8N+Ae2sTvIM5OYncb
MD5:	8B25D9317E18654C3F83EF8630D1DE16
SHA1:	B4503FB92DCB9B4B90E2CD2A534AE38C08F0589A
SHA-256:	1BE428F924402D7CC4586CA37A9E843C869B394F85085DB5E4E85D150AA87E04
SHA-512:	36AD3AD9E9DF0D52DEB4F350880BAEFA3F6871945D566118573AD1511F9CCDE55A5EC205AADCB7ACA156AAFC881587551996BBE27A47B27F8BD596CBCE04E 7B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\309C.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...5._.....@.....D...(.....0...@.....D..... text..... ..`.data.....@....nife.....@....kiza.....@....lagoti.....@....rsrc.....@..@. reloc..ZF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\3F71.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....I... ...`....@.. ..... ..@.....`I..K...`..... ..... ..H.....text....).. ...*..... ..`.rsrc.....`.....@....reloc..... .....0.....@..B.....I.....H.....?.....hX..}.....(...*..0..,.....(d...8....*.~....u....s....z&8.....8.....*.....*....(d...(....*...j*.... ..*.....*.....*.....*....(...*.~(....(^...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\A7F0.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**
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\BC16.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427 D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\BC16.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..U(...(...(...6.).1...6.?.W....I..+...(.....6.8.....6.(.)...6.-.)...Rich(.....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8.....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|.....@..@.reloc..4F...0...H...I.....@..B.....

C:\Users\user\AppData\Local\Temp\D452.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3576320
Entropy (8bit):	**7.9976863291960605**
Encrypted:	**true**
SSDEEP:	49152:Y+RSFqeQKgdJee+ntOkgd+TuRCg+687ZEYNFvKfDIcK8nAONaGGh:Yb8eQKg+tOV0T0z875NFKfDPK8nASA
MD5:	5800952B83AECEFC3AA06CCB5B29A4C2
SHA1:	DB51DDBDF8B5B1ABECD6CFAB36514985F357F7A8
SHA-256:	B8BED0211974F32DB2C385350FB62954F0B0F335BC592B51144027956524D674
SHA-512:	2A490708A2C5B742CEB14DE6E2180C4CB606FCCEB5F17DE69249CF532EDC37B984686B534A88AE861CC38471C5892785C26DA68C4F662959542458C583E77E3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....!7.....|.N. .... M.....@.....0.....@.....@...z.....@..... ...0.....@.....x+...P.....@.....1.....@....rsrc..... M.....L0.....@....28gybOo.....N.....1.....@....adata.....pS.....6.....@.....

C:\Users\user\AppData\Local\Temp\tejjnepq.exe	
Process:	C:\Users\user\AppData\Local\Temp\309C.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15600640
Entropy (8bit):	3.7768495924879493
Encrypted:	false
SSDEEP:	6144:xa1ijIN+Aee6+saxCBxHoM3sDKOd4xncb3wQ:xag8N+Ae2sTvIM5OYncb
MD5:	310337FA2432C256984AA89486B74D95
SHA1:	A5234B3EA059F3A553C55D262BC2B7CB347ED12E
SHA-256:	966557B6F228EDA641E155A858F574654E431743311D83E4841013D63044A994
SHA-512:	8E9F3F6404445BAE167845B77D173AA8FF982DFD7EB998FD33FFD57AC92FB111B4FEAB934A7A961349A00D7D0B925CD3451C814779E33E8FE9454BFED92C671
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R.....PE..L...5._..... .....@.....D...(.....0...@.....D.....text..... ..`.data.....@....nife.....@....kiza.....@....lagoti.....@....rsrc.....@..@.reloc..ZF.....p.....@..B.....

C:\Users\user\AppData\Roaming\gdrgbdj	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.6822544763975475
Encrypted:	false
SSDEEP:	6144:dTlJAM3EC/eddUaHyF9mqcMuS9W1uPVeHcENjQe:dY3ElWU9/pcO9rPVeqe
MD5:	9AF4D2022DC05C2DBBC4D218A8F0974C
SHA1:	F87C7511D2C4EA4894603D3CFDDD478C8C2B3EAD
SHA-256:	C8FE81088B2CAA9DF35D92A588FB266A145C95B81B5C66D5BFE181FA73B17D82
SHA-512:	71230365C1E7ACB2B8740434322A1F8AA87D417EADBB6D8D7FB1B2BF9ECB1247BFEC2B2568812F22D61F125B3F4F739989121B5E17C63CCD580D8E8B059C63C0
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R.....PE..L.....-`.....@.....(.....0...@.....D.....text...t..... ..`.data.....@....zug.....@....nafuti.....@....karom.....@....rsrc.....@..@.reloc...F.....H.....@..B.....

C:\Users\user\AppData\Roaming\gdrgbdj: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\SysWOW64\ozuqupbe\tejjnepq.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15600640
Entropy (8bit):	3.7768495924879493
Encrypted:	false
SSDEEP:	6144:xa1ijIN+Aee6+saxCBxHoM3sDKOd4xncb3wQ:xag8N+Ae2sTvIM5OYncb
MD5:	310337FA2432C256984AA89486B74D95
SHA1:	A5234B3EA059F3A553C55D262BC2B7CB347ED12E
SHA-256:	966557B6F228EDA641E155A858F574654E431743311D83E4841013D63044A994
SHA-512:	8E9F3F6404445BAE167845B77D173AA8FF982DFD7EB998FD33FFD57AC92FB111B4FEAB934A7A961349A00D7D0B925CD3451C814779E33E8FE9454BFED92C671
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...5._..... .....@.....D...(.....0...@.....D..... text..... ..`.data.....@....nife.....@....kiza.....@....lagoti.....@....rsrc.....@..@. reloc..ZF.....p.....@..B..... .....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2133338797531135
Encrypted:	false
SSDEEP:	12288:mxKBe46xNAzd/V0PjNF8ULoAGvE+dAHmdCAsKruqm03eS/SXjZoznH:AKBe46xNAzZV0PsZVrf3
MD5:	14806013B9BD43BA646F753EAFF9B390
SHA1:	1075C9847B578FB5C4AC7E5D353C7CA37D9EB28F
SHA-256:	3DFE3035D3C3273B157B5B4AC66EAD61262F684B5C6ADE9AC0A88B6EE432BBE7

C:\Windows\appcompat\Programs\Amcache.hve	
SHA-512:	2696AAB6EBADF79A9999B8E1EA97DCAB7352F7DC4236AD07EC5FF8D9BFBD37F344EFA3B0F2977DDCCD277BE33E83248F83B6290E3C19D831EE751054B3BE0BCC
Malicious:	false
Reputation:	unknown
Preview:	regfV...V...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>.L.v..... .....)G..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.458017950724434
Encrypted:	false
SSDEEP:	384:v5gC5BhIpnc8aTVgGpKLXZmnnBpx9787W0:a8nSc8AVgGYLXEnnBJ87W
MD5:	1E22C2B14F4E95B9E20BCC6DC83DA762
SHA1:	14496E143D23B42C0D5C2DE1B9D0F0495607443B
SHA-256:	6D7DCA21B04F335CA0A1C3ABE8C0F14736D1CB2BA0AB22602F395B64E90B3A76
SHA-512:	8106412CC3BA60DD5EA0CE230AB2FE504D74CB7F7AF93B3CF79B312CCFC873DCEB09918806FD98727C76B7FAD813B2331289DC61826FD9A50757D69E3D5AD09
Malicious:	false
Reputation:	unknown
Preview:	regfU...U...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>.L.v..... .....)G.HvLE.N.....U.....&X}$...`..4w-oB.....`... ..hbin.....p.\..,.....nk,.w%O.v..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .w%O.v..... ....Z.....Root.....lf.....Root....nk .w%O.v.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck.....p...

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.6822544763975475
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zmbGUZTICp.exe
File size:	319488

General

MD5:	9af4d2022dc05c2dbbc4d218a8f0974c
SHA1:	f87c7511d2c4ea4894603d3cfddd478c8c2b3ead
SHA256:	c8fe81088b2caa9df35d92a588fb266a145c95b81b5c66d5bfe181fa73b17d82
SHA512:	71230365c1e7acb2b8740434322a1f8aa87d417eadbb6d8d7fb1b2bf9ecb1247bfec2b2568812f22d61f125b3f4f739989121b5e17c63ccd580d8e8b059c63c0
SSDEEP:	6144:dTIJAM3EC/eddUaHyF9mqcMuS9W1uPVeHcENjQe:dY3EIWU9/pcO9rPVeqe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R.....g.R..])...R...S...R.....R.....R.....R.Rich..R.....PE..L.....-`.....

File Icon

Icon Hash:	c8d0d8e0f8e0f4e0

Static PE Info

General

Entrypoint:	0x41b3e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x602DA0A7 [Wed Feb 17 23:03:03 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	80fec6fca6f81033220e34b44810dbfd

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e474	0x3e600	False	0.581001847445	data	6.95435391538	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x11c988	0x1800	False	0.33984375	data	3.45568717424	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.zug	0x15d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.nafuti	0x15e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.karom	0x15f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x160000	0x83b8	0x8400	False	0.597064393939	data	5.82148733152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x169000	0x46fa	0x4800	False	0.347493489583	data	3.69367482599	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
Spanish	Colombia	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:43:44.633687973 CET	192.168.2.6	8.8.8.8	0x8523	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:45.077446938 CET	192.168.2.6	8.8.8.8	0x6b8b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:45.249844074 CET	192.168.2.6	8.8.8.8	0xb24d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:45.744626045 CET	192.168.2.6	8.8.8.8	0x7fc2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:46.185400963 CET	192.168.2.6	8.8.8.8	0x1213	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:46.366353035 CET	192.168.2.6	8.8.8.8	0x7ee1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:48.028930902 CET	192.168.2.6	8.8.8.8	0xf8ea	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:48.198477983 CET	192.168.2.6	8.8.8.8	0xfb93	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:48.390367031 CET	192.168.2.6	8.8.8.8	0x1b5e	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:50.684801102 CET	192.168.2.6	8.8.8.8	0xc627	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:50.858036041 CET	192.168.2.6	8.8.8.8	0x27bd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.026129961 CET	192.168.2.6	8.8.8.8	0x4517	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.332477093 CET	192.168.2.6	8.8.8.8	0x1fe2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.513241053 CET	192.168.2.6	8.8.8.8	0x2f07	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.683567047 CET	192.168.2.6	8.8.8.8	0xc35c	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.847625017 CET	192.168.2.6	8.8.8.8	0x34a3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:43:52.016745090 CET	192.168.2.6	8.8.8.8	0xad87	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.187030077 CET	192.168.2.6	8.8.8.8	0x9243	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.367851019 CET	192.168.2.6	8.8.8.8	0xbcdb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.539206982 CET	192.168.2.6	8.8.8.8	0x6463	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.230817080 CET	192.168.2.6	8.8.8.8	0x3b21	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.404676914 CET	192.168.2.6	8.8.8.8	0x5292	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.578222036 CET	192.168.2.6	8.8.8.8	0x6dba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.775106907 CET	192.168.2.6	8.8.8.8	0xfaf6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:58.634373903 CET	192.168.2.6	8.8.8.8	0xcd6c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:58.833694935 CET	192.168.2.6	8.8.8.8	0x9e96	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.021801949 CET	192.168.2.6	8.8.8.8	0xfa32	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.187329054 CET	192.168.2.6	8.8.8.8	0x4146	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:01.036515951 CET	192.168.2.6	8.8.8.8	0x798d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:01.201462030 CET	192.168.2.6	8.8.8.8	0xa9a1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:01.368493080 CET	192.168.2.6	8.8.8.8	0xae6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.079658031 CET	192.168.2.6	8.8.8.8	0x63ad	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:12.796425104 CET	192.168.2.6	8.8.8.8	0xc715	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:22.727591991 CET	192.168.2.6	8.8.8.8	0x1b8a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:22.909961939 CET	192.168.2.6	8.8.8.8	0xa1e2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:23.076080084 CET	192.168.2.6	8.8.8.8	0x8f81	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:23.241534948 CET	192.168.2.6	8.8.8.8	0xa5c6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:23.735255957 CET	192.168.2.6	8.8.8.8	0xe7ca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.017632008 CET	192.168.2.6	8.8.8.8	0x9fdc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.186546087 CET	192.168.2.6	8.8.8.8	0xf2be	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.353194952 CET	192.168.2.6	8.8.8.8	0xce72	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.792356968 CET	192.168.2.6	8.8.8.8	0xdfc3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.984512091 CET	192.168.2.6	8.8.8.8	0xe353	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.174129009 CET	192.168.2.6	8.8.8.8	0x6a12	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.381947994 CET	192.168.2.6	8.8.8.8	0x1cc3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.549240112 CET	192.168.2.6	8.8.8.8	0x74c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.719943047 CET	192.168.2.6	8.8.8.8	0xd01f	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:28.817889929 CET	192.168.2.6	8.8.8.8	0xfbca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:28.989167929 CET	192.168.2.6	8.8.8.8	0x47e3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.163213015 CET	192.168.2.6	8.8.8.8	0x6797	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.556011915 CET	192.168.2.6	8.8.8.8	0x8873	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.749594927 CET	192.168.2.6	8.8.8.8	0x4608	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:44:29.934479952 CET	192.168.2.6	8.8.8.8	0xaef6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.115786076 CET	192.168.2.6	8.8.8.8	0x8de9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.289908886 CET	192.168.2.6	8.8.8.8	0x3976	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.467227936 CET	192.168.2.6	8.8.8.8	0x94c2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.641408920 CET	192.168.2.6	8.8.8.8	0xc9ba	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:33.873652935 CET	192.168.2.6	8.8.8.8	0x2966	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:34.136259079 CET	192.168.2.6	8.8.8.8	0x58f7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.034046888 CET	192.168.2.6	8.8.8.8	0xcd85	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.399838924 CET	192.168.2.6	8.8.8.8	0x8f64	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.576474905 CET	192.168.2.6	8.8.8.8	0x7ce8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.841660023 CET	192.168.2.6	8.8.8.8	0x24fc	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.192677975 CET	192.168.2.6	8.8.8.8	0x7b69	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.358232975 CET	192.168.2.6	8.8.8.8	0xcb45	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.533195972 CET	192.168.2.6	8.8.8.8	0x3945	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.725630999 CET	192.168.2.6	8.8.8.8	0x3f25	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:53.396308899 CET	192.168.2.6	8.8.8.8	0x935c	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:55.346837997 CET	192.168.2.6	8.8.8.8	0xb5f1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:55.518959045 CET	192.168.2.6	8.8.8.8	0x5f2b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:55.711636066 CET	192.168.2.6	8.8.8.8	0xfd7b	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:59.094153881 CET	192.168.2.6	8.8.8.8	0x6c83	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:59.588779926 CET	192.168.2.6	8.8.8.8	0xa9ea	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:59.792838097 CET	192.168.2.6	8.8.8.8	0xc644	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:03.762748003 CET	192.168.2.6	8.8.8.8	0x3885	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:03.944444895 CET	192.168.2.6	8.8.8.8	0x721b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:04.970577955 CET	192.168.2.6	8.8.8.8	0x721b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:05.367841005 CET	192.168.2.6	8.8.8.8	0xaea6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:05.562896967 CET	192.168.2.6	8.8.8.8	0x5e9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.775547028 CET	192.168.2.6	8.8.8.8	0x2626	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:43.545881033 CET	192.168.2.6	8.8.8.8	0xada	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:43:44.922651052 CET	8.8.8.8	192.168.2.6	0x8523	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:45.096684933 CET	8.8.8.8	192.168.2.6	0x6b8b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:45.589972973 CET	8.8.8.8	192.168.2.6	0xb24d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:43:46.031016111 CET	8.8.8.8	192.168.2.6	0x7fc2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:46.204824924 CET	8.8.8.8	192.168.2.6	0x1213	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:46.676295996 CET	8.8.8.8	192.168.2.6	0x7ee1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:48.048309088 CET	8.8.8.8	192.168.2.6	0xf8ea	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:48.216015100 CET	8.8.8.8	192.168.2.6	0xfb93	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:48.703352928 CET	8.8.8.8	192.168.2.6	0x1b5e	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:50.703531981 CET	8.8.8.8	192.168.2.6	0xc627	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:50.876921892 CET	8.8.8.8	192.168.2.6	0x27bd	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.042943001 CET	8.8.8.8	192.168.2.6	0x4517	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.352010012 CET	8.8.8.8	192.168.2.6	0x1fe2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.532625914 CET	8.8.8.8	192.168.2.6	0x2f07	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.788089991 CET	8.8.8.8	192.168.2.6	0xc35c	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:51.869045019 CET	8.8.8.8	192.168.2.6	0x34a3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.034235001 CET	8.8.8.8	192.168.2.6	0xad87	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.204862118 CET	8.8.8.8	192.168.2.6	0x9243	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.387742996 CET	8.8.8.8	192.168.2.6	0xbcdb	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:52.558407068 CET	8.8.8.8	192.168.2.6	0x6463	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.249917984 CET	8.8.8.8	192.168.2.6	0x3b21	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.421777010 CET	8.8.8.8	192.168.2.6	0x5292	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.597048998 CET	8.8.8.8	192.168.2.6	0x6dba	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:54.793905973 CET	8.8.8.8	192.168.2.6	0xfaf6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:58.653935909 CET	8.8.8.8	192.168.2.6	0xcd6c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:58.851239920 CET	8.8.8.8	192.168.2.6	0x9e96	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.039109945 CET	8.8.8.8	192.168.2.6	0xfa32	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.207215071 CET	8.8.8.8	192.168.2.6	0x4146	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.207215071 CET	8.8.8.8	192.168.2.6	0x4146	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:43:59.207215071 CET	8.8.8.8	192.168.2.6	0x4146	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.207215071 CET	8.8.8.8	192.168.2.6	0x4146	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:43:59.207215071 CET	8.8.8.8	192.168.2.6	0x4146	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:01.056061029 CET	8.8.8.8	192.168.2.6	0x798d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:01.218846083 CET	8.8.8.8	192.168.2.6	0xa9a1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:01.385657072 CET	8.8.8.8	192.168.2.6	0xae6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.106473923 CET	8.8.8.8	192.168.2.6	0x63ad	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.106473923 CET	8.8.8.8	192.168.2.6	0x63ad	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.106473923 CET	8.8.8.8	192.168.2.6	0x63ad	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.106473923 CET	8.8.8.8	192.168.2.6	0x63ad	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.106473923 CET	8.8.8.8	192.168.2.6	0x63ad	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:10.106473923 CET	8.8.8.8	192.168.2.6	0x63ad	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:12.815992117 CET	8.8.8.8	192.168.2.6	0xc715	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:22.744677067 CET	8.8.8.8	192.168.2.6	0x1b8a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:22.927047968 CET	8.8.8.8	192.168.2.6	0xa1e2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:23.095449924 CET	8.8.8.8	192.168.2.6	0x8f81	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:23.580354929 CET	8.8.8.8	192.168.2.6	0xa5c6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:23.754772902 CET	8.8.8.8	192.168.2.6	0xe7ca	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.036843061 CET	8.8.8.8	192.168.2.6	0x9fdc	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.205995083 CET	8.8.8.8	192.168.2.6	0xf2be	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.643091917 CET	8.8.8.8	192.168.2.6	0xce72	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:24.812130928 CET	8.8.8.8	192.168.2.6	0xdfc3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.001595020 CET	8.8.8.8	192.168.2.6	0xe353	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.193222046 CET	8.8.8.8	192.168.2.6	0x6a12	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:44:25.401681900 CET	8.8.8.8	192.168.2.6	0x1cc3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.568310022 CET	8.8.8.8	192.168.2.6	0x74c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:25.739336014 CET	8.8.8.8	192.168.2.6	0xd01f	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:28.837270975 CET	8.8.8.8	192.168.2.6	0xfbca	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.006572962 CET	8.8.8.8	192.168.2.6	0x47e3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.187659979 CET	8.8.8.8	192.168.2.6	0x6797	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.187659979 CET	8.8.8.8	192.168.2.6	0x6797	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.575335979 CET	8.8.8.8	192.168.2.6	0x8873	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.766783953 CET	8.8.8.8	192.168.2.6	0x4608	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:29.957333088 CET	8.8.8.8	192.168.2.6	0xaef6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.132836103 CET	8.8.8.8	192.168.2.6	0x8de9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.313347101 CET	8.8.8.8	192.168.2.6	0x3976	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.487637043 CET	8.8.8.8	192.168.2.6	0x94c2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:30.968112946 CET	8.8.8.8	192.168.2.6	0xc9ba	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:33.891127110 CET	8.8.8.8	192.168.2.6	0x2966	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:34.155517101 CET	8.8.8.8	192.168.2.6	0x58f7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.060764074 CET	8.8.8.8	192.168.2.6	0xcd85	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.421783924 CET	8.8.8.8	192.168.2.6	0x8f64	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.607868910 CET	8.8.8.8	192.168.2.6	0x7ce8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:35.867207050 CET	8.8.8.8	192.168.2.6	0x24fc	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.210330963 CET	8.8.8.8	192.168.2.6	0x7b69	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.377250910 CET	8.8.8.8	192.168.2.6	0xcb45	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.552405119 CET	8.8.8.8	192.168.2.6	0x3945	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:47.744528055 CET	8.8.8.8	192.168.2.6	0x3f25	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:53.510515928 CET	8.8.8.8	192.168.2.6	0x935c	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:55.367500067 CET	8.8.8.8	192.168.2.6	0xb5f1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:44:55.538839102 CET	8.8.8.8	192.168.2.6	0x5f2b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:55.733985901 CET	8.8.8.8	192.168.2.6	0xfd7b	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:59.429790974 CET	8.8.8.8	192.168.2.6	0x6c83	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:59.608838081 CET	8.8.8.8	192.168.2.6	0xa9ea	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:44:59.810125113 CET	8.8.8.8	192.168.2.6	0xc644	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:03.782224894 CET	8.8.8.8	192.168.2.6	0x3885	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:04.989928961 CET	8.8.8.8	192.168.2.6	0x721b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:05.270993948 CET	8.8.8.8	192.168.2.6	0x721b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:05.384814024 CET	8.8.8.8	192.168.2.6	0xaea6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:05.585026979 CET	8.8.8.8	192.168.2.6	0x5e9	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.916101933 CET	8.8.8.8	192.168.2.6	0x2626	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.916101933 CET	8.8.8.8	192.168.2.6	0x2626	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.916101933 CET	8.8.8.8	192.168.2.6	0x2626	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.916101933 CET	8.8.8.8	192.168.2.6	0x2626	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.916101933 CET	8.8.8.8	192.168.2.6	0x2626	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:13.916101933 CET	8.8.8.8	192.168.2.6	0x2626	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:45:43.565538883 CET	8.8.8.8	192.168.2.6	0xada	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- jsplktel.org
  - host-data-coin-11.com
- ivfhujym.net
- nipgcts.com
- bxide.net
- rgxie.com
- jnolpkdknj.net

- stbgsgw.com
- uknnqg.net
- data-host-coin-8.com
- otraxus.net
- qsvubjh.com
- wwmessepf.com
- nlxvu.net
- xjjyulxcfs.com
- unicupload.top
- jdecaoxkel.org
- uhcpfe.com
- qwfybhxm.org
- odyvlsasq.com
- eahqahqv.net
- daixhajgka.com
- cghrkunn.com
- pfwxavhis.net
- 185.7.214.171:8080
- ebgfrfm.org
- covjb.org
- rguskwyq.org
- vpvxxeoni.org
- arpfh.net
- nnyntvsvo.org
- sopssp.net
- vhclpnkvya.com
- lphbdueqjj.com
- kakjdonis.net
- gpnorygxw.org
- ackvfel.net

- jrhwfdx.org
- yrgforv.org
- hwivor.org
- wpctxossq.com
- kkrgipwnic.net
- jqlty.com
- uqclrrn.org
- khnjbia.net
- gtapfy.com
- xokmpq.org
- nbjhuloh.com
- cifusjcgu.net
- jfioua.org
- usyqjbp.org
- lepql.com
- txdwk.net
- a0621298.xsph.ru
- phiqqvf.net
- tmtuscxant.net
- jpiimxqwms.net
- 185.215.113.35
- lsmlx.org
- etxdwvf.com
- 185.163.204.22
- 185.163.204.24
- lnxul.net
- krijk.com
- brqduyej.org
- imxgr.net
- koqghysihf.net

- kiocvqo.net
- kcgghyab.com
- smrwgxji.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: zmbGUZTICp.exe PID: 4404 Parent PID: 5260

General

Start time:	10:43:02
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\zmbGUZTICp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\zmbGUZTICp.exe"
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	9AF4D2022DC05C2DBBC4D218A8F0974C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: zmbGUZTICp.exe PID: 3416 Parent PID: 4404

General

Start time:	10:43:04
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\zmbGUZTICp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\zmbGUZTICp.exe"
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	9AF4D2022DC05C2DBBC4D218A8F0974C
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: 00000001.00000002.408517834.00000000005C1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.408471084.0000000000580000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3440 Parent PID: 3416

General

Start time:	10:43:10
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: 00000002.00000000.392111314.0000000004151000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: gdrgbdj PID: 2468 Parent PID: 936

General

Start time:	10:43:45
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\gdrgbdj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gdrgbdj
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	9AF4D2022DC05C2DBBC4D218A8F0974C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: gdrgbdj PID: 3492 Parent PID: 2468

General

Start time:	10:43:47
Start date:	14/01/2022

Path:	C:\Users\user\AppData\Roaming\gdrgbdj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gdrgbdj
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	9AF4D2022DC05C2DBBC4D218A8F0974C
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: 00000006.00000002.462828818.00000000020A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000002.462437704.0000000000460000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 1E7F.exe PID: 5200 Parent PID: 3440

General

Start time:	10:43:49
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\1E7F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1E7F.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	moderate

Analysis Process: 2DB3.exe PID: 5640 Parent PID: 3440

General

Start time:	10:43:52
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2DB3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2DB3.exe
Imagebase:	0x400000
File size:	322560 bytes
MD5 hash:	6009BCB680BE6C0F656AA157E56423DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.462596398.0000000000942000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000008.00000002.462596398.0000000000942000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: svchost.exe PID: 5636 Parent PID: 560

General

Start time:	10:43:52
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5668 Parent PID: 5636

General

Start time:	10:43:53
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 5200 -ip 5200
Imagebase:	0x1010000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 309C.exe PID: 5132 Parent PID: 3440

General

Start time:	10:43:56
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\309C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\309C.exe
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	8B25D9317E18654C3F83EF8630D1DE16
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: 0000000B.00000003.465535302.0000000000660000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000000B.00000002.483029167.0000000000630000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000000B.00000002.482701616.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: WerFault.exe PID: 5648 Parent PID: 5200

General

Start time:	10:43:58
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5200 -s 520
Imagebase:	0x1010000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: 3F71.exe PID: 5196 Parent PID: 3440

General

Start time:	10:43:59
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3F71.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3F71.exe
Imagebase:	0x130000
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: 0000000D.00000002.509652789.00000000035F1000.00000004.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 852 Parent PID: 5132

General

Start time:	10:44:02
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\ozuqupbe\
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 5296 Parent PID: 852

General

Start time:	10:44:02
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5820 Parent PID: 5132

General

Start time:	10:44:03
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\tejjnepq.exe" C:\Windows\SysWOW64\ozuqupbe\

Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 6068 Parent PID: 5820

General

Start time:	10:44:03
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 4636 Parent PID: 5132

General

Start time:	10:44:03
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create ozuqupbe binPath= "C:\Windows\SysWOW64\ozuqupbe\tejjnepq.exe /d\"C:\Users\user\AppData\Local\Temp\309C.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x7ff7ebed0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 3500 Parent PID: 4636

General

Start time:	10:44:04
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5360 Parent PID: 5132

General

Start time:	10:44:04
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description ozuqupbe "wifi internet conection
Imagebase:	0x1100000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 1360 Parent PID: 5360

General

Start time:	10:44:05
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 1148 Parent PID: 5132

General

Start time:	10:44:05
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start ozuqupbe
Imagebase:	0x1100000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 1352 Parent PID: 1148

General

Start time:	10:44:06
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tejjnepq.exe PID: 2320 Parent PID: 560

General

Start time:	10:44:06
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\ozuqupbe\tejjnepq.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ozuqupbe\tejjnepq.exe /d"C:\Users\user\AppData\Local\Temp\309C.exe"
Imagebase:	0x400000
File size:	15600640 bytes
MD5 hash:	310337FA2432C256984AA89486B74D95
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: 00000018.00000003.484958252.0000000000650000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000018.00000002.487069234.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000018.00000002.488137960.0000000000ED0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000018.00000002.487496290.0000000000630000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: netsh.exe PID: 5308 Parent PID: 5132

General

Start time:	10:44:06
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x9e0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3532 Parent PID: 5308

General

Start time:	10:44:07
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4692 Parent PID: 2320

General

Start time:	10:44:08
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xf20000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001B.00000002.639945191.00000000004D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 3F71.exe PID: 1508 Parent PID: 5196

General

Start time:	10:44:10
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\3F71.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3F71.exe
Imagebase:	0xfa0000
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: 0000001C.00000000.502914721.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001C.00000000.504088961.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001C.00000000.503538300.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001C.00000000.504557008.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 5368 Parent PID: 560

General

Start time:	10:44:11
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5728 Parent PID: 560

General

Start time:	10:44:22
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: A7F0.exe PID: 2200 Parent PID: 3440

General

Start time:	10:44:26
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\A7F0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A7F0.exe
Imagebase:	0x400000
File size:	905216 bytes
MD5 hash:	852D86F5BC34BF4AF7FA89C60569DF13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000001F.00000002.640601105.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000001F.00000002.662718681.0000000004D60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000001F.00000003.553585077.0000000004E00000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis