ID: 547895
Sample Name: nkINykHreE.exe
Cookbook: default.jbs
Time: 19:31:08
Date: 04/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

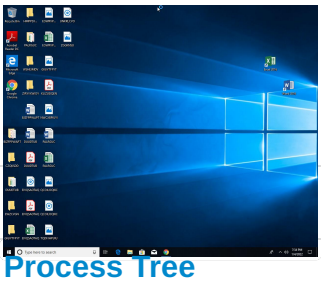
Windows Analysis Report nkINykHreE.exe

Overview

General Information

Sample Name:	nkINykHreE.exe
Analysis ID:	547895
MD5:	dc67c627917ff97..
SHA1:	4b7528999ad609..
SHA256:	26a4c5b36d9fde8.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

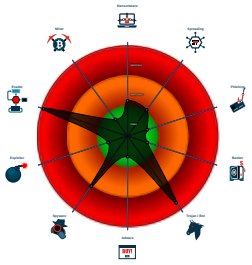
RedLine SmokeLoader Tofsee Vidar

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- nkINykHreE.exe (PID: 800 cmdline: "C:\Users\user\Desktop\nkINykHreE.exe" MD5: DC67C627917FF9724F3C1E6DB5F2DC27)
  - nkINykHreE.exe (PID: 3092 cmdline: "C:\Users\user\Desktop\nkINykHreE.exe" MD5: DC67C627917FF9724F3C1E6DB5F2DC27)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 115B.exe (PID: 340 cmdline: C:\Users\user\AppData\Local\Temp\115B.exe MD5: DC67C627917FF9724F3C1E6DB5F2DC27)
        - 115B.exe (PID: 1412 cmdline: C:\Users\user\AppData\Local\Temp\115B.exe MD5: DC67C627917FF9724F3C1E6DB5F2DC27)
      - 2997.exe (PID: 6936 cmdline: C:\Users\user\AppData\Local\Temp\2997.exe MD5: 1F935BFFF0F8128972BC69625E5B2A6C)
      - 18D.exe (PID: 4992 cmdline: C:\Users\user\AppData\Local\Temp\18D.exe MD5: B7B184D2B0910148CABB9B5E915753D6)
        - cmd.exe (PID: 6552 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\dbgxuqbr\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 1768 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\sdiimdop.exe" C:\Windows\SysWOW64\dbgxuqbr\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2856 cmdline: C:\Windows\System32\sc.exe" create dbgxuqbr binPath= "C:\Windows\SysWOW64\dbgxuqbr\sdiimdop.exe /d\"C:\Users\user\AppData\Local\Temp\18D.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 3952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 4784 cmdline: C:\Windows\System32\sc.exe" description dbgxuqbr "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 4696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6404 cmdline: "C:\Windows\System32\sc.exe" start dbgxuqbr MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 7000 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: 2076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - CBA.exe (PID: 5652 cmdline: C:\Users\user\AppData\Local\Temp\CBA.exe MD5: 6C72997AA5DD44A44B27BD36347BAED9)
        - CBA.exe (PID: 7052 cmdline: C:\Users\user\AppData\Local\Temp\CBA.exe MD5: 6C72997AA5DD44A44B27BD36347BAED9)
      - 2757.exe (PID: 2904 cmdline: C:\Users\user\AppData\Local\Temp\2757.exe MD5: 67B848B139E584BF3361A51160FC6731)
      - 4187.exe (PID: 6064 cmdline: C:\Users\user\AppData\Local\Temp\4187.exe MD5: C085684DB882063C21F18D251679B0CC)
      - 13E0.exe (PID: 3952 cmdline: C:\Users\user\AppData\Local\Temp\13E0.exe MD5: AA519DEEB511E886E73F8E0256180800)
      - 1B15.exe (PID: 6380 cmdline: C:\Users\user\AppData\Local\Temp\1B15.exe MD5: D8B78E7D4D822C10CCE3654D7F9E4931)
      - 28C2.exe (PID: 6488 cmdline: C:\Users\user\AppData\Local\Temp\28C2.exe MD5: F111EE7C9F26F50F9EFEEB6EF6C32A3C)
      - 315E.exe (PID: 7032 cmdline: C:\Users\user\AppData\Local\Temp\315E.exe MD5: 4FB3361FFC7E5DD2FAD4413866DB6D2E)
      - 4583.exe (PID: 4784 cmdline: C:\Users\user\AppData\Local\Temp\4583.exe MD5: 11124BB02075AD2D9D750343B42F932A)
- svchost.exe (PID: 6444 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6644 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6720 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6816 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6868 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6888 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4176 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 4140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- haifbcd (PID: 2908 cmdline: C:\Users\user\AppData\Roaming\haifbcd MD5: DC67C627917FF9724F3C1E6DB5F2DC27)
  - haifbcd (PID: 4544 cmdline: C:\Users\user\AppData\Roaming\haifbcd MD5: DC67C627917FF9724F3C1E6DB5F2DC27)
- sdiimdop.exe (PID: 4560 cmdline: C:\Windows\SysWOW64\dbgxuqbr\sdiimdop.exe /d"C:\Users\user\AppData\Local\Temp\18D.exe" MD5: F548B3529CA470C25E50AF6220AD3098)
  - svchost.exe (PID: 5180 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 7064 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- scifbcd (PID: 6852 cmdline: C:\Users\user\AppData\Roaming\scifbcd MD5: 1F935BFFF0F8128972BC69625E5B2A6C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.282842442.0000000003A61000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000011.00000002.370053936.0000000000751000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000031.00000002.609571282.0000000003AA7000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000002F.00000002.595854272.0000000000DF0000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000002F.00000002.595854272.0000000000DF0000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 46 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.nkINykHreE.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
18.2.18D.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
31.2.sdiimdop.exe.540e50.1.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
13.2.haifbcd.4715a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
34.2.svchost.exe.2bb0000.0.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 24 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Svchost Process

Sigma detected: Netsh Port or Application Allowed

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

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

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:

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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

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

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

Anti Debugging:

Tries to detect sandboxes and other dynamic analysis tools (window names)

Hides threads from debuggers

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

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

Modifies the windows firewall

Stealing of Sensitive Information:

- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- Yara detected Vidar stealer
- Yara detected Tofsee
- Tries to harvest and steal browser information (history, passwords, etc)

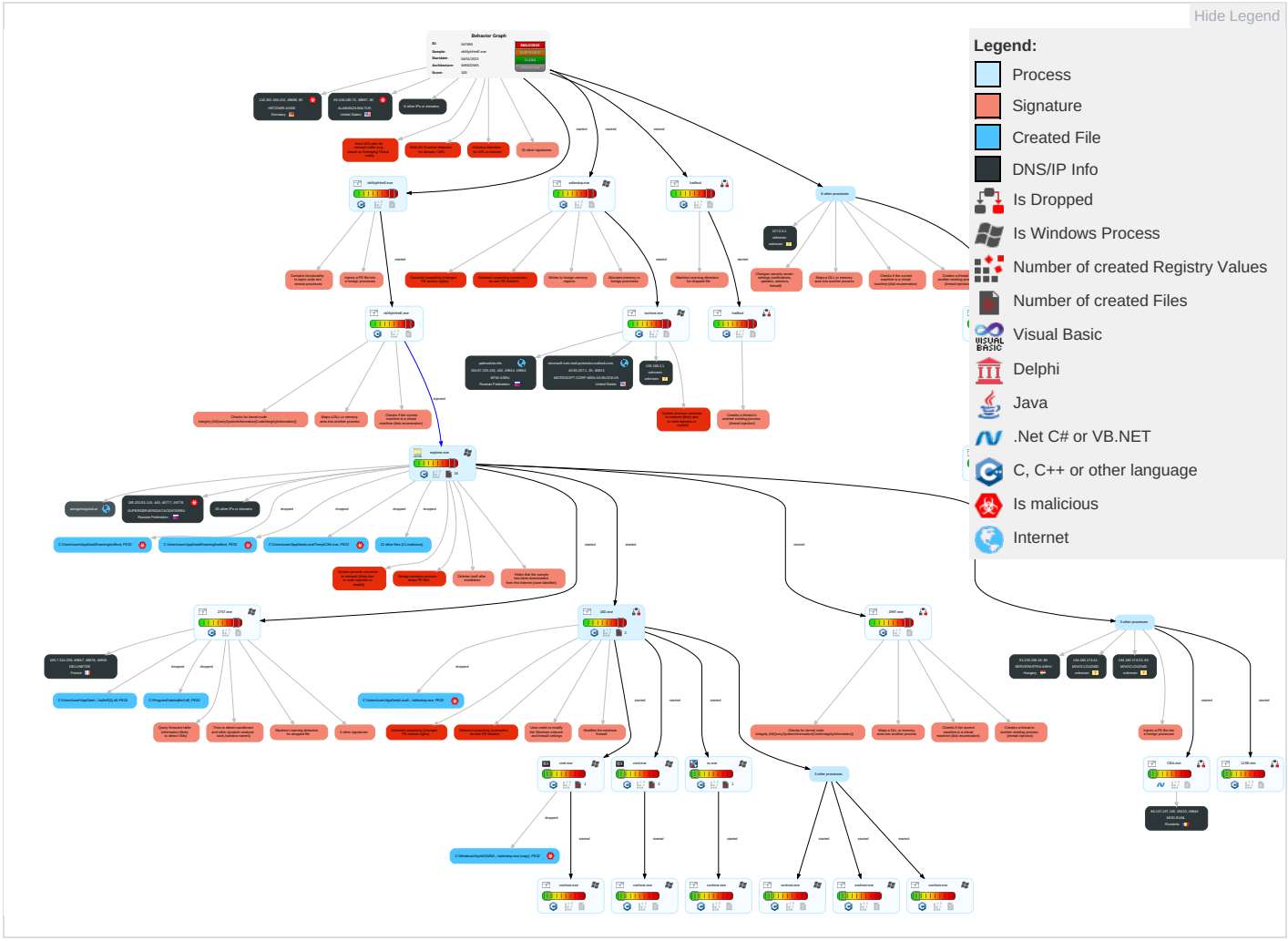
Remote Access Functionality:

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

Mitre Att&ck Matrix

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

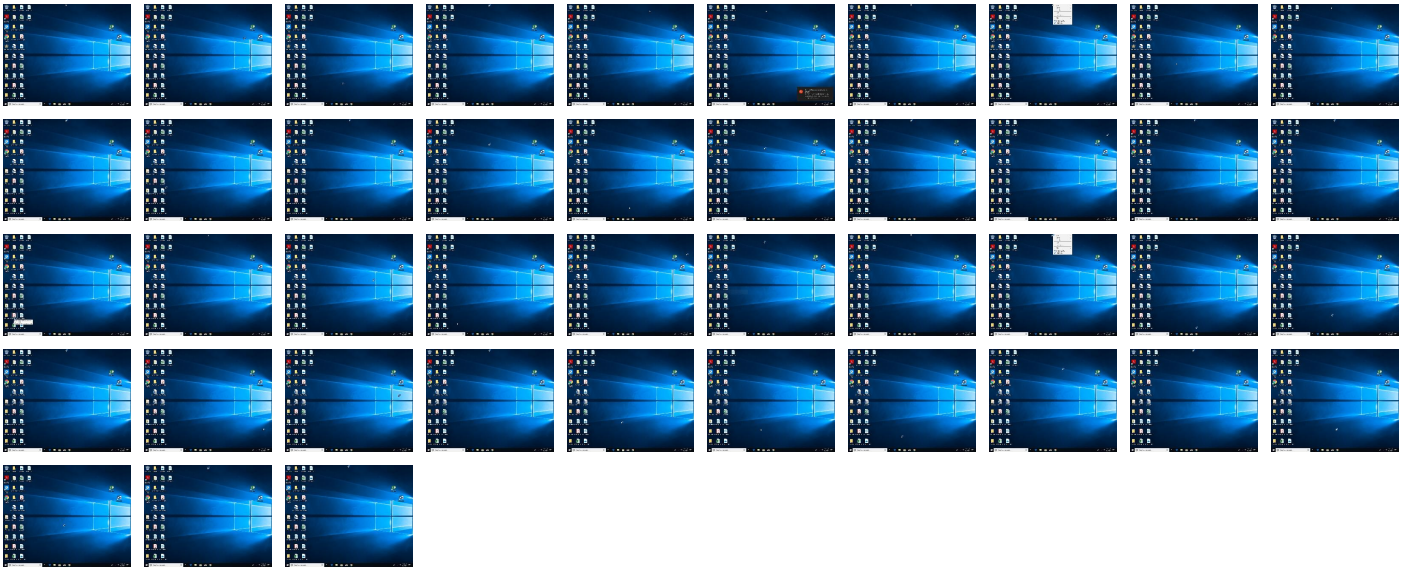
Behavior Graph



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
nkINykHreE.exe	25%	Virustotal		Browse
nkINykHreE.exe	26%	ReversingLabs		
nkINykHreE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\115B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\scifbcd	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CBA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4187.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\18D.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2997.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\315E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4BED.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1B15.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\28C2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4583.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\haifbcd	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\sdiimdop.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2757.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.nkINykHreE.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.nkINykHreE.exe.5415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.2997.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.haifbcd.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.2757.exe.1150000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.2757.exe.1150000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.sdiimdop.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.3.sdiimdop.exe.570000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.3.2997.exe.5d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.svchost.exe.2bb0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
31.2.sdiimdop.exe.600000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
15.0.haifbcd.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.nkINykHreE.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.2757.exe.1150000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.3.18D.exe.560000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.1.haifbcd.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.2757.exe.1150000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.115B.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.nkINykHreE.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.18D.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.0.nkINykHreE.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.3.scifbcd.5e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.1.115B.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.115B.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.115B.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.scifbcd.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.2997.exe.5c0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.haifbcd.4715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.haifbcd.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.scifbcd.5d0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.1.2757.exe.1150000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.2757.exe.1150000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.3.2757.exe.1070000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.18D.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.2.sdiimdop.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
14.2.115B.exe.4715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.nkINykHreE.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.haifbcd.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.4187.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1127993		Download File
16.2.115B.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://65.108.180.72/msvcp140.dll	10%	Virustotal		Browse
http://65.108.180.72/msvcp140.dll	100%	Avira URL Cloud	malware	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://91.243.44.130/stlr/maps.exe	9%	Virustotal		Browse
http://91.243.44.130/stlr/maps.exe	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://65.108.180.72/mozglue.dll	11%	Virustotal		Browse
http://65.108.180.72/mozglue.dll	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://91.219.236.18/capibarl	100%	Avira URL Cloud	phishing	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://65.108.180.72/706	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://185.7.214.239/sqlite3.dll	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://194.180.174.41/	0%	Avira URL Cloud	safe	
http://privacytools-foryou-777.com/downloads/toolspab2.exe	100%	Avira URL Cloud	malware	
http://91.219.236.148/capibarN	0%	Avira URL Cloud	safe	
http://116.202.186.120/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://65.108.180.72/freebl3.dll	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/8584_1641133152_551.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/2184_1641247228_8717.exe	100%	Avira URL Cloud	malware	
http://91.219.236.148/capibarl	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://185.7.214.239/POeNDXYchB.php	0%	Avira URL Cloud	safe	
http://91.219.236.148/capibarg	0%	Avira URL Cloud	safe	
http://91.219.236.18/3	100%	Avira URL Cloud	phishing	
http://194.180.174.53/capibar0	100%	Avira URL Cloud	phishing	
http://unic11m.top/install1.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mediafire.com	104.16.203.237	true	false		high
kent0mushinec0n3t.casacam.net	95.143.179.186	true	false		high
bitly.com	67.199.248.15	true	false		high
patmushta.info	194.87.235.183	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high
mstdn.social	116.202.14.219	true	false		high
natribu.org	178.248.232.78	true	false		high
unicupload.top	54.38.220.85	true	false		high
qoto.org	51.91.13.105	true	false		high
amogohuigotuli.at	152.0.118.227	true	false		high
host-data-coin-11.com	89.223.65.17	true	false		high
bit.ly	67.199.248.11	true	false		high
f0616073.xsph.ru	141.8.193.236	true	false		high
f0616068.xsph.ru	141.8.193.236	true	false		high
microsoft-com.mail.protection.outlook.com	40.93.207.1	true	false		high
f0616071.xsph.ru	141.8.193.236	true	false		high
goo.su	172.67.139.105	true	false		high
transfer.sh	144.76.136.153	true	false		high
privacytools-foryou-777.com	89.223.65.17	true	false		high
data-host-coin-8.com	89.223.65.17	true	false		high
unic11m.top	54.38.220.85	true	false		high
vk.com	87.240.190.72	true	false		high
srtuiyhuali.at	unknown	unknown	false		high
fufuiloirtu.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://65.108.180.72/msvcp140.dll	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://91.243.44.130/stlr/maps.exe	true	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://65.108.180.72/mozglue.dll	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://65.108.180.72/706	true	• Avira URL Cloud: safe	unknown
http://185.7.214.239/sqlite3.dll	false	• Avira URL Cloud: safe	unknown
http://privacytools-foryou-777.com/downloads/toolspab2.exe	true	• Avira URL Cloud: malware	unknown
http://116.202.186.120/vcruntime140.dll	true	• Avira URL Cloud: safe	unknown
http://65.108.180.72/freebl3.dll	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/8584_1641133152_551.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/2184_1641247228_8717.exe	true	• Avira URL Cloud: malware	unknown
http://185.7.214.239/POeNDXYchB.php	false	• Avira URL Cloud: safe	unknown
http://f0616073.xsph.ru/Music.exe	false		high
http://unic11m.top/install1.exe	true	• Avira URL Cloud: malware	unknown
http://f0616068.xsph.ru/crp.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.87.235.183	patmushta.info	Russian Federation		48347	MTW-ASRU	false
40.93.207.1	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.16.203.237	www.mediafire.com	United States		13335	CLOUDFLARENETUS	false
87.240.190.72	vk.com	Russian Federation		47541	VKONTAKTE-SPB-AShttpvkcomRU	false
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
172.67.139.105	goo.su	United States		13335	CLOUDFLARENETUS	false
89.223.65.17	host-data-coin-11.com	Russian Federation		49345	CONTINENTAL_GROUP-ASRU	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
194.180.174.41	unknown	unknown		39798	MIVOCLOUDMD	false
116.202.14.219	mstdn.social	Germany		24940	HETZNER-ASDE	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.7.214.171	unknown	France		42652	DELUNETDE	true
178.248.232.78	natribu.org	Russian Federation		197068	QRATORRU	false
51.91.13.105	qoto.org	France		16276	OVHFR	false
67.199.248.15	bitly.com	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
152.0.118.227	amogohuigotuli.at	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
67.199.248.11	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
185.7.214.239	unknown	France		42652	DELUNETDE	false
189.129.105.161	unknown	Mexico		8151	UninetSAdeCVMX	false
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
65.108.180.72	unknown	United States		11022	ALABANZA-BALTUS	true
116.202.186.120	unknown	Germany		24940	HETZNER-ASDE	true
61.98.7.133	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
194.180.174.53	unknown	unknown		39798	MIVOCLOUDMD	false
61.98.7.132	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
151.251.30.69	unknown	Bulgaria		13124	IBGCBG	false
141.8.193.236	f0616073.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.219.236.18	unknown	Hungary		56322	SERVERASTRA-ASHU	false
91.243.44.130	unknown	Russian Federation		395092	SHOCK-1US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	547895
Start date:	04.01.2022
Start time:	19:31:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nkINykHreE.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	49
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@57/40@107/34
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.6% (good quality ratio 19.6%) • Quality average: 58% • Quality standard deviation: 40.4%
HCA Information:	• Successful, ratio: 74% • 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
19:32:13	API Interceptor	3x Sleep call for process: svchost.exe modified
19:32:47	Task Scheduler	Run new task: Firefox Default Browser Agent 57D5564316429876 path: C:\Users\user\AppData\Roaming\haifbcd
19:33:27	Task Scheduler	Run new task: Firefox Default Browser Agent FA0C4CD8D97D977B path: C:\Users\user\AppData\Roaming\scifbcd
19:33:28	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
19:33:36	API Interceptor	1x Sleep call for process: 2757.exe modified
19:33:56	API Interceptor	2x Sleep call for process: 4187.exe modified

Time	Type	Description
19:34:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Music "C:\Users\user\AppData\Roaming\Music\Music.exe"
19:34:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Music "C:\Users\user\AppData\Roaming\Music\Music.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):	0.24857862142789358
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU42:BJiRdwfu2SRU42
MD5:	2A0ECA1698DAC02C685F470FF624FF73
SHA1:	B8250FAB9FE7DC4BD428779AF392893D157C4AD6
SHA-256:	B6B4013F5FCDA7AF3F4D249B6DB3B491BA688EE1F0D8BF49FF9BB9B77C8A7A59
SHA-512:	607FB01FE53B1D424D39DF6C67F5CBE569F9F678DC9E434EDC69FE26D5BD392EF4F8C10542268246241441AE6A30B53E4E7E7270EEBC76E41BAAFB55685DDF 1
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x250ef644, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25059013638213035
Encrypted:	false
SSDEEP:	384:0+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:LSB2nSB2RSjlK/+mLesOj1J2

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
MD5:	599F97CEA152346091DED811F2AC97D0
SHA1:	90BE68D3225D157ABACA71817F0796E8A9D93FA6
SHA-256:	B5E37DA5E782434B72D3F7F6B763751950450DBA3D94B9F92FB5EAEC40430A3E
SHA-512:	AF9E5BE4EAF0FE3B8BFEB440A6D49D1D18B0E2E2883236D6701C6B8A90A91D186B7F00AABB9A3F34E089358826D48D871BABFC29CC8FCE7CC3CB14E444585(D0
Malicious:	false
Reputation:	unknown
Preview:	%..D... .....e.f.3...w.....&.....w... ...zu.h.(.....3...w.....B.....@..... ....3...w..... .....X..R. ...zu.....iG.G. ...zu..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07509385199835537
Encrypted:	false
SSDEEP:	3:Am17Evrc88l/bJdAtiPIF1All3VkttlmlnI:D1i38t4M41A3
MD5:	641F90FED18A8DC34616C7FB5B02935E
SHA1:	A8E7391E4C41BC5821C336DE2CD26E4C24799685
SHA-256:	033E0B5558CE302B744B7F2608DF9D1DD114B5B932D7FD8B2F0EB89994910CF1
SHA-512:	8CE75AF915AB2B478CFA029CC73961730CA528082DE7645597C9959F0E49016421BB08885C0099CCC49D4CE02849EEBC4F731B72CB8542DE0D9F22DC57DDBF 4
Malicious:	false
Reputation:	unknown
Preview:	O.....3...w... ...zu.....w.....w.....w....:O.....w.....iG.G. ...zu..... ....

C:\ProgramData\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798(
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....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc..'.....(.....@.0B/4.....`....0.....@..@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CBA.exe.log	
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\sqlite3[1].dll	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls.... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C...`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Temp\115B.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	343040
Entropy (8bit):	6.634640145792183
Encrypted:	false
SSDEEP:	6144:5lA3X2bDueST6gKO1tqT7b4YlCTFGbGQ273pQGfT:5lA3X22e0VKYY70A4FOGQKt
MD5:	DC67C627917FF9724F3C1E6DB5F2DC27
SHA1:	4B7528999AD6095B3FBB3AEC059EFB88D999EA95
SHA-256:	26A4C5B36D9FDE80EA47137EB53B40DACF240432A5895F98417EAE51B6B681DA
SHA-512:	977AAB0AC60948315435E0698058598F40F42D7830B87EE7668BB209938CB388AA5B07C13B66C56DB1AFFA6F86A859B3C01666A22E437C808B6C9DB38975C7B0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....R.....Rich.....PE..L.... (._.....@.....P....@.....I=..(.....`.....P..8#..`..... ...@.....text....>. .....@..... ..`.data...H%...P.....D.....@....bekuvox.....Z.....@....jutu...K.....\.....@....vezev.....^.....@....mubone.....`..... .....@....rsrc...`.....n.....@..@.reloc...>...P...@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\13E0.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2030423
Entropy (8bit):	6.581224020190253
Encrypted:	false
SSDEEP:	24576:hZ7Xar2VsBq/OebTdhbj8C2cBiw9PVf7x3Tszozbaw2pYqZEWzMdX3UdN9RdN:NswfblVPZv32pYqZ3aUdjRdN
MD5:	AA519DEEB511E886E73F8E0256180800
SHA1:	653B5155ABD17EB35F13543EED5F3A0794000171
SHA-256:	B8EDF8B69FD72F728790CAC7FA5F2642A5C386EEC1ACE836CD05A19177252E2B
SHA-512:	6156B3391118A458130C6FF6FE8B0B0B05895B16E8B43C6A269C4D5A9136BB622E3AEC6B13C1D397C00642A82563A830D43CAB48D6BC7824090BB7174C65D428
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\13E0.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.k...k...k..c.a..k..c.c.[k..c.b..k..l.W..k...5./.k...5./.k...5./.k.....k.... ...k...k..!k..@5./.k..@5./.k..E5o..k..@5./.k..Rich.k.....PE..L....}|^.....V.....4.....p....@.....@.....4...4...<....p..... ...P...&..`..T.....@.....p.. .....text....U.....V..... ..`.rdata..t....p.....Z.....@..@.data....N.....@....gfids.....`..... .....@..@.rsrc.....p.....@..@.reloc...&...P...(.....@..B..... .....

C:\Users\user\AppData\Local\Temp\18D.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	342528
Entropy (8bit):	6.631057078600846
Encrypted:	false
SSDEEP:	6144:7AH3plu5xWDwtTwKc6+9YwoTPxSeI2co8mfgW:7AH3pCxvTS6Wh6PIeI/
MD5:	B7B184D2B0910148CABB9B5E915753D6
SHA1:	C5285CFF52A33103F1511D1049185F767F656BF9
SHA-256:	65D20D76E0E30EFBCD8D9864BDB6BA40C22C7148A0397EE4484C303F2BED12A1
SHA-512:	5B0857A7F0C5709DC83AE1BA997E6604F16241DF6FC1D9E9C36CD2B7B306C30FDA0FF54630ECF658DA03B68DA03508BD4B5C617912D66A15FD239B651AC0A28
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....R.....Rich.....PE..L...15.`.....>.....+.....P....@.....*(.....<;..(.....`.....P..,#..`..... ...@.....text...n<. .....>..... ..`.data...H%...P.....B.....@....lave.....X.....@....fidoce.K.....Z.....@....pihudu.....\.....@....lafog.....^..... .....@....rsrc...`.....I.....@..@.reloc...>...P...@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\1B15.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	816128
Entropy (8bit):	7.441400608749297
Encrypted:	false
SSDEEP:	24576:LIf1GQIfOzkechO5QhGRBQPcnUdvs5ubra:0tGPfOzrcogEnYvK
MD5:	D8B78E7D4D822C10CCE3654D7F9E4931
SHA1:	355A02E87F393AAE822C89F54B7A26187B889A19
SHA-256:	77F8245BB300970C5D60F028BC2E084BAB3B3464FDAC14094A94E47FAA6A08B1
SHA-512:	03749AC5D0238898987C4FFE4799307C612A9912F8FD9B182A700E933D0BB72E8F2201689F3DF836ABFCAA02BAA7F3D4903B99A2C739E01C9A3B1F0587E0E1B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w.....w.....w..C....w...v.W.w.....w.....w.....w.Rich..w.....PE..L...._.....@.....jh.....l...(.....h.....4#..P.....h...@..... .....text...\..... ..`.data.....@....nulec.....@....pexano.K.....@....tufeh.....@....rijeyo..... .....@....rsrc...h.....@..@.reloc...B.....D...0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\2757.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1497920
Entropy (8bit):	7.935012575598995
Encrypted:	false
SSDEEP:	24576:Z5o4ghlDlYMi1GJTGINb/yvUZmBoq7m2PM0IGyo2lgqeDW0F0dj71O6+iIzsbEjp:iDlhi1SGIpyvfoeV2KWK0d/g9vzsbE1
MD5:	67B848B139E584BF3361A51160FC6731
SHA1:	0D8C86D200BD19973F7DC833CA8809D8E60B8854
SHA-256:	B8B942C702F57D78578F42ABAA04906A42BB09C8C88731E71B9509A5509AAE2F
SHA-512:	EB8E57175BB33FEC20D375C6A85446ED51C0EEEEFCB8B01FC1B0C941D2DA52BBCD1ED9080BE67F4A51C2A0EA73C5B06E60A5B7AA1A5E3EAD7293E35831C5CFC0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\2757.exe

Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.........+..R...d:.....Q..... ....PE..L.....a.....H.....`*.....@....@.....+.....^....@.....%.P....%..... ...reloc....%.....`.itext.....%.....@....rsrc.....%.i.....@..@.rdata.....`*.}}.....@..... .....(.%..z..~E..V..9.Rt..a....1.:.

C:\Users\user\AppData\Local\Temp\28C2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	783872
Entropy (8bit):	6.576079323203091
Encrypted:	false
SSDEEP:	12288:WfZoHSPPvc9PU6ynVQQTUnAD5MRJSa7V7m3rjY:UrviAVvEC5CJSa7V7Srs
MD5:	F111EE7C9F26F50F9EFEEB6EF6C32A3C
SHA1:	B4239A2662A2835F8BFF098D0F0CBD4A51095144
SHA-256:	5F1E42B60BBB3EB1BB895C9A94886A775312F0AB8527B96187F9E084A08413B4
SHA-512:	973D51072EB6C4F18691E33B70187F34B7032A17AAD7575EFAC06A34009ADD3934A01261F9540FDF4A4F9429A4421E730DE947BE817C52D32FF95B83C711F04D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p.O.p.O.p.O."hO.p.O."yO.p.O."oO.p.O...O.p.O.p.O.p.O."fO.p .O."xO.p.O."}O.p.ORich.p.O.....PE..L...@._`.....0....?.....]....@....@.....K.....|X..<....pJ.....A..... .....xT..@.....@..@.....text..../.....0..... ..`.rdata.....@... ...4.....@..@.data....>..`.....T.....@....wibobahr....`J.....f.....@..@ .rsrc.....pJ.....j.....@..@..... .....

C:\Users\user\AppData\Local\Temp\2997.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	358912
Entropy (8bit):	6.278717191933335
Encrypted:	false
SSDEEP:	6144:7e+RhbrOOFh9v2Y8zBk3L3gXO1RdFggj:7e6aOFhB8zBk3L3b1R
MD5:	1F935BFFF0F8128972BC69625E5B2A6C
SHA1:	18DB55C519BBE14311662A06FAEECC97566E2AFD
SHA-256:	2BFA0884B172C9EAFF7358741C164F571F0565389AB9CF99A8E0B90AE8AD914D
SHA-512:	2C94C1EA43B008CE164D7CD22A2D0FF3B60A623017007A2F361BDFF69ED72E97B0CC0897590BE9CC56333E014CD003786741EB6BB7887590CB2AAD832EA8A3D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..S/.../.../...1.Z.=...1.L.W....6..*.../.....1.K.....1.[.....1.^.....Rich/..... .....PE..L...t..`.....<...J.....4.....P....@.....A.....,9..<....0...Y.....#..P.....X...@..... .....text...4:.....<..... ..`.data...`....P.....@.....@....pamicak.....@....dos....K.....@....modav.....@. ...nugirof..... .....@....rsrc....Y...0...Z.....@..@.reloc...>.....@...:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\315E.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1531904
Entropy (8bit):	7.9884438553546415
Encrypted:	false
SSDEEP:	24576:ojJwQQzNL/zYGLw/6xjcjLkCKMglDhkwgmvd6Y0nJWmHIlG7kEaHNYK3o0:o3QzBYX/6qnjKMgl9kwgmV6YgolG7Naf
MD5:	4FB3361FFC7E5DD2FAD4413866DB6D2E
SHA1:	067B41BD44034FF7638E4DEE36C14F2A7D0FD460
SHA-256:	DB0D62482F5E1D8A2E1732604D43A74D9641D4F56E7D14492560BB2CE76C7D33
SHA-512:	EE432B3BD1A0BA968CD3DDCAFA79A778D1C0E52C1630670AEE57519ED43C06E8CF236A0E3E948278F658A1BBECD6A955D55BD430A84EABC9C6DF823C21F2070D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\315E.exe

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......>..$zy.wzy.wzy.wn..vwy.wn..v.y.wn..vly.w(..vky.w(..vny.w(..v0y .wn..v.y.wzy.w$y.w...v{y.w...w{y.w...v{y.wRichzy.w.......................PE..L......a.................$..................@....@..........................2.......+....................................|.-......P........ ....@...............0.....................@...............@...b...&.............@........... ...0............. ....@....rsrc........P.....................@........... ....0.............@............... ....F.............@............(..0...r...H.............@....7w0DPA1......-.....................@....adata........2... ...`.............@..

C:\Users\user\AppData\Local\Temp\4187.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	760832
Entropy (8bit):	7.455489986534232
Encrypted:	false
SSDEEP:	12288:NmnQAJTFOZULSeNYKa+0R7sGtakDxKUXjE9woqT4lYf9icr/PlokJVd074tFEZ1i:NqQcBOZv8YKlksGcgUUTEGBcenr/gJVM
MD5:	C085684DB882063C21F18D251679B0CC
SHA1:	2B5E71123ABDB276913E4438AD89F4ED1616950A
SHA-256:	CDA92BB8E0734752DC6366275020CE48D75F95D78AF9793B40512895ECD2D470
SHA-512:	8158AA6D5A6D2130B711671D3DAC1A335B01D08118FB8AC91DC491ED17EE04CCA8559B634EDD4C03DECBD8278709AD70DB7FB0615DF73F25D42242EA4B255 B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......z8~R>Y..>Y..>Y.. ...,Y.. ...FY....k.;Y..>Y...Y.. ...~Y.. ...?Y.. ...?Y.. Rich>Y..........PE..L......`.................l...<.......g............@..........................PH.....e.......................................$j..<....0...Y...................H..#..@..................................@.................. ........................text....j.......l.................. ..`.data...h............p.............@....johac....... ....@....rsrc.....;..0...Z.................@..@.reloc..tB....H..D...X.............@..B...... ....

C:\Users\user\AppData\Local\Temp\4583.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	453632
Entropy (8bit):	5.066707207289782
Encrypted:	false
SSDEEP:	3072:hmDsLlCSV7TXJnlGsMbRA9Zjhdlzi/1eY5jHDdesUXztjqO4pHh8OMjKy23AF+Yz:wQLlCSVHxlvZ9ZjufjUDH4p2kYFhvBB
MD5:	11124BB02075AD2D9D750343B42F932A
SHA1:	9BEAA5B27E610A92DF153E4B5628E1804CAD2B20
SHA-256:	00E365FB7DA89657B15CA8B16273B3B30FE66DBBEDE7F52B678D2E37AF51FA19
SHA-512:	C92123280F5C696ACA446306512293DB636D9BD70D359C4EA1F416AB192B19BF0478590076C71D6E57E72D1FE6AAE9E365792B2F223FC83F09004933C2552B07
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$...........q.O.q.O.q.O.#hO.q.O.#yO.q.O.#oO.q.O...O.q.O.q.O.q.O.#fO.q .O.#xO.q.O.#}O.q.ORich.q.O........PE..L....=K_.................(....?.....\........@....@..........................F..... ....W..<....pE. ....A......................... .....S..@............@..D...........................text....'.......(.................. ..`.rdata.......@... ...,.............@..@.data.....>..`.......L.............@....himav..r....`E......^.............@..@.rsrc... ....pE......b..............@..@.. ....

C:\Users\user\AppData\Local\Temp\4BED.exe

Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	652928
Entropy (8bit):	7.903105089614694
Encrypted:	false
SSDEEP:	12288:nvc5Q+JQWNWFrF2rkO+T2dgXPVK3F7xGV2+AQq3KVUlgluTfE:v6ftNWprT2qXQ3FITAQiKngluT
MD5:	DE573B83DB582FB0354CF72CBBBD7176
SHA1:	A99B01FB00D13BDB8AAF89BA84A7CB292E05B744
SHA-256:	BDEC451319F1A86616FF05A77BBCE9272DBFE1C3900E9D8C94C7FEC1AABCBDF2
SHA-512:	CB5161180F26E39BE5F506AD22F972F309E247FFEA312D0CFD6D7E89D92AC4769013C0FA11CAF3960C8B93AEC2F378A0B7FB5AEA4322E098205D27953A18F17
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\4BED.exe	
Preview:	MZ.E@.....}..J$.....Ma.E.d".j..m.4.;%.X.....`.J...k.S.....Q..... .....PE..L.....a.....D.....`.....`....@.....0..... .....L.... ...1..... .....`.....@....rsrc....1... ...1.....@..@.....`..y....8.....@..... .....+.....!...L..v..J$@d.k,.. ..

C:\Users\user\AppData\Local\Temp\AS2N7900	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\BJZFPPWAPT.docx	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861D C
Malicious:	false
Reputation:	unknown
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\CBA.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	539136
Entropy (8bit):	5.841944907736123
Encrypted:	false
SSDEEP:	12288:XJSPWI/m1ZNhIyNPRQSOrve+rW4mqlQbHFuYB:XJSPR0dIyNP6eNHR
MD5:	6C72997AA5DD44A44B27BD36347BAED9
SHA1:	A1EE2A54095F7ECD8DC3AFAF9BCE96543EB7BB41
SHA-256:	5261F20B37DA1A726D4E5A632A93F0DB4EA8EDA81EE3095E2ECF80DDB5B89DA2
SHA-512:	16DDFE0F81DE4F29832016D9DAD432816CABA2C778A780B763A1840EDCCCB3BE21B47ABAE8E59543FCAE0CF1300B2EDE139A0850CF7AEB0F23CC2A02FDDE ACB9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\CBA.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[;.....0..2.....O... ...`....@.. ..... ..@.....O..K....`..... .....H.....text....0... ...2..... ..`.rsrc.....`.....4.....@....reloc..... .....8.....@..B.....O.....H.....E.....Z..I.....(....*..0..1.....8....*(g...8....~....u....s....z&8.....8.....!.....*.....*....(g...(....*.. .j*.....*.....*.....*.....*.....*....(....*.~(....(a...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*.....*....(...*..0.....*....*....0.....*.(....t.A... .....t.A.....*.....

C:\Users\user\AppData\Local\Temp\DUUDTUBZFW.docx	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701195573484743
Encrypted:	false
SSDEEP:	24:CXuIDWqLgX6vdVaxL46BNaYMbtbF+qEBHi7z/dd0Vc/6cUmeDs:ODHgX6vd0l4gnMbtbF+qEMPdNiTmcs
MD5:	2530C45A92F347020337052A8A7D7B00
SHA1:	7EB2D17587824A2ED8BA10D7C7B05E2180120498
SHA-256:	8BEAEA56B1D06BFFFE6142E95BC808FD28015E6A3FF32BC2FAC4C5A7552FC853
SHA-512:	78F4D4E93139D099D59F17867A6BB87A7DB92E1637A520B522A32DF14D18A39602F1C255C64C4C406BA45138294D9467850FEEA90C199D3434D60AE1C7F6B4DA
Malicious:	false
Reputation:	unknown
Preview:	DUUDTUBZFWQODSNPWYYAIDZFECIUBQYLVGHZRZFDGGWVZPGQSHTPZANMRMNDUZLXCVYYIRRTMYEOTHOFJLCKQKOCQKNMRKZTHKIIPBKXIKLDAZ FJGRVUHMDDXAMADOCGROYYDTNZZUEROBUVEGQEAZOMYVDGVHXUWCBVRBLFLWITRUFMXJJLQTZTWLOSFUMQDKRZDXVRLBYBKLXGLTGADROPECYT RYJQJWZDWJQHGRYFIQLJDBJUFPEPZLWGXGGDQGOLJCVZAPHJZOSIZQHISQFRJJGEZIJEFACYWHJRHAADQBMDQFJAGFBEZNQNGWDHSAAXOAEHIE HTAEPMOFJSOCRPTEUZGGSVYGVNUAYJPFNXFSYEEMDNDGDUBNXUOHVEJQBDRGSCASTDANAAFPQYQEHHTAOTYKYJJYXDZMUTBXBCIFNYSYWNMYAE EUEIGDANIBIJWTMCMGVDPOCAVEJZDTVMKOQPOOOKMLFWWMOASXZUZVHWZKPBVANJIBBDPCEKXDPEFNTXPTFJRBFUPHQCKMDMMXQPDZLJPURSOL PQREZLEFYXCGNKSFQRMLKDMGSNURCWGNTDQUIOYBPNJAYWOVTXRGROGVHNGIEDBYKUHNRBBDKYQXANPQWPKEOHDUBNRSQPALMLJE QFMXCQMEOAKBRREEJTYCHGUEGBGPJLGWRCLYLAKRESHJPMPCUHRFXHVUIQCQZYDTCNRGWVTYBMIILXIIIOGMHAQBLHFXCLTIKGXWDVRGSSRDNC YOVCLTUUEWRIDEOSWWZKTQLGLSIFPVAFJDGWVZYJUOVTMGGZMWUYOQYCLDNLMKWCJBKOXTWTPCMMIEYMISQTQCKMPNWJVAXPFISOGTRIMGKBHK EJOEDYIGOBOPVFADMXZUZQZVMUDYSPUHDXFZMAVPGIHURQNBZXXDWPSHUEZEFABRCKBUQLCPYBNGKJCWBTBSWMABCFIYQJOHFJJEPNNMRWWMNL OTWSMOXCILCCNICPDFTO

C:\Users\user\AppData\Local\Temp\DUUDTUBZFW.pdf	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701195573484743
Encrypted:	false
SSDEEP:	24:CXuIDWqLgX6vdVaxL46BNaYMbtbF+qEBHi7z/dd0Vc/6cUmeDs:ODHgX6vd0l4gnMbtbF+qEMPdNiTmcs
MD5:	2530C45A92F347020337052A8A7D7B00
SHA1:	7EB2D17587824A2ED8BA10D7C7B05E2180120498
SHA-256:	8BEAEA56B1D06BFFFE6142E95BC808FD28015E6A3FF32BC2FAC4C5A7552FC853
SHA-512:	78F4D4E93139D099D59F17867A6BB87A7DB92E1637A520B522A32DF14D18A39602F1C255C64C4C406BA45138294D9467850FEEA90C199D3434D60AE1C7F6B4DA
Malicious:	false
Reputation:	unknown
Preview:	DUUDTUBZFWQODSNPWYYAIDZFECIUBQYLVGHZRZFDGGWVZPGQSHTPZANMRMNDUZLXCVYYIRRTMYEOTHOFJLCKQKOCQKNMRKZTHKIIPBKXIKLDAZ FJGRVUHMDDXAMADOCGROYYDTNZZUEROBUVEGQEAZOMYVDGVHXUWCBVRBLFLWITRUFMXJJLQTZTWLOSFUMQDKRZDXVRLBYBKLXGLTGADROPECYT RYJQJWZDWJQHGRYFIQLJDBJUFPEPZLWGXGGDQGOLJCVZAPHJZOSIZQHISQFRJJGEZIJEFACYWHJRHAADQBMDQFJAGFBEZNQNGWDHSAAXOAEHIE HTAEPMOFJSOCRPTEUZGGSVYGVNUAYJPFNXFSYEEMDNDGDUBNXUOHVEJQBDRGSCASTDANAAFPQYQEHHTAOTYKYJJYXDZMUTBXBCIFNYSYWNMYAE EUEIGDANIBIJWTMCMGVDPOCAVEJZDTVMKOQPOOOKMLFWWMOASXZUZVHWZKPBVANJIBBDPCEKXDPEFNTXPTFJRBFUPHQCKMDMMXQPDZLJPURSOL PQREZLEFYXCGNKSFQRMLKDMGSNURCWGNTDQUIOYBPNJAYWOVTXRGROGVHNGIEDBYKUHNRBBDKYQXANPQWPKEOHDUBNRSQPALMLJE QFMXCQMEOAKBRREEJTYCHGUEGBGPJLGWRCLYLAKRESHJPMPCUHRFXHVUIQCQZYDTCNRGWVTYBMIILXIIIOGMHAQBLHFXCLTIKGXWDVRGSSRDNC YOVCLTUUEWRIDEOSWWZKTQLGLSIFPVAFJDGWVZYJUOVTMGGZMWUYOQYCLDNLMKWCJBKOXTWTPCMMIEYMISQTQCKMPNWJVAXPFISOGTRIMGKBHK EJOEDYIGOBOPVFADMXZUZQZVMUDYSPUHDXFZMAVPGIHURQNBZXXDWPSHUEZEFABRCKBUQLCPYBNGKJCWBTBSWMABCFIYQJOHFJJEPNNMRWWMNL OTWSMOXCILCCNICPDFTO

C:\Users\user\AppData\Local\Temp\EIVQSAOTAQ.pdf	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.692024230831571
Encrypted:	false
SSDEEP:	24:RXklo22NBtmSOCPX4hQpKZCuvImjwxwo1:v22NBtxOCYQ0EuwmMxz
MD5:	086908C2D2FAA8C9284EAB6D70682A47
SHA1:	1BCA47E5FFEC5FD3CE416A922BC3F905C8FE27C4
SHA-256:	40C76F418FBB2A515AF4DEC81E501CEB725FD4C916D50FCA1A82B9F5ABC1DCCF
SHA-512:	02C48E3CDA1DC748CD3F30B2384D515B50C1DFD63651554AD3D4562B1A47F5446098DCED47A0766D184DDB30B3F158ABEC5877C9CA28AB191CEBB0782C26B0

C:\Users\user\AppData\Local\Temp\EIVQSAOTAQ.pdf	
Malicious:	false
Reputation:	unknown
Preview:	EIVQSAOTAQGMTJLIEKHIWADNDLJLEWUUXVGOFMOKPHABQUHVNBFVSKQIGVIHICGEEXRLSTKQNZUKOHPLLTCYQSLQJMPWPWNUJFUONDXMYCCUPD UBYMPUSUKUOWWSWDLZMDWKNMUKNPKBXAJATSGOQUAMHMZDCDDJRHKOUEDMLSCIOXAHAUFDQKBUBESAKMMFMHDLSSVUQLOZXARPGP MGAAKVDEITBYGGXWIGUIJRVXQOBOIOJWPYSPHZBHWQTMDCUFCWBQSAZNRUOPCLATAERLBPATETXMFUGXBEGMNPKKEZVSRLCYPFEPWIAEINAMGS OXLYWMUKYSQACPSUTGHDCTFLXKAMLOCGYHCMAETHVZNZOCWWUHYAPHFILDNLLBMLSLXIMOFGWTDVLWPHHRGGAWSIGNXEJRIBIBLWFBUASCLZPU IVDERXYLWTNLLRLTFZJTTDGFOEYPFXIPHFKEXHOGEHSFYCCCTGNFQFYETBADKAEAOXYXJWDJWNZPEOBJZTKPLJPPMICDOWUIVDKBQQMHETDORV KZPOWTAZRBAQYYQHBNHIWFZXBILGKHZBLSQJJEIYBHUIDAOEXERQEUMMKBWDXSMLJVAZJQPZARLOBNSTUDCVKLCVBPTKTJWSMPMKSFOQPINFTN EGPVSYCWOXABSGFFKRQDFQEIJWDUMZKILALUHYQZGZOLYMKSAOZGUYCKJOJLYINHVKCTZVXLYIYPGOQZQQAGXVWEBSURTQECDRXYKQAJBEKDNS IHNBZCUBIKPKVWLUOFFCIZSKQBAAPGFMBASMUOKLLGWEHHMYDJCOQEKOBYLYWOOZLBASOJJYLIHZKUGUKHZQBIAVUPYHYEWAYGUFNARHCUKTFM LHSFLRVAELAFCQHPEFUSGNONWLLYQVUVSVEKHDRXJHDSSFJATGDRCTMICJWPFPKKLXECKUXREXEAQNPOBPRKFYRWIWXEWLAPUSHGKXWYYIJNUM GQHBJPMOYZIXPGOJLOQG

C:\Users\user\AppData\Local\Temp\EIVQSAOTAQ.xlsx	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.692024230831571
Encrypted:	false
SSDEEP:	24:RXklo22NBtmSOCPX4hQpKZCuvImjwxwo1:v22NBtxOCYQ0EuwmMxz
MD5:	086908C2D2FAA8C9284EAB6D70682A47
SHA1:	1BCA47E5FFEC5FD3CE416A922BC3F905C8FE27C4
SHA-256:	40C76F418FBB2A515AF4DEC81E501CEB725FD4C916D50FCA1A82B9F5ABC1DCCF
SHA-512:	02C48E3CDA1DC748CD3F30B2384D515B50C1DFD63651554AD3D4562B1A47F5446098DCED47A0766D184DDB30B3F158ABEC5877C9CA28AB191CEBB0782C26B0
Malicious:	false
Reputation:	unknown
Preview:	EIVQSAOTAQGMTJLIEKHIWADNDLJLEWUUXVGOFMOKPHABQUHVNBFVSKQIGVIHICGEEXRLSTKQNZUKOHPLLTCYQSLQJMPWPWNUJFUONDXMYCCUPD UBYMPUSUKUOWWSWDLZMDWKNMUKNPKBXAJATSGOQUAMHMZDCDDJRHKOUEDMLSCIOXAHAUFDQKBUBESAKMMFMHDLSSVUQLOZXARPGP MGAAKVDEITBYGGXWIGUIJRVXQOBOIOJWPYSPHZBHWQTMDCUFCWBQSAZNRUOPCLATAERLBPATETXMFUGXBEGMNPKKEZVSRLCYPFEPWIAEINAMGS OXLYWMUKYSQACPSUTGHDCTFLXKAMLOCGYHCMAETHVZNZOCWWUHYAPHFILDNLLBMLSLXIMOFGWTDVLWPHHRGGAWSIGNXEJRIBIBLWFBUASCLZPU IVDERXYLWTNLLRLTFZJTTDGFOEYPFXIPHFKEXHOGEHSFYCCCTGNFQFYETBADKAEAOXYXJWDJWNZPEOBJZTKPLJPPMICDOWUIVDKBQQMHETDORV KZPOWTAZRBAQYYQHBNHIWFZXBILGKHZBLSQJJEIYBHUIDAOEXERQEUMMKBWDXSMLJVAZJQPZARLOBNSTUDCVKLCVBPTKTJWSMPMKSFOQPINFTN EGPVSYCWOXABSGFFKRQDFQEIJWDUMZKILALUHYQZGZOLYMKSAOZGUYCKJOJLYINHVKCTZVXLYIYPGOQZQQAGXVWEBSURTQECDRXYKQAJBEKDNS IHNBZCUBIKPKVWLUOFFCIZSKQBAAPGFMBASMUOKLLGWEHHMYDJCOQEKOBYLYWOOZLBASOJJYLIHZKUGUKHZQBIAVUPYHYEWAYGUFNARHCUKTFM LHSFLRVAELAFCQHPEFUSGNONWLLYQVUVSVEKHDRXJHDSSFJATGDRCTMICJWPFPKKLXECKUXREXEAQNPOBPRKFYRWIWXEWLAPUSHGKXWYYIJNUM GQHBJPMOYZIXPGOJLOQG

C:\Users\user\AppData\Local\Temp\EOWRVPQCCS.xlsx	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.692990330209164
Encrypted:	false
SSDEEP:	24:NCzz4hMQMxH70HULgnraTryj1S0KEX64u+O572j79DwzpnQf8A:axH70cauYS0k4u+O125wtnm8A
MD5:	DD71B9C0322AD45992E56A9BCE43FE82
SHA1:	60945B6BC3027451A2E1CFA29D263A994F50E91A
SHA-256:	19AC62FD471E562088365029F7B0672623511CF3E58F2EF6DE1A15C14A2E94E7
SHA-512:	86EA2B42FEB542977FCF534B4708F7A07E09F4ACC413307E660B905408BC4AA9E26C50E907FA02379EA3EBFD18C532CC9DC269B6EA5994E3290082E429CAAE03
Malicious:	false
Reputation:	unknown
Preview:	EOWRVPQCCSGUYRPSSKREBPXVQXUWKHGDIJHLBLYMXTIUESLNTSFMRJGDSQHOWECQAJMENKQNNWPVETUPWMXJTCUIAKPCZEENXVLTKYPKROZPDE BFNAJOVCNEXQJFUHQCMLNHGMRJJIPLOMWFWJKKXSTRHWFVLVQPEMFBLDTSCCSXADJIIDQIYCEGSDEDZDWUEJLTYJHMYEHHMBFZCRDHXZVPESWN DGUEFQZTJFSJVKZMWREMIZGAIZANQJKWWXITTXHDQDZOEOGKCEMDUUBDTMNWBRSOWEKQXQDCYJXERQRAMVQCWCTYJPEAJUAWNBRQ WGFJAHXJJFRYTZMSGCREPRECKHXXMJGSQEKUCUNCWUAAPBWQVSMWCJGYSLPHJJHJGXSMNLNICJMSGSWRKARHMQXLYSAOPDAPXSMO RZLUWYOQTJQNKSCAJWRUEYRFPNOVSMNYRKMTSGRIFLOAJUGJYDTLINOTCEADKRENVYNODFSIJGSDCICIDXZTLLSKKJQSOHYTZRBSHPHXWZOOSK QIRSGPTAOQPBVJAMXOGPYNJMJXAKCTMRRTFCBPOAMNJORWRNZOGZMNBVCCZYQPOQOUXBGKNLFSQWAWEREFQBRDLTVHEFNRUSOARH JPRECDRMPANZRBGCANIUWEBUDVWLYHFTPGBHSZBZBEFUWFHUZPJOVMHGSINZWDUKWPGMGSNSSJNOMETOCJILXRQRGZQFAJCWYQEENIZIMHRBTZ UYEOKCQXYLWCKFHOHCOVRVPNTEUARVJEFALBUVYXIYZRMGJWZNYNLPYHZSSCODVXZBIWXIOAVMGMPKCPYIFZIKWRIHNIYASXZLMOLNZOMMYUSC RZBCXRANWWODLPHCXXDPLNYLMHYIUYZJWQLECFNXQEERYDVDBPXOLGZLZQCVYUYKFZGKXWVDQANPXQYAATYFJALGENVLDMHDASWKNNXODUHLXY GCBUKEFWISCCUWXNUNETWMTQHQDJMAXNPFPLMPQO

C:\Users\user\AppData\Local\Temp\KLIZUSIQEN.pdf	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\KLIZUSIQEN.pdf	
Size (bytes):	1026
Entropy (8bit):	4.696703751818505
Encrypted:	false
SSDEEP:	24:b16WkAmEUwq/rBFGdG3NQGsu7DYh3NTgfAtxoLxLP/VEmcM:hkAYzzbG4NPsuYh3N0fAjaxLnl
MD5:	19255ED5D4F37A096C105CEF82D0F5C0
SHA1:	96C5E995A91C8BC479E1C2ADB32C7E022EB8FAC7
SHA-256:	A0E9C6A5B14DB7AB22994C5017930720299F4492CE99D95A07BEB46BF2BAE7E8
SHA-512:	CDCD7E54677DE3BCE65BD80C855DE9684517F931ECA4D17E984C1D02E5E5CE9B50582ECCFA43F71A4F0A4E1743D74FCF3D588424AF519BFAE628EA49082C6 68
Malicious:	false
Reputation:	unknown
Preview:	KLIZUSIQENZWQAFPHPIZMRSSYSYIINGOAPFQHPCFTPTNYLSNMTRTDZSWEBKDRHIUFOFGWKTHENHAQWTYTMOJNOWPWJAPIZKOPDMUAKVTHXYWDB HBVWDTBCFVXJHDCUGTPASHSDSKUVYPRPPUXKURDNZYJENQKRHCARIUAOIAFRFWGQDXOAPXUJAUWRVEASXCVARWJMIPINSQDPGOWLRMNRCAEZGZ IYDWBEWCOJWHLMOUROGZKCFGXDKPHAJADQCYUZYSYXQOIEGZIJWZLUJEKZUASKHQOGVFGVEXIQTENJDEKERNBPZGKNXWYZVXDDAYNSFBZAKWCE EYDSJONDKOYOBSAVICMHPZZRHRLNYDOIDQNYLXFDCCUOIJANPQCOIJDXFLDMIBVHBYSNYGAVWTHYCIPBRPTWSQXWXZZJBFNAUOMALKDRYIMJCR JXXQXCEREPQGNQHHOFEMEOXMSZEWOLTOLCOUCQNPRIPXUSVZNATFZKIJQZKGKTCYOMBXFTSXBXYIHMOONWWGRKPSNEMONASEFSVW NWIBXDSMEKQJIDCFPVMGAAUPBVOYAIKYQEFVSXOFTEMHNXVNMMENORLDYPZUSILNZRPHITCWDQMLEFZOEGPJDXQLBSIYRONLBYOSJVTEMBHNVX CMMRDVOAYSMNNRKRLBSQBIWIWHYUMBKTIYQTROZKTGZZMEFWINSQAXMWWLRRSPXAQZURXOTMUHPNLOUWMXRQSGXIAQILQCZUUTRJZVRNLBSHAD NHZSDOQIYIZCEZHFRITTHSZOSBZGNCQVHXSFZJCEVSJCZZYTCFXLNBKMTPXYHPDXMMMXHUAAQWYYFHMKXWZBXZBWKFQHLPMVMGYFZBMVSYGKGT OLLJCBFKHHWFIVPPXPTVEJEBZBXHKNYKDYLIAKLLPJZFPVJAROJUOZZUWNZRRDZNYLGBHMNWUKJLSAXBUBWJZYCMVLYBCQJLBOROBDSZGHMCIA SVUCVNDTGDALKYLTOMJK

C:\Users\user\AppData\Local\Temp\LFU3OHDJ	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4507667042986948
Encrypted:	false
SSDEEP:	96:V/WU+bDoYysX0uhnydVjN9DLjGQLBE3u:V/l+bDo3irhnydVj3XBBE3u
MD5:	8D1E4EF2C47505BE17244F97D8591000
SHA1:	09EC63BD44834AC76F888D87C0A358532665D8B6
SHA-256:	A395EB3FFB419984F33F2AC9EE04A6257730A4600580812A5518957F50BB6D88
SHA-512:	B7EB3FE94FF62DD8D6BFEF55C0D79ABB2DAC65E30757E016B37CF78F29C27BDE89D0798CD21357B438EE4007D917AD830A11521DA3DC5C1988D73CBD9990F D1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\OHVS0ZUA	
Process:	C:\Users\user\AppData\Local\Temp\2757.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\Local\Temp\PALRGUCVEH.docx	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026

C:\Users\user\AppData\Local\Temp\PALRGUCVEH.docx	
Entropy (8bit):	4.696508269038202
Encrypted:	false
SSDEEP:	24:RSjVGe9uHEleifrd16Wa05tSl2jFQzpqPMXexMApqIjsp:2Ge9MQ/d16Wjtc2j64Phxjpq82
MD5:	0E9E92228B27AD7E7B4449467A529B0C
SHA1:	209F92CDFC879EE2B98DEF315CCE166AFEC00331
SHA-256:	284937D0EBFEDD95B2347297D957320D8D5CA5FC48218296767069CABA6B14A6
SHA-512:	CECA5F634268817B4A076414FFAB7D81F93EEC7E7D08B8691CCE0B2BCAF8FC694365455886E36983B4D8D758BC65BC1868BE8DB51AD41E082473726BB1FFD7I 8
Malicious:	false
Reputation:	unknown
Preview:	PALRGUCVEHIRKBYGKJJWKNMNYKFUTLHCEDOTKTWJCZHNZMOUNMNREQTGFDNZTATQQPDFONRIRAZYJEPXQVIVWNBDQIMKULZMUINYTVUPNMQBQQ YLGCAJYFEIWZTWGYTHEJPFBRNGCTANCYOISUQMRINVDUEIROITGPJZCCOVCZIZBHLYBDARSNRLEOQQDWOSMHXNRNBXNWMRVAQZUASARYHEITVT VSLHRGBYURPTEUNAUCYMZTXOZXKDXUEUUVTNGWGSBRAWIJZDVZDLMZBKEVESROLUEDPITQGUXFSRFAVNSESAFZLNXMXUYRFUEUKCMNFITMUQEW TCKEGDPOXHJSXBDLFIOLLHDYIVOQVEYJEZMDIOFXZFCPXJEQLPCSHKUGRQKXAUMKTHUMHWFQZRGBRZHGHYRXRODJXEBANQHOOVFBZXKJHDCAAK HZGSWGKGEDWOOCFCEYHPAQBYBKRXOTJWSCPMRDXNRYAQFQHSHOFCHWJDKTFHACROGLPZFWDCIBJSUTMTRHJKEGAHSBAQLDTWPTXB LVYYBNJBKDUNGOUDVWZOBKOJKSMZERYOYBNMDSYUPHFDPUXOMKCYNSEBJHJVXSWTIMBDLPWYMYMQKYICPQEWMYDUMYJRSVQHDEELUFOEQYUIZB TNUNJNZQTDTIJKNOJNFJDDGEYVGDXTQINCQDGJRRPOBRUHQLMKFJSSNNCQMDHWQYMHWIBVNPHRQCBTMYBSOJYXCUAYTWUDETCJTTEQSPXKTRSQ BDJYENXLXJTQIYOZHEFAQOFBXKATTASAWEYGDPTTLZDAFVKRYLRNFSWZYBGUMRHHMNPVCVECBEVWEXNMSCXSGJRAQKAYEIULWHXXFKTJWPDMYU AOSFBKCTNCTQQXTLXIIJKYOPYBMSFGYLZDGOXTVIHYLUMJCRDRQXFLBDAUXBTNAPMACHVQILKZSQLNPPJVGXAXUMTOUMJJJYJSPJALITYYHOOM VVOQNOSSPBLMRBWWPYXB

C:\Users\user\AppData\Local\Temp\PALRGUCVEH.xlsx	
Process:	C:\Users\user\AppData\Local\Temp\2757.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696508269038202
Encrypted:	false
SSDEEP:	24:RSjVGe9uHEleifrd16Wa05tSl2jFQzpqPMXexMApqIjsp:2Ge9MQ/d16Wjtc2j64Phxjpq82
MD5:	0E9E92228B27AD7E7B4449467A529B0C
SHA1:	209F92CDFC879EE2B98DEF315CCE166AFEC00331
SHA-256:	284937D0EBFEDD95B2347297D957320D8D5CA5FC48218296767069CABA6B14A6
SHA-512:	CECA5F634268817B4A076414FFAB7D81F93EEC7E7D08B8691CCE0B2BCAF8FC694365455886E36983B4D8D758BC65BC1868BE8DB51AD41E082473726BB1FFD7I 8
Malicious:	false
Reputation:	unknown
Preview:	PALRGUCVEHIRKBYGKJJWKNMNYKFUTLHCEDOTKTWJCZHNZMOUNMNREQTGFDNZTATQQPDFONRIRAZYJEPXQVIVWNBDQIMKULZMUINYTVUPNMQBQQ YLGCAJYFEIWZTWGYTHEJPFBRNGCTANCYOISUQMRINVDUEIROITGPJZCCOVCZIZBHLYBDARSNRLEOQQDWOSMHXNRNBXNWMRVAQZUASARYHEITVT VSLHRGBYURPTEUNAUCYMZTXOZXKDXUEUUVTNGWGSBRAWIJZDVZDLMZBKEVESROLUEDPITQGUXFSRFAVNSESAFZLNXMXUYRFUEUKCMNFITMUQEW TCKEGDPOXHJSXBDLFIOLLHDYIVOQVEYJEZMDIOFXZFCPXJEQLPCSHKUGRQKXAUMKTHUMHWFQZRGBRZHGHYRXRODJXEBANQHOOVFBZXKJHDCAAK HZGSWGKGEDWOOCFCEYHPAQBYBKRXOTJWSCPMRDXNRYAQFQHSHOFCHWJDKTFHACROGLPZFWDCIBJSUTMTRHJKEGAHSBAQLDTWPTXB LVYYBNJBKDUNGOUDVWZOBKOJKSMZERYOYBNMDSYUPHFDPUXOMKCYNSEBJHJVXSWTIMBDLPWYMYMQKYICPQEWMYDUMYJRSVQHDEELUFOEQYUIZB TNUNJNZQTDTIJKNOJNFJDDGEYVGDXTQINCQDGJRRPOBRUHQLMKFJSSNNCQMDHWQYMHWIBVNPHRQCBTMYBSOJYXCUAYTWUDETCJTTEQSPXKTRSQ BDJYENXLXJTQIYOZHEFAQOFBXKATTASAWEYGDPTTLZDAFVKRYLRNFSWZYBGUMRHHMNPVCVECBEVWEXNMSCXSGJRAQKAYEIULWHXXFKTJWPDMYU AOSFBKCTNCTQQXTLXIIJKYOPYBMSFGYLZDGOXTVIHYLUMJCRDRQXFLBDAUXBTNAPMACHVQILKZSQLNPPJVGXAXUMTOUMJJJYJSPJALITYYHOOM VVOQNOSSPBLMRBWWPYXB

C:\Users\user\AppData\Local\Temp\sdiimdop.exe	
Process:	C:\Users\user\AppData\Local\Temp\18D.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14973440
Entropy (8bit):	4.645907802057032
Encrypted:	false
SSDEEP:	6144:+AH3plu5xWDwtTwKc6+9YwoTPxSeI2co8mfgWddddddddddddddddddddddddddt:+AH3pCxvTS6Wh6PIeI/
MD5:	F548B3529CA470C25E50AF6220AD3098
SHA1:	A241FBA1FD229664849616D3425AC80DA447583B
SHA-256:	B9029679671D745FEE6E41A455E8DAAC8D64FC9DA159416596D02736A544D4AB
SHA-512:	1E6C0914678E07D1DBCA262F57D88ED54E35E6B15AC4E5ADFE74EBB001D323BB45CEA47F1CCB9995BC65B02C00CEAE5ACE2AE3AF590829050963514351AA5 CA7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....R.....Rich.....PE..L...15.`.....>.....+.....P....@.....*(.....<;..(.....`.....P..,#..`..... ...@.....text...n<.....>..... ..`.data...H%...P.....B.....@....lave.....X.....@....fidoce.K.....Z.....@....pihudu.....\.....@....lafog.....^.....@....rsrc...`.....l.....@..@.reloc...>...P.....@..B.....

C:\Users\user\AppData\Roaming\haifbcd	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	343040
Entropy (8bit):	6.634640145792183
Encrypted:	false
SSDEEP:	6144:5lA3X2bDueST6gKO1tqT7b4YlCTFGbGQ273pQGfT:5lA3X22e0VKYY70A4FOGQKt
MD5:	DC67C627917FF9724F3C1E6DB5F2DC27
SHA1:	4B7528999AD6095B3FBB3AEC059EFB88D999EA95
SHA-256:	26A4C5B36D9FDE80EA47137EB53B40DACF240432A5895F98417EAE51B6B681DA
SHA-512:	977AAB0AC60948315435E0698058598F40F42D7830B87EE7668BB209938CB388AA5B07C13B66C56DB1AFFA6F86A859B3C01666A22E437C808B6C9DB38975C7B0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....R.....Rich.....PE..L.... (._.....@.....P....@.....I=..(.....`.....P..8#..`..... ...@.....text....>. .....@..... ..`.data...H%...P.....D.....@....bekuvox.....Z.....@....jutu...K.....\.....@....vezev.....^.....@....mubone.....`..... .....@....rsrc...`.....n.....@..@.reloc...>...P...@.....@..B..... .....

C:\Users\user\AppData\Roaming\haifbcd: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:\Users\user\AppData\Roaming\scifbcd	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	358912
Entropy (8bit):	6.278717191933335
Encrypted:	false
SSDEEP:	6144:7e+RhbrOOFh9v2Y8zBk3L3gXO1RdFggj:7e6aOFhB8zBk3L3b1R
MD5:	1F935BFFF0F8128972BC69625E5B2A6C
SHA1:	18DB55C519BBE14311662A06FAEECC97566E2AFD
SHA-256:	2BFA0884B172C9EAFF7358741C164F571F0565389AB9CF99A8E0B90AE8AD914D
SHA-512:	2C94C1EA43B008CE164D7CD22A2D0FF3B60A623017007A2F361BDFF69ED72E97B0CC0897590BE9CC56333E014CD003786741EB6BB7887590CB2AAD832EA8A3D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..S/.../.../...1.Z.=...1.L.W....6..*.../.....1.K.....1.[.....1.^.....Rich/..... .....PE..L...t..`.....<...J.....4.....P....@.....A.....,9..<....0...Y.....#..P.....X...@..... .....text...4:.....<..... ..`.data...`....P.....@.....@....pamicak.....@....dos....K.....@....modav.....@. ...nugirof..... .....@....rsrc....Y...0...Z.....@..@.reloc...>.....@...:.....@..B..... .....

C:\Users\user\AppData\Roaming\wratetu	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	248375
Entropy (8bit):	**7.99937643116622**

C:\Users\user\AppData\Roaming\wratetu	
Encrypted:	**true**
SSDEEP:	6144:IkACiiHYkyeqaRSZryvUV2l1UQpP3lNfoY6TA:4C1YkGaUFoSAR
MD5:	5CFC7301CEC69F9AA0EDF70A574D4436
SHA1:	F739E265A1CE0AE4F83E408CC9F52878541B3718
SHA-256:	B4F15FCE9A5739BC29C5F2A9A22ADC707EA244763D4D4E79199202C8180A33CC
SHA-512:	26A6FF5587FA2CDAA9381728AE8E91D45F5A45D51431CC9710D625C4330723E802FA8393619CCABE8303B6C1F046FE3F91C8F68CEF37680BDD1E56ECD14A572
Malicious:	false
Reputation:	unknown
Preview:	

..{P..8......{.....l.(aU..-...K@n.$.....R...Z>..V.f.~.N..?i.}............pg*#...4.9~>S...x.T.(c80J9&... >QUT./,O...J...yp.A.R.....|...tf..,A.9-......F...#j...........B..!...#...v..Y.-..e<...r....6.V\.
.I.w..&..}.2b....x.-.qw.C.8..i..#c46I.......^..D.&@Ye.).U.wK...2{l..s..~...........Ja..1......B....s.[..)<.k.nNn.3Qk...+a..6G.x..5Y.WY....U.{l..}...c........I.....0.}.#, rJ...,dht......6....rw.}.6j`/}
.a/5,}..Z.%U.......qa.9.j(c.q.7..o..e.up.`.{.(o.*.....h....O........E..~..........bZ..Y.|.P.;..2..v#.0MV+.P.KW..8.90..l(.~..d.~wP.:.............dz.A...X..\ .5|V.|.if.(.2V7..l{J......M.ey..K..-..I..k
....V..z/mt......Ru..?C../K...;...D.}X...4~y.:=.H....J..`.){s...D.m!-.bv...D....=.....J.o..3..."{.^..7(@.H6........C.IL.#0m;.<9..+s..k....O....:X@|..+IR.g.Ja...L....yJ...xE.o1.P`.......5^U.M
....a.(t.rVs.mG..5.A..B..Ar.2Zi..|.^G...p?m...V.s$..~b..........o.. ..r..|zO.y=.h.Y5...jc..ei...0.....T.t.[O.*...$.NX#.T//.NM....x...j..l.......\...3`.$.G.

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

{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	7250
Entropy (8bit):	3.1662738963358006
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEE+Abd:cY+38+DJc+iGr+MZ+65+6tg+ECf+U
MD5:	D84538A0E9147E5B95BC1467B1B2896E
SHA1:	1FEDFAF48A265C0DE88815A8EA821B48F70CA1BA
SHA-256:	385EBB80F9EEBAD4B6B05FD2518ABBFC508981C992566B8844A9937BFD2EE9B0
SHA-512:	325545DCE9302944A12C8715BCFD5E23085E522D91133471EB4C818998725EC65ECF44EC033F3B237EBA0A1AF64048F5011DC4A97B3F014CDB246C9FDA85940
Malicious:	false
Reputation:	unknown
Preview:	

..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:.
.".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.
4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.
0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-
.-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220105_033224_675.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.312992075887116
Encrypted:	false
SSDEEP:	96:PCFdQ2o+HK5Lu9D2YPmCKTvI2l5SkGP4nlT2FbYFzGUMCl6JRW:Kf5Cml2CJxnC+w
MD5:	699F867B2888AADC69EA64322AFA75D9
SHA1:	1B6A8DFECF131411C6F6E4A2951A1C9ED8AA324B
SHA-256:	2DB7A93AD5A6FDD71E29DC63581BA513221F106F577A530AA84C4599795579A8
SHA-512:	AB460B75F2E7ED82E48301554696B523BEB69E7193686FF30911C62A38031F2736BAAE8AF021E80EF687CB4B4F09BF0C18426EE1BB843C0BA9ADE575DF400C18
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220105_033224_675.etl	
Preview:	....!.....I...@...M.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1...../_8..... .....h.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.:.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o.s.v.c...2.0.2.2.0.1.0.5._.0.3.3.2.2.4._.6.7.5...e.t.l.....P.P.l...@...M..... .....

C:\Windows\SysWOW64\dbgxuqbr\sdiimdop.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14973440
Entropy (8bit):	4.645907802057032
Encrypted:	false
SSDEEP:	6144:+AH3plu5xWDwtTwKc6+9YwoTPxSeI2co8mfgWddddddddddddddddddddddddddddt:+AH3pCxvTS6Wh6PIeI/
MD5:	F548B3529CA470C25E50AF6220AD3098
SHA1:	A241FBA1FD229664849616D3425AC80DA447583B
SHA-256:	B9029679671D745FEE6E41A455E8DAAC8D64FC9DA159416596D02736A544D4AB
SHA-512:	1E6C0914678E07D1DBCA262F57D88ED54E35E6B15AC4E5ADFE74EBB001D323BB45CEA47F1CCB9995BC65B02C00CEAE5ACE2AE3AF590829050963514351AA5CA7
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....R.....Rich.....PE..L...15.`.....>.....+.....P....@.....*(.....<;..(.....`.....P..,#..`..... ...@.....text...n<.....>..... ..`.data...H%...P.....B.....@....lave.....X.....@....fidoce.K.....Z.....@....pihudu.....\.....@....lafog.....^.....@....rsrc...`.....I.....@..@.reloc...>...P.....@..B..... .....

\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):	6.634640145792183
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:	nkINykHreE.exe
File size:	343040
MD5:	dc67c627917ff9724f3c1e6db5f2dc27
SHA1:	4b7528999ad6095b3fbb3aec059efb88d999ea95

General

SHA256:	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da
SHA512:	977aab0ac60948315435e0698058598f40f42d7830b87e7668bb209938cb388aa5b07c13b66c56db1affa6f86a859b3c01666a22e437c808b6c9db38975c7b0
SSDEEP:	6144:5lA3X2bDueST6gKO1tqT7b4YlCTFGbGQ273pQGfT:5lA3X22e0VKYY70A4FOGQKt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....R.....Rich.....PE..L....(._.....@.....

File Icon

Icon Hash:	c8d0d8e0f8e8f4e8

Static PE Info

General

Entrypoint:	0x422e10
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F83280E [Sun Oct 11 15:43:10 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	e64508a754c560e6e71788b6f0d7d44d

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x43e9e	0x44000	False	0.564783432904	data	6.85301887621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x45000	0x12548	0x1600	False	0.234907670455	data	3.04465131618	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bekuvox	0x58000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.jutu	0x59000	0x4b	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.vezev	0x5a000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.mubone	0x5b000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5c000	0x8d60	0x8e00	False	0.550533670775	data	5.61683000137	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	0x65000	0x3e84	0x4000	False	0.444885253906	data	4.56707219047	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
Spanish	Colombia	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 4, 2022 19:32:46.068125010 CET	192.168.2.5	8.8.8.8	0xa222	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:46.522274017 CET	192.168.2.5	8.8.8.8	0x1dac	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:46.762934923 CET	192.168.2.5	8.8.8.8	0x3779	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:49.101771116 CET	192.168.2.5	8.8.8.8	0xc7a1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:49.602319002 CET	192.168.2.5	8.8.8.8	0x6825	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:49.792771101 CET	192.168.2.5	8.8.8.8	0x32ab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:50.012084007 CET	192.168.2.5	8.8.8.8	0x8894	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:50.247939110 CET	192.168.2.5	8.8.8.8	0x737b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:51.090269089 CET	192.168.2.5	8.8.8.8	0xd2c8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:52.477201939 CET	192.168.2.5	8.8.8.8	0x6d65	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:52.706748009 CET	192.168.2.5	8.8.8.8	0x9137	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:52.900149107 CET	192.168.2.5	8.8.8.8	0x94cc	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:58.898350954 CET	192.168.2.5	8.8.8.8	0x1aac	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.098107100 CET	192.168.2.5	8.8.8.8	0xe35f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.327708006 CET	192.168.2.5	8.8.8.8	0x8438	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.674631119 CET	192.168.2.5	8.8.8.8	0xe561	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 4, 2022 19:32:59.864639997 CET	192.168.2.5	8.8.8.8	0x704a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.076483965 CET	192.168.2.5	8.8.8.8	0x5d01	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.225028038 CET	192.168.2.5	8.8.8.8	0x7970	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.468554020 CET	192.168.2.5	8.8.8.8	0xe4e9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.660439968 CET	192.168.2.5	8.8.8.8	0x4743	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.858905077 CET	192.168.2.5	8.8.8.8	0x519a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.054914951 CET	192.168.2.5	8.8.8.8	0xd873	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.209578991 CET	192.168.2.5	8.8.8.8	0xda71	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.414587975 CET	192.168.2.5	8.8.8.8	0x4d1b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.599988937 CET	192.168.2.5	8.8.8.8	0x2fd5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:03.951637030 CET	192.168.2.5	8.8.8.8	0x976c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.237740993 CET	192.168.2.5	8.8.8.8	0x31e8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.671008110 CET	192.168.2.5	8.8.8.8	0xc580	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.939270973 CET	192.168.2.5	8.8.8.8	0x41f1	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:06.717139959 CET	192.168.2.5	8.8.8.8	0x90ad	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:06.937068939 CET	192.168.2.5	8.8.8.8	0x7076	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:07.161817074 CET	192.168.2.5	8.8.8.8	0x9148	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:19.001461029 CET	192.168.2.5	8.8.8.8	0xa28d	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:21.695975065 CET	192.168.2.5	8.8.8.8	0x5f1a	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:26.991641045 CET	192.168.2.5	8.8.8.8	0xc31b	Standard query (0)	srtuiyhuali.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.102307081 CET	192.168.2.5	8.8.8.8	0xfdaf	Standard query (0)	fufuiloirtu.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.401127100 CET	192.168.2.5	8.8.8.8	0xd20f	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:28.449157000 CET	192.168.2.5	8.8.8.8	0x677a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:28.648585081 CET	192.168.2.5	8.8.8.8	0xeac7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:28.864703894 CET	192.168.2.5	8.8.8.8	0xaf9d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:29.094826937 CET	192.168.2.5	8.8.8.8	0x391e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:29.316817999 CET	192.168.2.5	8.8.8.8	0x269d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:29.844449997 CET	192.168.2.5	8.8.8.8	0xcc97	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.447838068 CET	192.168.2.5	8.8.8.8	0x12fe	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.099167109 CET	192.168.2.5	8.8.8.8	0xc397	Standard query (0)	unic11m.top	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.174964905 CET	192.168.2.5	8.8.8.8	0x4747	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.128079891 CET	192.168.2.5	8.8.8.8	0xaf8d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.340699911 CET	192.168.2.5	8.8.8.8	0x10d6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.422482967 CET	192.168.2.5	8.8.8.8	0xffce	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.560332060 CET	192.168.2.5	8.8.8.8	0xc629	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.560527086 CET	192.168.2.5	8.8.8.8	0xe0bf	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 4, 2022 19:33:34.753875971 CET	192.168.2.5	8.8.8.8	0x5b0c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.005836964 CET	192.168.2.5	8.8.8.8	0x8a73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.208940983 CET	192.168.2.5	8.8.8.8	0x5e72	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.405631065 CET	192.168.2.5	8.8.8.8	0x4282	Standard query (0)	bitly.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.613956928 CET	192.168.2.5	8.8.8.8	0x3f02	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.803725958 CET	192.168.2.5	8.8.8.8	0x95fd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:36.023104906 CET	192.168.2.5	8.8.8.8	0x1073	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:39.749269009 CET	192.168.2.5	8.8.8.8	0x701e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.010328054 CET	192.168.2.5	8.8.8.8	0x2760	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.206621885 CET	192.168.2.5	8.8.8.8	0xa59c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.420351028 CET	192.168.2.5	8.8.8.8	0x9126	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.626512051 CET	192.168.2.5	8.8.8.8	0x5442	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.345593929 CET	192.168.2.5	8.8.8.8	0x6e9f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.560367107 CET	192.168.2.5	8.8.8.8	0x6967	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.754925966 CET	192.168.2.5	8.8.8.8	0xecbb	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:42.468024015 CET	192.168.2.5	8.8.8.8	0x8583	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:42.671868086 CET	192.168.2.5	8.8.8.8	0xdb32	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:42.878957033 CET	192.168.2.5	8.8.8.8	0xda5b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.082484007 CET	192.168.2.5	8.8.8.8	0xace2	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.530966997 CET	192.168.2.5	8.8.8.8	0xe291	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.755482912 CET	192.168.2.5	8.8.8.8	0xbe44	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.944658041 CET	192.168.2.5	8.8.8.8	0x50d2	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:44.127238989 CET	192.168.2.5	8.8.8.8	0xfbff	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:44.359674931 CET	192.168.2.5	8.8.8.8	0xb809	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.159487963 CET	192.168.2.5	8.8.8.8	0xfe7d	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.899182081 CET	192.168.2.5	8.8.8.8	0xbcb0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.899224043 CET	192.168.2.5	8.8.8.8	0x75bd	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.156876087 CET	192.168.2.5	8.8.8.8	0xe695	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.337910891 CET	192.168.2.5	8.8.8.8	0xe22	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.527611971 CET	192.168.2.5	8.8.8.8	0xf446	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.782988071 CET	192.168.2.5	8.8.8.8	0xe2bc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:49.615017891 CET	192.168.2.5	8.8.8.8	0xf5c2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:50.413440943 CET	192.168.2.5	8.8.8.8	0x229b	Standard query (0)	f0616068.xsph.ru	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.840620041 CET	192.168.2.5	8.8.8.8	0x552e	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.842330933 CET	192.168.2.5	8.8.8.8	0x20b7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.032028913 CET	192.168.2.5	8.8.8.8	0x7863	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.235112906 CET	192.168.2.5	8.8.8.8	0x5562	Standard query (0)	vk.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 4, 2022 19:33:55.874588013 CET	192.168.2.5	8.8.8.8	0x6dd4	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.889983892 CET	192.168.2.5	8.8.8.8	0xb791	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.095582962 CET	192.168.2.5	8.8.8.8	0xb3a8	Standard query (0)	natribu.org	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.359882116 CET	192.168.2.5	8.8.8.8	0x463	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.645442963 CET	192.168.2.5	8.8.8.8	0xeeb3	Standard query (0)	natribu.org	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.882695913 CET	192.168.2.5	8.8.8.8	0x6c1f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:57.091738939 CET	192.168.2.5	8.8.8.8	0xd80f	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:57.651737928 CET	192.168.2.5	8.8.8.8	0x77fa	Standard query (0)	mstdn.social	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.141839981 CET	192.168.2.5	8.8.8.8	0x9f39	Standard query (0)	qoto.org	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.661042929 CET	192.168.2.5	8.8.8.8	0x21ac	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:01.010947943 CET	192.168.2.5	8.8.8.8	0x38e7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.255312920 CET	192.168.2.5	8.8.8.8	0xcf58	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.317835093 CET	192.168.2.5	8.8.8.8	0x99	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.948523045 CET	192.168.2.5	8.8.8.8	0x644d	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:15.646044970 CET	192.168.2.5	8.8.8.8	0xfa2c	Standard query (0)	f0616071.xsph.ru	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:18.409645081 CET	192.168.2.5	8.8.8.8	0x635b	Standard query (0)	f0616073.xsph.ru	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:25.871715069 CET	192.168.2.5	8.8.8.8	0xc663	Standard query (0)	kent0mushinec0n3t.casacam.net	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:52.711987019 CET	192.168.2.5	8.8.8.8	0x6309	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 4, 2022 19:32:46.353008986 CET	8.8.8.8	192.168.2.5	0xa222	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:46.541034937 CET	8.8.8.8	192.168.2.5	0x1dac	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:47.085211992 CET	8.8.8.8	192.168.2.5	0x3779	No error (0)	privacytools-foryou-777.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:49.419750929 CET	8.8.8.8	192.168.2.5	0xc7a1	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:49.620958090 CET	8.8.8.8	192.168.2.5	0x6825	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:49.810087919 CET	8.8.8.8	192.168.2.5	0x32ab	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:50.031019926 CET	8.8.8.8	192.168.2.5	0x8894	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:50.579771042 CET	8.8.8.8	192.168.2.5	0x737b	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:51.108448029 CET	8.8.8.8	192.168.2.5	0xd2c8	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:52.495677948 CET	8.8.8.8	192.168.2.5	0x6d65	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:52.725264072 CET	8.8.8.8	192.168.2.5	0x9137	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:32:53.194371939 CET	8.8.8.8	192.168.2.5	0x94cc	No error (0)	data-host-coin-8.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:58.915494919 CET	8.8.8.8	192.168.2.5	0x1aac	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.117124081 CET	8.8.8.8	192.168.2.5	0xe35f	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.346348047 CET	8.8.8.8	192.168.2.5	0x8438	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.693615913 CET	8.8.8.8	192.168.2.5	0xe561	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:32:59.883378983 CET	8.8.8.8	192.168.2.5	0x704a	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.179717064 CET	8.8.8.8	192.168.2.5	0x5d01	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.243674040 CET	8.8.8.8	192.168.2.5	0x7970	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.487281084 CET	8.8.8.8	192.168.2.5	0xe4e9	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.679090023 CET	8.8.8.8	192.168.2.5	0x4743	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:00.875922918 CET	8.8.8.8	192.168.2.5	0x519a	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.073401928 CET	8.8.8.8	192.168.2.5	0xd873	No error (0)	data-host-coin-8.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.228178024 CET	8.8.8.8	192.168.2.5	0xda71	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.433686972 CET	8.8.8.8	192.168.2.5	0x4d1b	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:01.618597984 CET	8.8.8.8	192.168.2.5	0x2fd5	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:03.967916012 CET	8.8.8.8	192.168.2.5	0x976c	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.256407022 CET	8.8.8.8	192.168.2.5	0x31e8	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.689863920 CET	8.8.8.8	192.168.2.5	0xc580	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.959872007 CET	8.8.8.8	192.168.2.5	0x41f1	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.959872007 CET	8.8.8.8	192.168.2.5	0x41f1	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.959872007 CET	8.8.8.8	192.168.2.5	0x41f1	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.959872007 CET	8.8.8.8	192.168.2.5	0x41f1	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:04.959872007 CET	8.8.8.8	192.168.2.5	0x41f1	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:06.735904932 CET	8.8.8.8	192.168.2.5	0x90ad	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:06.956106901 CET	8.8.8.8	192.168.2.5	0x7076	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:07.180413961 CET	8.8.8.8	192.168.2.5	0x9148	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:19.018482924 CET	8.8.8.8	192.168.2.5	0xa28d	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:19.018482924 CET	8.8.8.8	192.168.2.5	0xa28d	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:19.018482924 CET	8.8.8.8	192.168.2.5	0xa28d	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:19.018482924 CET	8.8.8.8	192.168.2.5	0xa28d	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:19.018482924 CET	8.8.8.8	192.168.2.5	0xa28d	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:19.018482924 CET	8.8.8.8	192.168.2.5	0xa28d	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:22.009233952 CET	8.8.8.8	192.168.2.5	0x5f1a	No error (0)	patmushta.info		194.87.235.183	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.024240017 CET	8.8.8.8	192.168.2.5	0xc31b	Server failure (2)	srtuiyhuali.at	none	none	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:27.790396929 CET	8.8.8.8	192.168.2.5	0xd20f	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:28.468234062 CET	8.8.8.8	192.168.2.5	0x677a	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:28.667419910 CET	8.8.8.8	192.168.2.5	0xeac7	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:28.881932974 CET	8.8.8.8	192.168.2.5	0xaf9d	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:29.113784075 CET	8.8.8.8	192.168.2.5	0x391e	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:29.335551977 CET	8.8.8.8	192.168.2.5	0x269d	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:30.222142935 CET	8.8.8.8	192.168.2.5	0xcc97	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:31.466578007 CET	8.8.8.8	192.168.2.5	0x12fe	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.120434046 CET	8.8.8.8	192.168.2.5	0xc397	No error (0)	unic11m.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:32.514951944 CET	8.8.8.8	192.168.2.5	0x4747	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.146827936 CET	8.8.8.8	192.168.2.5	0xaf8d	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.357781887 CET	8.8.8.8	192.168.2.5	0x10d6	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.439455032 CET	8.8.8.8	192.168.2.5	0xffce	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.577033997 CET	8.8.8.8	192.168.2.5	0xc629	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.772905111 CET	8.8.8.8	192.168.2.5	0x5b0c	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:34.882680893 CET	8.8.8.8	192.168.2.5	0xe0bf	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.024795055 CET	8.8.8.8	192.168.2.5	0x8a73	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.226968050 CET	8.8.8.8	192.168.2.5	0x5e72	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.226968050 CET	8.8.8.8	192.168.2.5	0x5e72	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.423835993 CET	8.8.8.8	192.168.2.5	0x4282	No error (0)	bitly.com		67.199.248.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.423835993 CET	8.8.8.8	192.168.2.5	0x4282	No error (0)	bitly.com		67.199.248.14	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.630799055 CET	8.8.8.8	192.168.2.5	0x3f02	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:35.820178032 CET	8.8.8.8	192.168.2.5	0x95fd	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:36.348193884 CET	8.8.8.8	192.168.2.5	0x1073	No error (0)	data-host-coin-8.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:39.769187927 CET	8.8.8.8	192.168.2.5	0x701e	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.029031992 CET	8.8.8.8	192.168.2.5	0x2760	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.223347902 CET	8.8.8.8	192.168.2.5	0xa59c	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.438524961 CET	8.8.8.8	192.168.2.5	0x9126	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.438524961 CET	8.8.8.8	192.168.2.5	0x9126	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.650187969 CET	8.8.8.8	192.168.2.5	0x5442	No error (0)	www.mediafire.com		104.16.203.237	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:40.650187969 CET	8.8.8.8	192.168.2.5	0x5442	No error (0)	www.mediafire.com		104.16.202.237	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.363959074 CET	8.8.8.8	192.168.2.5	0x6e9f	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.579073906 CET	8.8.8.8	192.168.2.5	0x6967	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.579073906 CET	8.8.8.8	192.168.2.5	0x6967	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.771428108 CET	8.8.8.8	192.168.2.5	0xecbb	No error (0)	www.mediafire.com		104.16.203.237	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:41.771428108 CET	8.8.8.8	192.168.2.5	0xecbb	No error (0)	www.mediafire.com		104.16.202.237	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:42.485076904 CET	8.8.8.8	192.168.2.5	0x8583	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:42.689954042 CET	8.8.8.8	192.168.2.5	0xdb32	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:42.895642042 CET	8.8.8.8	192.168.2.5	0xda5b	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.105460882 CET	8.8.8.8	192.168.2.5	0xace2	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.105460882 CET	8.8.8.8	192.168.2.5	0xace2	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.549119949 CET	8.8.8.8	192.168.2.5	0xe291	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.774574041 CET	8.8.8.8	192.168.2.5	0xbe44	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:43.963344097 CET	8.8.8.8	192.168.2.5	0x50d2	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:44.144305944 CET	8.8.8.8	192.168.2.5	0xfbff	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:44.378165007 CET	8.8.8.8	192.168.2.5	0xb809	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:46.598094940 CET	8.8.8.8	192.168.2.5	0xfe7d	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917447090 CET	8.8.8.8	192.168.2.5	0xbcb0	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:47.917687893 CET	8.8.8.8	192.168.2.5	0x75bd	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.173059940 CET	8.8.8.8	192.168.2.5	0xe695	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.355176926 CET	8.8.8.8	192.168.2.5	0xe22	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.546367884 CET	8.8.8.8	192.168.2.5	0xf446	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:48.801156044 CET	8.8.8.8	192.168.2.5	0xe2bc	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:49.633609056 CET	8.8.8.8	192.168.2.5	0xf5c2	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:50.536936998 CET	8.8.8.8	192.168.2.5	0x229b	No error (0)	f0616068.xsph.ru		141.8.193.236	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.859932899 CET	8.8.8.8	192.168.2.5	0x552e	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:54.861382008 CET	8.8.8.8	192.168.2.5	0x20b7	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.048371077 CET	8.8.8.8	192.168.2.5	0x7863	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.254973888 CET	8.8.8.8	192.168.2.5	0x5562	No error (0)	vk.com		87.240.190.72	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.254973888 CET	8.8.8.8	192.168.2.5	0x5562	No error (0)	vk.com		87.240.190.78	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.254973888 CET	8.8.8.8	192.168.2.5	0x5562	No error (0)	vk.com		93.186.225.208	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.254973888 CET	8.8.8.8	192.168.2.5	0x5562	No error (0)	vk.com		87.240.139.194	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.254973888 CET	8.8.8.8	192.168.2.5	0x5562	No error (0)	vk.com		87.240.137.158	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.254973888 CET	8.8.8.8	192.168.2.5	0x5562	No error (0)	vk.com		87.240.190.67	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:55.895823956 CET	8.8.8.8	192.168.2.5	0x6dd4	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:33:55.909377098 CET	8.8.8.8	192.168.2.5	0xb791	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.112481117 CET	8.8.8.8	192.168.2.5	0xb3a8	No error (0)	natribu.org		178.248.232.78	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.378345013 CET	8.8.8.8	192.168.2.5	0x463	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.710943937 CET	8.8.8.8	192.168.2.5	0xeeb3	No error (0)	natribu.org		178.248.232.78	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:56.901292086 CET	8.8.8.8	192.168.2.5	0x6c1f	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:57.376915932 CET	8.8.8.8	192.168.2.5	0xd80f	No error (0)	data-host-coin-8.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:57.669960976 CET	8.8.8.8	192.168.2.5	0x77fa	No error (0)	mstdn.social		116.202.14.219	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.163434982 CET	8.8.8.8	192.168.2.5	0x9f39	No error (0)	qoto.org		51.91.13.105	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:33:58.680798054 CET	8.8.8.8	192.168.2.5	0x21ac	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:01.027271986 CET	8.8.8.8	192.168.2.5	0x38e7	No error (0)	host-data-coin-11.com		89.223.65.17	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		152.0.118.227	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		187.156.124.76	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		110.14.121.125	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		189.129.105.161	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.271924019 CET	8.8.8.8	192.168.2.5	0xcf58	No error (0)	amogohuigotuli.at		61.98.7.133	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:02.645013094 CET	8.8.8.8	192.168.2.5	0x99	No error (0)	patmushta.info		194.87.235.183	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.969244003 CET	8.8.8.8	192.168.2.5	0x644d	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.969244003 CET	8.8.8.8	192.168.2.5	0x644d	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.969244003 CET	8.8.8.8	192.168.2.5	0x644d	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.969244003 CET	8.8.8.8	192.168.2.5	0x644d	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.969244003 CET	8.8.8.8	192.168.2.5	0x644d	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:13.969244003 CET	8.8.8.8	192.168.2.5	0x644d	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:15.665023088 CET	8.8.8.8	192.168.2.5	0xfa2c	No error (0)	f0616071.xsph.ru		141.8.193.236	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:18.436789989 CET	8.8.8.8	192.168.2.5	0x635b	No error (0)	f0616073.xsph.ru		141.8.193.236	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:26.044899940 CET	8.8.8.8	192.168.2.5	0xc663	No error (0)	kent0mushinec0n3t.casacam.net		95.143.179.186	A (IP address)	IN (0x0001)
Jan 4, 2022 19:34:53.007128000 CET	8.8.8.8	192.168.2.5	0x6309	No error (0)	patmushta.info		194.87.235.183	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mnxwgte.com
  - host-data-coin-11.com
- fcsijwjo.com
- privacytools-foryou-777.com
- xxvce.org
- nbivn.net
- mqtuiygbd.org
- hyipaj.net
- ixfmgcxna.org
- hcnexlv.com
- shqbxq.com

- mrxnaw.com
- data-host-coin-8.com
- kyrrypaj.net
- wpjrovehat.org
- gemicjpf.com
- kgdrt.com
- pbwsr.com
- unicupload.top
- tinpgbjvs.net
- trkju.org
- affpnhtco.com
- biuigjh.net
- bbqijtelr.com
- ergvrb.org
- dcppl.net
- 185.7.214.171:8080
- gnleqagbe.net
- ffijaqcca.net
- edakogho.org
- ccihwcxvgc.net
- vnhfrdnsx.net
- nbajd.com
- sehol.com
  - amogohuigotuli.at
- qquvonfakj.net
- rqgjiitwa.com
- wkshgd.net
- lpdsum.com
- pefdgmtoj.com
- 91.243.44.130

- opjngj.com
- rbkjpfevn.com
- unic11m.top
- xujjips.org
- luqilpnni.org
- smurvjp.com
- pbysostxi.net
- xggvos.org
- upxogvba.net
- qjoorlrk.org
- tahqfcsy.com
- tuosodl.net
- 185.7.214.239
- mnrycwnvnv.com
- lqhxjo.org
- hhtdbo.net
- pcfbatp.net
- yytvtctaug.net
- lmpxg.com
- nxxtbccl.net
- uqmves.org
- xhxsjp.org
- skgfhxg.org
- qlaiw.org
- qopqxs.net
- cqutypagk.com
- ahkpouvwup.com
- gxtcaqi.org
- hrsmjturj.org
- jwmtctjvqt.org

- amqeeswq.net
- f0616068.xsph.ru
- gnnwam.com
- hwgkv.com
- fleiunffw.com
- vk.com
- ouwak.org
- gyuyyjn.com
- natribu.org
- sxetmnxgu.com
- whjllmlg.org
- jjrpdilcbv.org
- 65.108.180.72
- 116.202.186.120
- ersxoxafng.com
- f0616071.xsph.ru
- f0616073.xsph.ru

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: nkINykHreE.exe PID: 800 Parent PID: 1544

General

Start time:	19:32:03
Start date:	04/01/2022
Path:	C:\Users\user\Desktop\nkINykHreE.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nkINykHreE.exe"
Imagebase:	0x400000
File size:	343040 bytes
MD5 hash:	DC67C627917FF9724F3C1E6DB5F2DC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: nkINykHreE.exe PID: 3092 Parent PID: 800

General

Start time:	19:32:05
Start date:	04/01/2022
Path:	C:\Users\user\Desktop\nkINykHreE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nkINykHreE.exe"
Imagebase:	0x400000
File size:	343040 bytes
MD5 hash:	DC67C627917FF9724F3C1E6DB5F2DC27
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: 00000001.00000002.297306514.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.297326406.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3472 Parent PID: 3092

General

Start time:	19:32:11
Start date:	04/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000000.282842442.0000000003A61000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6444 Parent PID: 556

General

Start time:	19:32:13
Start date:	04/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6644 Parent PID: 556

General

Start time:	19:32:23
Start date:	04/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6720 Parent PID: 556

General

Start time:	19:32:24
Start date:	04/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6816 Parent PID: 556

General

Start time:	19:32:24
Start date:	04/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 6868 Parent PID: 556

General

Start time:	19:32:25
Start date:	04/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff797770000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6888 Parent PID: 556

General

Start time:	19:32:26
Start date:	04/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: haifbcd PID: 2908 Parent PID: 904

General

Start time:	19:32:47
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Roaming\haifbcd
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\haifbcd
Imagebase:	0x400000
File size:	343040 bytes
MD5 hash:	DC67C627917FF9724F3C1E6DB5F2DC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 115B.exe PID: 340 Parent PID: 3472

General

Start time:	19:32:47
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\115B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\115B.exe
Imagebase:	0x400000
File size:	343040 bytes
MD5 hash:	DC67C627917FF9724F3C1E6DB5F2DC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: haifbcd PID: 4544 Parent PID: 2908

General

Start time:	19:32:49
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Roaming\haifbcd
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\haifbcd
Imagebase:	0x400000
File size:	343040 bytes
MD5 hash:	DC67C627917FF9724F3C1E6DB5F2DC27
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: 0000000F.00000002.352429754.0000000002091000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000F.00000002.352266837.00000000005C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 115B.exe PID: 1412 Parent PID: 340

General

Start time:	19:32:50
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\115B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\115B.exe
Imagebase:	0x400000
File size:	343040 bytes
MD5 hash:	DC67C627917FF9724F3C1E6DB5F2DC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 2997.exe PID: 6936 Parent PID: 3472

General

Start time:	19:32:57
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2997.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2997.exe
Imagebase:	0x400000
File size:	358912 bytes
MD5 hash:	1F935BFFF0F8128972BC69625E5B2A6C
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: 00000011.00000002.370053936.0000000000751000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.370019662.0000000000620000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 18D.exe PID: 4992 Parent PID: 3472

General

Start time:	19:33:02
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\18D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\18D.exe
Imagebase:	0x400000
File size:	342528 bytes
MD5 hash:	B7B184D2B0910148CABB9B5E915753D6
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: 00000012.00000002.390911110.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000012.00000002.390725871.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000012.00000003.369452134.0000000000560000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: CBA.exe PID: 5652 Parent PID: 3472

General

Start time:	19:33:05
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\CBA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CBA.exe
Imagebase:	0xcb0000
File size:	539136 bytes
MD5 hash:	6C72997AA5DD44A44B27BD36347BAED9
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: 00000013.00000002.408243360.0000000004121000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 6552 Parent PID: 4992

General

Start time:	19:33:08
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\dbgxuqbr\
Imagebase:	0x150000
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: 5032 Parent PID: 6552

General

Start time:	19:33:08
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1768 Parent PID: 4992

General

Start time:	19:33:09
Start date:	04/01/2022
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\sdiimdop.exe" C:\Windows\SysWOW64\dbgxuqbr\
Imagebase:	0x150000
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: 4996 Parent PID: 1768

General

Start time:	19:33:09
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 2856 Parent PID: 4992

General

Start time:	19:33:10
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create dbgxuqbr binPath= "C:\Windows\SysWOW64\dbgxuqbr\sdiimdop.exe /d\"C:\Users\user\AppData\Local\Temp\18D.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x1170000
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: 3952 Parent PID: 2856

General

Start time:	19:33:10
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 4784 Parent PID: 4992

General

Start time:	19:33:11
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description dbgxuqbr "wifi internet conection
Imagebase:	0x1170000
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: 4696 Parent PID: 4784

General

Start time:	19:33:11
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6404 Parent PID: 4992

General

Start time:	19:33:12
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start dbgxuqbr
Imagebase:	0x1170000
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: 6972 Parent PID: 6404

General

Start time:	19:33:13
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 7000 Parent PID: 4992

General

Start time:	19:33:13
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x11f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: sdiimdop.exe PID: 4560 Parent PID: 556

General

Start time:	19:33:15
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\dbgxuqbr\sdiimdop.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\dbgxuqbr\sdiimdop.exe /d"C:\Users\user\AppData\Local\Temp\18D.exe"
Imagebase:	0x400000
File size:	14973440 bytes
MD5 hash:	F548B3529CA470C25E50AF6220AD3098
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: 0000001F.00000002.396765412.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001F.00000003.395236716.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001F.00000002.396983806.0000000000600000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001F.00000002.396894340.0000000000540000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 2076 Parent PID: 7000

General

Start time:	19:33:15
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CBA.exe PID: 7052 Parent PID: 5652

General

Start time:	19:33:15
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\CBA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CBA.exe
Imagebase:	0xf90000
File size:	539136 bytes
MD5 hash:	6C72997AA5DD44A44B27BD36347BAED9
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: 00000021.00000000.402116569.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000021.00000000.403620699.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000021.00000000.401238970.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000021.00000002.515289620.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000021.00000000.403113050.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 5180 Parent PID: 4560

General

Start time:	19:33:17
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0x930000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000022.00000002.550647204.0000000002BB0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 7064 Parent PID: 556

General

Start time:	19:33:22
Start date:	04/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 4176 Parent PID: 6888

General

Start time:	19:33:27
Start date:	04/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff66d780000

File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4140 Parent PID: 4176

General

Start time:	19:33:27
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: scifbcd PID: 6852 Parent PID: 904

General

Start time:	19:33:27
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Roaming\scifbcd
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\scifbcd
Imagebase:	0x400000
File size:	358912 bytes
MD5 hash:	1F935BFFF0F8128972BC69625E5B2A6C
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: 00000026.00000002.444174815.0000000000951000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000026.00000002.442728079.0000000000630000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: 2757.exe PID: 2904 Parent PID: 3472

General

Start time:	19:33:31
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2757.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2757.exe
Imagebase:	0x1150000
File size:	1497920 bytes
MD5 hash:	67B848B139E584BF3361A51160FC6731
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: 00000027.00000002.537263879.00000000008C7000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000027.00000002.537263879.00000000008C7000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: 4187.exe PID: 6064 Parent PID: 3472

General

Start time:	19:33:37
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\4187.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\4187.exe
Imagebase:	0x400000
File size:	760832 bytes
MD5 hash:	C085684DB882063C21F18D251679B0CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis