ID: 552969
Sample Name:
U3E7zMaux2.exe
Cookbook: default.jbs
Time: 00:13:36
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

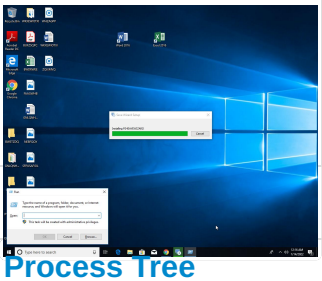
Windows Analysis Report U3E7zMaux2.exe

Overview

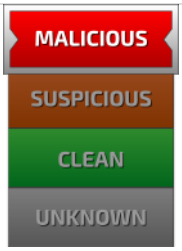
General Information

Sample Name:	U3E7zMaux2.exe
Analysis ID:	552969
MD5:	8362e0f91ae3379.
SHA1:	ec761f77bbe9900.
SHA256:	adfea20237be615.
Tags:	CoinMiner exe
Infos:	

Most interesting Screenshot:



Detection



Amadey Raccoon RedLine SmokeLoader Tofsee Vidar

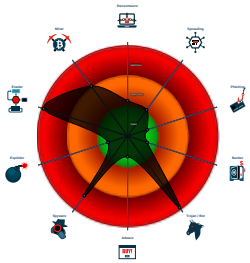
Score: 100
Range: 50 - 100

Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- U3E7zMaux2.exe (PID: 6688 cmdline: "C:\Users\user\Desktop\U3E7zMaux2.exe" MD5: 8362E0F91AE3379C73422BBCA7BAC493)
  - U3E7zMaux2.exe (PID: 6728 cmdline: "C:\Users\user\Desktop\U3E7zMaux2.exe" MD5: 8362E0F91AE3379C73422BBCA7BAC493)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - D984.exe (PID: 5756 cmdline: C:\Users\user\AppData\Local\Temp\D984.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 6712 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5756 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - E666.exe (PID: 4780 cmdline: C:\Users\user\AppData\Local\Temp\E666.exe MD5: 8362E0F91AE3379C73422BBCA7BAC493)
        - E666.exe (PID: 4388 cmdline: C:\Users\user\AppData\Local\Temp\E666.exe MD5: 8362E0F91AE3379C73422BBCA7BAC493)
      - 7CA1.exe (PID: 5352 cmdline: C:\Users\user\AppData\Local\Temp\7CA1.exe MD5: 3754DB9964B0177B6E905999B6F18FD7)
      - 86C4.exe (PID: 1368 cmdline: C:\Users\user\AppData\Local\Temp\86C4.exe MD5: B11C5DEFDBA76C2B3EE67EE1B474389D)
        - cmd.exe (PID: 5208 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\shayesoq\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - conhost.exe (PID: 4648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - cmd.exe (PID: 5464 cmdline: C:\Windows\sysnative\cmd" /c "C:\Users\user\AppData\Local\Temp\738C.tmp\738D.tmp\738E.bat C:\Users\user\AppData\Local\Temp\9A02.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
              - extd.exe (PID: 6816 cmdline: C:\Users\user\AppData\Local\Temp\738C.tmp\738D.tmp\extd.exe "/hideself" "" "" "" "" "" "" "" "" "" "" MD5: 139B5CE627BC9EC1040A91EBE7830F7C)
        - cmd.exe (PID: 6392 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\lagavljy.exe" C:\Windows\SysWOW64\shayesoq\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 3496 cmdline: C:\Windows\System32\sc.exe" create shayesoq binPath= "C:\Windows\SysWOW64\shayesoq\lagavljy.exe /d\"C:\Users\user\AppData\Local\Temp\86C4.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 1716 cmdline: C:\Windows\System32\sc.exe" description shayesoq "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 4728 cmdline: "C:\Windows\System32\sc.exe" start shayesoq MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 5988 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: 5560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 8EC4.exe (PID: 6024 cmdline: C:\Users\user\AppData\Local\Temp\8EC4.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 8EC4.exe (PID: 6240 cmdline: C:\Users\user\AppData\Local\Temp\8EC4.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - 7801.exe (PID: 7032 cmdline: C:\Users\user\AppData\Local\Temp\7801.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - 8ED5.exe (PID: 5992 cmdline: C:\Users\user\AppData\Local\Temp\8ED5.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
        - mjlooy.exe (PID: 5568 cmdline: "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" MD5: 8B239554FE346656C8EEF9484CE8092F)
      - 9A02.exe (PID: 6000 cmdline: C:\Users\user\AppData\Local\Temp\9A02.exe MD5: 6E7430832C1C24C2BF8BE746F2FE583C)
- svchost.exe (PID: 2480 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6140 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- uufaeea (PID: 2804 cmdline: C:\Users\user\AppData\Roaming\uufaeea MD5: 8362E0F91AE3379C73422BBCA7BAC493)
  - uufaeea (PID: 6944 cmdline: C:\Users\user\AppData\Roaming\uufaeea MD5: 8362E0F91AE3379C73422BBCA7BAC493)
- svchost.exe (PID: 5444 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5680 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5788 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 5756 -ip 5756 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4936 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- lagavljy.exe (PID: 4544 cmdline: C:\Windows\SysWOW64\shayesoq\lagavljy.exe /d"C:\Users\user\AppData\Local\Temp\86C4.exe" MD5: 7A36C0AD3083A1519CCE3A67BB377D18)
  - svchost.exe (PID: 5940 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000032.00000002.864947877.0000000000BF0000.00000004.00000040.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
00000013.00000002.784101177.00000000006A1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000002E.00000003.894641410.00000000022C0000.00000004.00000040.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
00000032.00000002.864706939.00000000005F0000.00000004.00000020.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
00000027.00000002.922686278.0000000000320000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 42 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.uufaeea.4615a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
21.2.86C4.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
40.0.8EC4.exe.400000.10.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
19.2.E666.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
40.0.8EC4.exe.400000.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 34 entries				

Sigma Overview

System Summary:

- Sigma detected: Suspect Svchost Activity
- Sigma detected: Copying Sensitive Files with Credential Data
- Sigma detected: Suspicious Svchost Process
- Sigma detected: Netsh Port or Application Allowed
- Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

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

Bitcoin Miner:

- Found strings related to Crypto-Mining

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Yara detected BatToExe compiled binary

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

Persistence and Installation Behavior:

Yara detected Amadey bot

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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

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

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

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

- Found API chain indicative of debugger detection
- Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings
- Modifies the windows firewall

Stealing of Sensitive Information:

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Yara detected SmokeLoader
- Yara detected Amadey bot
- Yara detected Raccoon Stealer
- Yara detected Vidar stealer
- Yara detected Tofsee
- Tries to steal Mail credentials (via file / registry access)
- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

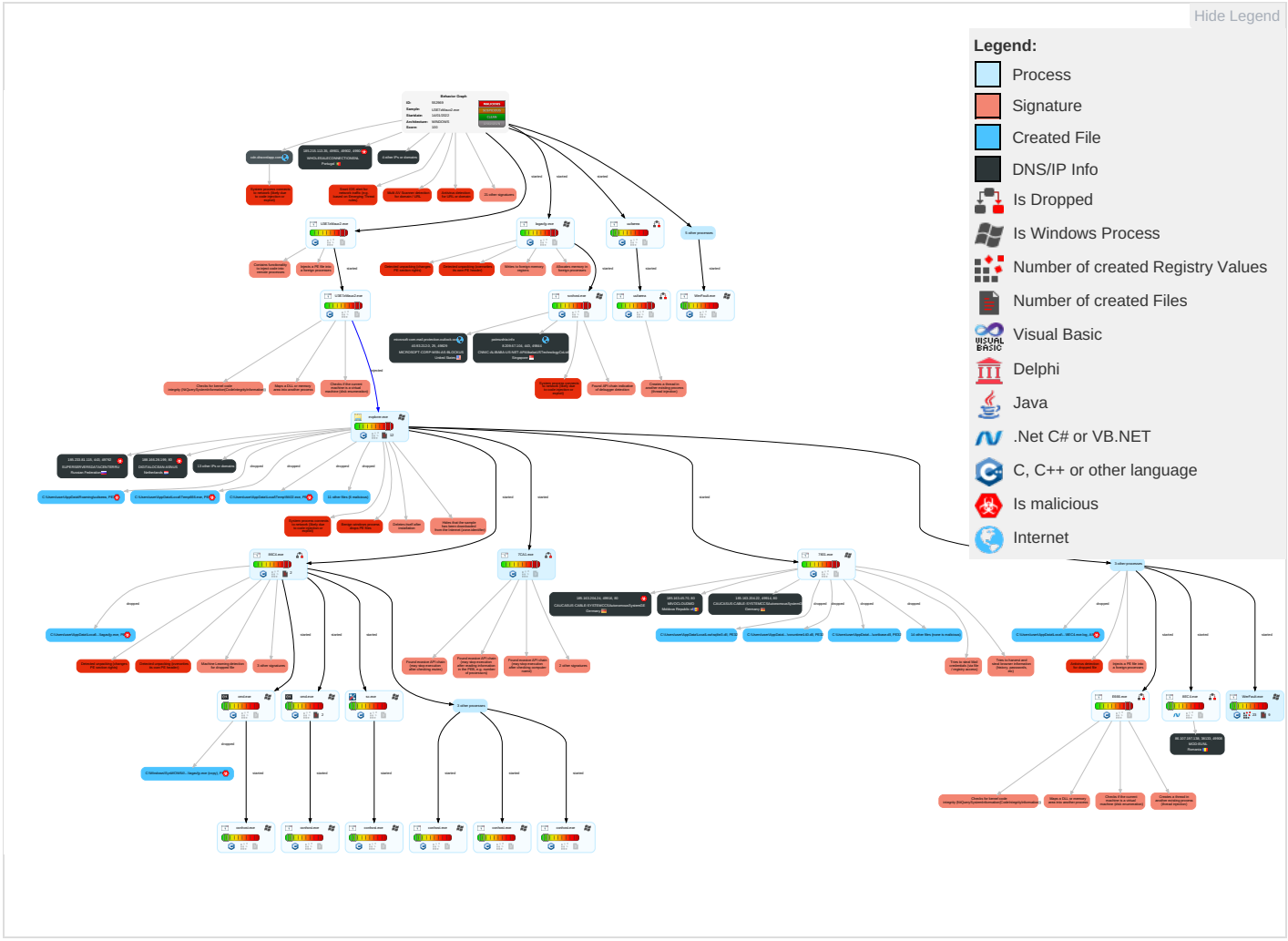
- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- Yara detected Raccoon Stealer
- Yara detected Vidar stealer
- Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Scripting 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 5 4 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypte Channe

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

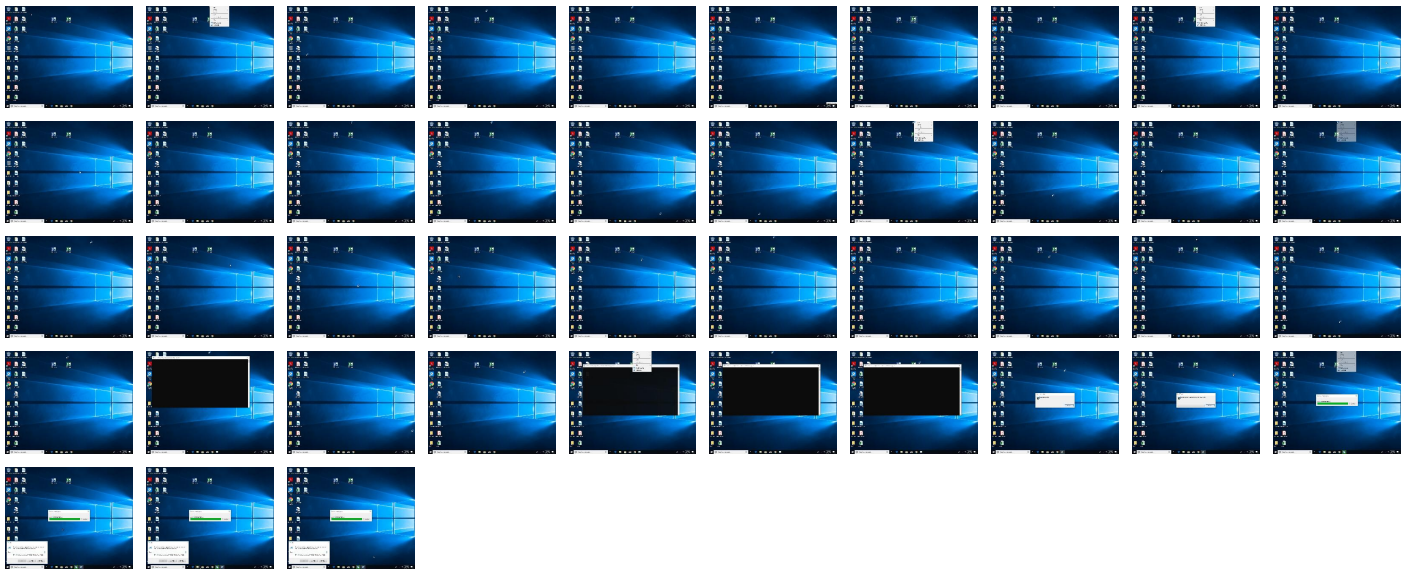
Behavior Graph



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
U3E7zMaux2.exe	41%	Virustotal		Browse
U3E7zMaux2.exe	46%	ReversingLabs	Win32.Trojan.CrypterX	
U3E7zMaux2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\8EC4.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\7801.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8EC4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8ED5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9A02.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\86C4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7CA1.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy.dll	0%	Metadefender		Browse

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
40.0.8EC4.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
43.3.7801.exe.4d60000.2.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
14.0.D984.exe.620e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.2.7801.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1127993		Download File
40.0.8EC4.exe.610000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
21.2.86C4.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.D984.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.8EC4.exe.fa0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.8EC4.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
19.2.E666.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
21.3.86C4.exe.560000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.8EC4.exe.610000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.0.uufaeea.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.U3E7zMaux2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.8EC4.exe.610000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.E666.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.8EC4.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
36.2.lagavljy.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
14.2.D984.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.E666.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.610000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.U3E7zMaux2.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.7CA1.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.uufaeea.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.610000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.0.8EC4.exe.fa0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.1.U3E7zMaux2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.610000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.1.E666.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.3.D984.exe.630000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.E666.exe.5415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.7CA1.exe.570e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.D984.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.610000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.E666.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.U3E7zMaux2.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.8EC4.exe.fa0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
36.3.lagavljy.exe.490000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
36.2.lagavljy.exe.650000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
14.2.D984.exe.620e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.610000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.8EC4.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
12.1.uufaeea.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.8EC4.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
39.2.svchost.exe.320000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
40.0.8EC4.exe.610000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.0.8EC4.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
11.2.uufaeea.4615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.86C4.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
40.0.8EC4.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
0.2.U3E7zMaux2.exe.5315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.uufaeea.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8EC4.exe.610000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.0.D984.exe.620e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.lagavljy.exe.470e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.3.7CA1.exe.590000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.U3E7zMaux2.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.uufaeea.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://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	13%	Virustotal		Browse
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	0%	Avira URL Cloud	safe	
http://185.163.204.24/	4%	Virustotal		Browse
http://185.163.204.24/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	16%	Virustotal		Browse
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/870316542b6e8d6795384509412b3780ad4b1d32	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18Response	0%	URL Reputation	safe	
http://185.215.113.35/d2VxjasuwS/plugins/cred.dll	100%	Avira URL Cloud	malware	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id3Response	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pool-fr.supportxmr.com	91.121.140.167	true	false		high
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	93.189.42.167	true	false		high
patmushta.info	8.209.67.104	true	false		high
cdn.discordapp.com	162.159.130.233	true	false		high
privacy-tools-for-you-780.com	93.189.42.167	true	false		high
microsoft-com.mail.protection.outlook.com	40.93.212.0	true	false		high
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high
data-host-coin-8.com	93.189.42.167	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pool.supportxmr.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.163.204.24/	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://a0621298.xsph.ru/advert.msi	false		high
http://a0621298.xsph.ru/9.exe	false		high
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/45512.exe	false		high
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://a0621298.xsph.ru/File.exe	false		high
http://a0621298.xsph.ru/443.exe	false		high
http://185.163.204.24//l/f/S2zKVH4BZ2GIX1a3NFPE/870316542b6e8d6795384509412b3780ad4b1d32	true	• Avira URL Cloud: safe	unknown
http://185.215.113.35/d2VxjasuwS/plugins/cred.dll	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.163.45.70	unknown	Moldova Republic of		39798	MIVOCLOUDMD	false
185.215.113.35	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
40.93.212.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.21.38.221	goo.su	United States		13335	CLOUDFLARENETUS	false
93.189.42.167	host-data-coin-11.com	Russian Federation		41853	NTCOM-ASRU	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
8.209.67.104	patmushta.info	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
185.7.214.171	unknown	France		42652	DELUNETDE	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false
185.163.204.22	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false
185.163.204.24	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552969
Start date:	14.01.2022
Start time:	00:13:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	U3E7zMaux2.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	50
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.mine.winEXE@60/50@96/18
EGA Information:	• Successful, ratio: 92.3%
HDC Information:	• Successful, ratio: 47.6% (good quality ratio 37.6%) • Quality average: 64% • Quality standard deviation: 39%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:15:09	Task Scheduler	Run new task: Firefox Default Browser Agent 8F76897F18632802 path: C:\Users\user\AppData\Roaming\uufaeea
00:15:24	API Interceptor	1x Sleep call for process: 7CA1.exe modified
00:15:32	API Interceptor	1x Sleep call for process: WerFault.exe modified
00:15:33	API Interceptor	8x Sleep call for process: svchost.exe modified
00:16:06	API Interceptor	4x Sleep call for process: 7801.exe modified
00:16:06	API Interceptor	414x Sleep call for process: mjlooy.exe modified
00:16:08	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
00:16:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
00:16:34	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_e1.exe
00:16:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
00:16:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_e1.exe
00:17:09	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\start ChromeUpdate.lnk

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_D984.exe_bcd76db1fe5d7f46e1bf3aadcd0e64871c556_e6d2f5c0_1ad174c5\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8140048802892536
Encrypted:	false
SSDEEP:	96:z+FmDLAM1kOQoJ7R3V6tpXIQcQec6tycEfcw3m+HbHg/8BRTf3o8Fa9iVfOyWYmq:as3AMR8HQ0lbjlq/u7s9S274ltr
MD5:	A77187FFD082A4C6C4803FF0494824A7
SHA1:	35CF158AFC534025FE186F1FFAA6DC320623566D
SHA-256:	85DFD5A39411BA976F6A87B3D2915C9EECB867A37B34E4D13A0A267F8A1C74B8
SHA-512:	77B9FA28B7AF746B8DE7192F75C5EB76FBD493A3110CE4678A44CA748396B0C0552260B91BE7B3818C27F79EC56E5959CCC227BC0CC9525A73F7F5D6A7CE14E A
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.5.8.9.3.2.2.5.3.4.1.1.6.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.5.8.9.3.3.0.8.4.6.5.5.4.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.c.3.d.4.c.3.-.0.9.a.9.-.4.2.f.9.-.b.a.2.6.-.4.d.c.2.2.4.9.e.8.0.2.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.b.7.c.e.d.c.6.-.6.9.2.2.-.4.1.7.8.-.9.0.4.5.-.0.7.4.3.c.a.4.6.9.8.b.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.D.9.8.4...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.7.c.-.0.0.0.1.-.0.0.1.b.-.a.d.e.6.-.a.a.6.a.d.3.0.8.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.b.f.3.7.4.4.3.4.4.9.b.5.e.c.b.5.4.f.6.4.0.f.a.2.5.6.e.b.5.8.5.0.0.0.0.2.9.0.1.!.0.0.0.0.5.9.9.5.a.e.9.d.0.2.4.7.0.3.6.c.c.6.d.3.e.a.7.4.1.e.7.5.0.4.c.9.1.3.f.1.f.b.7.6.!.D.9.8.4...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.1././.1.2.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E45.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	59464
Entropy (8bit):	3.0415890459619677
Encrypted:	false
SSDEEP:	1536:rHHZvP5xQZDcKdcZRqoPikqjL/15hokyLNh2DqwixlV:rHHZvP5xQZDcKdcZRqoPikqjL/15hZyT
MD5:	BBF079652672E4A164C9D1F6600E9E1B
SHA1:	CB38376B0999BD10686C79A7341B27D7F6BBDAE7
SHA-256:	D506F771465D8185C355E35DFF9D7A75D004D0558E6BBC175E0AAED4E8281EBA
SHA-512:	060E0BA93F1113209B6CF858D67D965B0016D3521E2BC27EBDF7E1DECCC653512C37E3DCEDBC87A9052FED1106FD38102BD338D5FE1BF6FA0C4F36310AE920 D
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E45.tmp.csv	
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER29CF.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6982673798413264
Encrypted:	false
SSDEEP:	96:9GiZYWzRIskYeYAWjqhHX+YEZCLtbimPZrZwhe22zaHjLcO3mlWy3:9jZD45yqnueTaHjLcO3hWy3
MD5:	1E3428F52B7045A77CFD7B0166F40F77
SHA1:	25F5A37E4DBE6DDCB22043B7284BAFCDA1645610
SHA-256:	B011C6766F78C6D95F95404ED5D3BF04BF9875F733ACE46F7641FDE96D27EFF6
SHA-512:	F2C9711D92BAD9C0EFA1B085C08913886B3E39BEAAF2ADE00ABAF4E0092BBDBECD4063EB5E91B89216E802565ED222E93840476860AF62B4CAAAA8C35A4EE43D
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EAC.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54386
Entropy (8bit):	3.0523324327765002
Encrypted:	false
SSDEEP:	1536:/1HBybnA6sgK/x2PRj2nzhmRd1TuOc+3MSi:/1HBybnA6sgK/x2PRj2nzhmRd1TuD+3Y
MD5:	9E2A4C710BF0EF1AB96E0FBC83A94F97
SHA1:	451F103D667B3BC780C511CCC5A517F2E941BDD1
SHA-256:	25A919E83C233B48D3BE7CAFE118537F38C5F1E51868109C002E9ABD7F0DF830
SHA-512:	CAD7424179BF5EA01535947342D5517A6F9A4F5D1BA52E5D61F199145B1D5FF844A0885932C9D91C95DBCBC3C27772D359D15F518BFEA9E5E6774B049E20EC7
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F3.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6960340998589127
Encrypted:	false
SSDEEP:	96:9GiZYWUwJQffYfYkWjqv8HlYEZ+ct6iPPIc+Wwn64k7/aXURiRj6IKx3:9jZDAYWqvhF6P/aXURiRjtKx3
MD5:	7AF93D6F1A0032753A596F52EFCD1423
SHA1:	651104BA14D35EEB3171D1274F415351F61A623B
SHA-256:	39FAFCCC867A221D859CC815615344DE9CFF040779FEB82EE10566D0A96961B3
SHA-512:	C1B52BF2ED2D5EA3627C0BECD3A65121590843EEB6088A7FFFFE8600D7AC9872773A266998C5D61AD9D17871E3D79FA9E3718957813590036C64081B98923A5E
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F3.tmp.txt	
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD6FE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jan 13 23:15:23 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	42152
Entropy (8bit):	2.0055914487492963
Encrypted:	false
SSDEEP:	192:nf+MTOf4LTvbOeh0k3O+Kyx1BQU+A8TxB1NCUVgyT85OtEGVP:oWieeHVLFuG5
MD5:	2A644774142729880A64441FCAE80948
SHA1:	3416A4D49E064E9D094FE99D1EB58DDE93630F17
SHA-256:	82AB2AD8EB0BB51F5B97E9F0FB3875BA4D6C6590267D95664C1F483C055AD5DD
SHA-512:	36B63A7E203E949B9798C0EE669014EE470A24FA2293995CE765DB5704E7D55C43390A2F7EBE4CEDCA9B07AD45894449F8E937E3FF993F9F850E859A208A1528
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....a.....4...v(.....T.....8.....T.....x.....d.....U.....B.....GenuineIn telW.....T.....|.....a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD49.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8392
Entropy (8bit):	3.701438796962995
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNihr6n6YrPSUjgmfORSNQa+pDi89bQssfKwm:RrlsNid6n6YDSUjgmfORS6Q/f8
MD5:	66F461C0EC0330D64B5D27D1E42648D3
SHA1:	F6F499237FE73C3A8B7B53D0EA42F47F6A0E5631
SHA-256:	E7CA29D3A434B2ED3E585CA292AA9A055860117EB9423D0945F16F136301375A
SHA-512:	98F0238DD3C54F793BDB14C75935EC1255A197EB6B608F38F567A3A42FFA75C7A6D935BB22F7E00C1CB18E38539693FE61D2FBC968413E7AA53CE641C265635
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.7.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE103.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.475981505955246
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9XfWSC8BZ8fm8M4JZ8qFcfi+q8vh8R6gxdAOHS3d:uITfQ0OSNoJiiKREAOHS3d
MD5:	867BAA274A448D5C6FE96CE722E9FF4A
SHA1:	353CF987A6D75C60C49B186B123D89FBF891B6EA
SHA-256:	ECBECDDA4BE1B31B50F5B1D2AA05A0CAA15C954398FCD4E2DE76BA658B507E7B
SHA-512:	0CA515EAA2FED710FF3751D4D9EA6404DE814073C3B8C414087A447A64D64A3D3A408F2139B4972692E3AD04CA034A1891962BC35DB1F08942EEEEE3FC548A1
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1341146" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE103.tmp.xml

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\7801.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\7801.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:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.....}{.....}{.....}{.....Rich.....PE..L...C@.\.....!.....b.....0.....~p....@.....p.....h.....0...T.....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T..U..T...U...U...U..T...URich...U.....PE..L...<@.\.....!.....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T.....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....*.....@..@.reloc..<.....D.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&|.J...K&|.J...K&|uK...K&|.J...KRich...K.....PE..L...J@.\.....''!.....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\MapiProxy.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD53D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....''!.....@.....0.....@.....0:.....:..d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+I.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A. {*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....''!.....t.....0.....S....@.....P...P.....(.....`...T..... .....@.....0..D.....text..... ..`.rdata...I...0...n... .....@..@.data.....@....rsrc.....@..@.reloc... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\dI3hX2r.zip	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Reputation:	unknown
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o.....[.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`.M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\.../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.\|k.5...XF.Y..lVVW..C..\|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..\|!.....O....M....>.>.$\.%..L.zF.I...3

C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....@.\.....!.....f.....p.....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\.....!.....f..... .....0.....@.....x..... .....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...l.....@....rsrc...x.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe

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

C:\Users\user\AppData\LocalLow\sG8rM8v\lgpllibs.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F90313272081760 59CD03F53C8C5934C1050897F
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E6765A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l...l..l.....l..~....l..9...l..~....l..~....l..~....l.....l..l....l..l...l..l..l..l..l....l.. l....l..l....l..l..l..l....l..Rich.l.....PE..L...z@.\.....''!.....2.....t.....@.....x.....T..... .....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x.... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\libEGL.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T- ~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....''!.....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. .....''..@..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\nssdbm3.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624

C:\Users\user\AppData\LocalLow\sG8rM8v\nssdbm3.dll	
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwl41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E5E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4..5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L....@.\.....!.....0.....0.....*q....@..... ?.....(@.....`..x.....L.....p.....:.T.....(;..@.....0..X.....text..... ..`.rdata..D....0.. .....@..@.data.....P.....>.....@....rsrc...x....`.....@.....@..@.reloc.....p.....D.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[.$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\.....!..... ... .....%.....0.....p.....`/....@.....5.....p7..x....P..x.....@.....`..$...`1..T.....1..@.....0.....text...2..... ....`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc...x....P.....8.....@..@.reloc..$....`.....<.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\qipcap.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91A9E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W..7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\.....!..... .....`.....r....@.....$..P....@..x.....".....P.. ....T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@.....@..@.reloc.. ....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\softokn3.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC

C:\Users\user\AppData\LocalLow\sG8rM8v\softokn3.dll	
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@.\.....''!.....b.....P.....|....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\ucrtbase.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....l.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\vcruntime140.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39nil35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y.....''!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. ....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\7801.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8EC4.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\8EC4.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\7801.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\7CA1.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	327680
Entropy (8bit):	5.555665914483739
Encrypted:	false
SSDEEP:	3072:QOWFvVSz4X34ToHWGPOeh20XTF2xi69YPUy0ZPv4J3vfrhVggjcGkNIVqI:QO0sMITBsh20XTIp6M5Pv4tX7ITsq
MD5:	3754DB9964B0177B6E905999B6F18FD7
SHA1:	F47B3FCF01C76AF3B174792519D44171413D25AE
SHA-256:	F56B4C870E0B40ED1BF4F1019346F14443BBE8608D6F75ACB92B176D138F74B7
SHA-512:	8BF6439AD6FDC8A8F48F4520FB33A4D69E014BFB70EE3E691DBC611ACA11F1FE2C4B0D3901176455E6D46B8AA661B21C93069E0ABAF78DC93284935E866B29FA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\7CA1.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj._.j`.BjRicha.Bj.....PE..L.....,_..... ...\.....`3.....0....@.....w.....(.....1.....s..@.....0.....text..... ....`.rdata..nY...0...Z...$.....@..@.data.....~.....@....rsrc.....".....@..@.....

C:\Users\user\AppData\Local\Temp\86C4.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	313344
Entropy (8bit):	5.391612297954252
Encrypted:	false
SSDEEP:	3072:3UXmSAohOX34vYHW6gl/rdGolEt1KBCLZISE8LqVpqVggjcGkNIVqI:3UWkWIvxNNkwEt1z9LoS7ITsq
MD5:	B11C5DEFDBA76C2B3EE67EE1B474389D
SHA1:	CCFA42FFB4378AFD337C14514B3EEA9BCF3FC03D
SHA-256:	6380B2CE70ACCB02DE54067A3CDFF27D87E2FAD23F36870C8F90E825E0AE8F2B
SHA-512:	D6683BC03CBF250D17D7BCE5AF562C9D94007669C2321037E644447FE5885B18461BEEAE4B8E848DEBB8DC70B1921A229CDE550ED566D0E13581DCEF2A6B65B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.BjRicha.Bj.....PE..L.....,_..... ..."....`3.....0....@.....@.....7.....(...`.....1.....s..@.....0.....text..... ....`.rdata..nY...0...Z...$.....@..@.data...x.....l...~.....@....rsrc.....`.....@..@.....

C:\Users\user\AppData\Local\Temp\8EC4.exe

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

C:\Users\user\AppData\Local\Temp\8ED5.exe

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

C:\Users\user\AppData\Local\Temp\8ED5.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..U(...(...(...6.).1...6.?.W....l..+...(.....6.8....6.(.)...6.-.)...Rich(..... .....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8..... .....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|..... @..@.reloc..4F...0...H...l.....@..B.....

C:\Users\user\AppData\Local\Temp\9A02.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.848593493266229
Encrypted:	false
SSDEEP:	6144:v5aWbksiNTBiNg5/dEQECtD2YajndnU4aomwStqUJE0ra7yswH:v5atNTMNg5eQX2BdUcDStq+J4bwH
MD5:	6E7430832C1C24C2BF8BE746F2FE583C
SHA1:	158936951114B6A76D665935AD34F6581556FCDF
SHA-256:	972D533E4DF0786799C0E7C914AA6C04870753C10757C5D58CD874B92A7F4739
SHA-512:	79289323C1104F7483FAC9BF2BCAB5B3804C8F2315C8EDEA9D7C83C8B68B64473122F9B38627169D64A35A960A5F74A3364159CA9CB37B0A2B1BA1B41607A8C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2....\.....0....@..... .....lq.....pt..<.....code...~8.....`..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... .....

C:\Users\user\AppData\Local\Temp\ACEF.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3570176
Entropy (8bit):	**7.997630766149595**
Encrypted:	**true**
SSDEEP:	98304:Eyu1PF0IdV1/b4gfya9kofb/4rosp08oUPQH:EjtFp/tfyOTQrosGrUP0
MD5:	DDC599DB99362A7D8642FC19ABE03871
SHA1:	11199134356D8DE145D2EE22AAC37CA8AABA8A0B
SHA-256:	5D94F66FD3315E847213E16E19DFEB008B020798CFFF1334D48AC3344B711F22
SHA-512:	E35DBE56828E804AA78FE436E1717C3A09C416DBE2873FFFC9B44393E7EC2336CE9C544E4D6011C58E7E706819AEABC027AF9A85AA2A2509BDFC39699560ABD
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... T.....b.6.....|IO. .....M..... .....@.....0.....@..... ....&....@.....@.....0.....@.....1...P.....@.....02...../.....@....rsrc.....M.....40.....@....T3QbYgM.....`O.....1..... ..@....adata.....T.....z6.....@.....

C:\Users\user\AppData\Local\Temp\B58B.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\B58B.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\BEB3.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	557664
Entropy (8bit):	7.687250283474463
Encrypted:	false
SSDEEP:	12288:fWxcQhhhhhn8bieAtJlllLtrHWnjkQrK8iBHZkshvesxViA9Og+:fWZhhhhhUATlLtrUbK8oZphveoMA9
MD5:	6ADB5470086099B9169109333FADAB86
SHA1:	87EB7A01E9E54E0A308F8D5EDFD3AF6EBA4DC619
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3EDCD
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$...*..... ...`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...",..

C:\Users\user\AppData\Local\Temp\CC60.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	354816
Entropy (8bit):	7.859676161369944
Encrypted:	false
SSDEEP:	6144:ezBkLL2NTBY2j1gmB0cR8zGnlu4TBJCb2WefmJwJS6jbMXC3DvMk7y:eKyNTa25ccRPlu49JmYt3jbM/
MD5:	DF7952A5FC82DFB2E49AE81B6A1BE135
SHA1:	4F3A8CD939FBE37426EFDA7C88FBD2E49D8F8986
SHA-256:	F04B77C60C896B33ED8FE286DE3341FC3FFD0211A987435475DC7E9D0ABCB0CC
SHA-512:	96A495E5D30E66A236C0AEA19DAEDF95B31F254E457647B6553F2D6CAE117F0A6DA2468550333FBAE3FFA94D0960E2459D2259D3B4C2598EFE49FC03E6C36F1A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....^..... ....@..... .....ta.....4.....hd.,.....code....7.....8..... ..`.text.....P.....<..... ..`.rdata...3... ...4.....@..@.data...$....`.....@.....@....rsrc...4.....R.....@..@..... ....

C:\Users\user\AppData\Local\Temp\D984.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i.hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@..... .....e..P.....2..... Y..@..... .0.....text..... ..`.rdata..D?...0...@..."..... @..@.data...X....p...$...b.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\E666.exe

<table>
<tr><td>Process:</td><td>C:\Windows\explorer.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (GUI) Intel 80386, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>294400</td></tr>
<tr><td>Entropy (8bit):</td><td>5.164848187454738</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:Uv7CHCUfMX34IHHW1UJNZoVkzUl1V9gALVggjcGkNIVqI:UvByIIIW1UJNZo/VV7ITsq</td></tr>
<tr><td>MD5:</td><td>8362E0F91AE3379C73422BBCA7BAC493</td></tr>
<tr><td>SHA1:</td><td>EC761F77BBE9900AED7FFA0A9303DC6801A9EFFB</td></tr>
<tr><td>SHA-256:</td><td>ADFEA20237BE615461C44FEA423D6043FC74BF1C5303EE33FCECD8ACD201291E</td></tr>
<tr><td>SHA-512:</td><td>A509F836E79276E35EE721AEB596214550E410753A122CE254CB3943EDA371713A9FE597717471BC13D884B497D767C393715C4224777F725C4F3EBED9286CAB</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj
._.j`.BjRicha.Bj................PE..L......`................ ....`3.......0....@...........................................................................(.... ..............................1..............................s..@............0<br>..............................text............ .................. ..`.rdata..nY...0...Z...$.............@..@.data...x........"...~.............@....rsrc........ ....@..@...
....
....</td></tr>
</table>

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

<table>
<tr><td>Process:</td><td>C:\Users\user\AppData\Local\Temp\86C4.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (GUI) Intel 80386, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>10543104</td></tr>
<tr><td>Entropy (8bit):</td><td>6.35786276890293</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>49152:xLORQkvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvP:xLORQ</td></tr>
<tr><td>MD5:</td><td>7A36C0AD3083A1519CCE3A67BB377D18</td></tr>
<tr><td>SHA1:</td><td>60416774DCA16DAC538703FC0DBF17E9D5F284DA</td></tr>
<tr><td>SHA-256:</td><td>B968714F907A742E784710A566FC7178C278C074CAA95C5405D40573F35DBEBC</td></tr>
<tr><td>SHA-512:</td><td>D9ACD8081190D480227E1B61FD3C8D7AA85B687AE53AFC90E412CCA158368AC2FEDFE50F62BE25C893F90ED65AE4E22EAFEBBEE352A94680BC8EAC6548170
76</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj
._.j`.BjRicha.Bj................PE..L....._................. ..."......`3.......0....@..........................@.......7..(....`..............................1..............................s..@....<br>........0..............................text............ .................. ..`.rdata..nY...0...Z...$.............@..@.data...x........l...~.............@....rsrc........`......................@..@...
....
....</td></tr>
</table>

C:\Users\user\AppData\Roaming\uufaeea

<table>
<tr><td>Process:</td><td>C:\Windows\explorer.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (GUI) Intel 80386, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>294400</td></tr>
<tr><td>Entropy (8bit):</td><td>5.164848187454738</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:Uv7CHCUfMX34IHHW1UJNZoVkzUl1V9gALVggjcGkNIVqI:UvByIIIW1UJNZo/VV7ITsq</td></tr>
<tr><td>MD5:</td><td>8362E0F91AE3379C73422BBCA7BAC493</td></tr>
<tr><td>SHA1:</td><td>EC761F77BBE9900AED7FFA0A9303DC6801A9EFFB</td></tr>
<tr><td>SHA-256:</td><td>ADFEA20237BE615461C44FEA423D6043FC74BF1C5303EE33FCECD8ACD201291E</td></tr>
<tr><td>SHA-512:</td><td>A509F836E79276E35EE721AEB596214550E410753A122CE254CB3943EDA371713A9FE597717471BC13D884B497D767C393715C4224777F725C4F3EBED9286CAB</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj
._.j`.BjRicha.Bj................PE..L......`................ ....`3.......0....@...........................................................................(.... ..............................1..............................s..@............0<br>..............................text............ .................. ..`.rdata..nY...0...Z...$.............@..@.data...x........"...~.............@....rsrc........ ....@..@...
....
....</td></tr>
</table>

C:\Users\user\AppData\Roaming\uufaeea:Zone.Identifier

<table>
<tr><td>Process:</td><td>C:\Windows\explorer.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>26</td></tr>
</table>

C:\Users\user\AppData\Roaming\uufaeea:Zone.Identifier

Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\SysWOW64\shayesoq\lagavljy.exe (copy)

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10543104
Entropy (8bit):	6.35786276890293
Encrypted:	false
SSDEEP:	49152:xLORQkvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvP:xLORQ
MD5:	7A36C0AD3083A1519CCE3A67BB377D18
SHA1:	60416774DCA16DAC538703FC0DBF17E9D5F284DA
SHA-256:	B968714F907A742E784710A566FC7178C278C074CAA95C5405D40573F35DBEBC
SHA-512:	D9ACD8081190D480227E1B61FD3C8D7AA85B687AE53AFC90E412CCA158368AC2FEDFE50F62BE25C893F90ED65AE4E22EAFEBBEE352A94680BC8EAC6548170 76
Malicious:	**true**
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......%l,9a.Bja.Bja.Bj._.j\|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj ._.j`.BjRicha.Bj................PE..L....._................. ..."......`3.......0....@..........................@.......7..(....`..............................1..............................s..@.... ........0..............................text............ .................. ..`.rdata..nY...0...Z...$.............@..@.data...x........l...~.............@....rsrc........`.....................@..@.. ....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.236050220640177
Encrypted:	false
SSDEEP:	12288:/+hTI+sxo6OWrn9KBr9JQM7W6EX4gsVhIrSXOMOEpll41x/s:GhTI+sxo6Oun9KtK6
MD5:	3A981F75C79C87C66C2E3C993FB7A1C9
SHA1:	E447E1AB82B13A9649001FA037AEDEA394BFFABF
SHA-256:	83B31472AC406793A71F32EC8192392C190E17B1C2D7D34054D38BB83AE42926
SHA-512:	555E753BD31D48649DF9BD994502ACEE6C1DF21BA8233A5474DA1705453C1C6974B9A09794C6E0ED3132DE8F630B82C5351A06A21EDFD16A1E1F1A28C87FC75
Malicious:	false
Reputation:	unknown
Preview:	regfH...H...p.\..,.................. ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4............E.4............E.....5............E.rmtm"{ho.. ....c2.. ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.343015280987901
Encrypted:	false
SSDEEP:	384:fDe5K5pPmKgnVVeeDzeG1NKZtjeT8GVwD35N9M8B:bwKRg/eeDzeoNYtjrGVwDhM8
MD5:	491C1A22271D000AADFD943296472D2C
SHA1:	44B8CF79D15C31CFA752EB16907A33792133108C
SHA-256:	42147A6458BEDAC8A7876F60936731C57A5FB75E195C6A26F5167036C944FC0C
SHA-512:	6568F87D8F49E4AC276EBA782CCE0BE72A99345C65F0EEF985946346559FDBA5A2233BCE24F4898490DFFDD5C915A0E60E26BE8B25FF48B4F635E28521A5F40
Malicious:	false

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Reputation:	unknown
Preview:	regfG...G...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm"{ho..... ....c2HvLE.N.....G.....p..dE.....O..... ..hbin.....p.\..,.....nk,...jo..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...jo..... ....Z.....Root.....lf.....Root....nk ...jo..... .....*.....DeviceCensus..... ...vk.....WritePermissionsCheck.....p...

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iliNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iliNOoHTou7bhBllydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8
SHA-512:	48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090F
Malicious:	false
Reputation:	unknown
Preview:	..A specified value is not valid.....Usage: add rule name=<string>.. dir=in|out.. action=allow|block|bypass.. [program=<program path>].. [service=<service short name>|any].. [description=<string>].. [enable=yes|no (default=yes)].. [profile=public|private|domain|any[,...]].. [localip=any|<IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [localport=0-65535|<port range>[,...]|RPC|RPC-EPMap|IPHTTPS|any (default=any)].. [remoteport=0-65535|<port range>[,...]|any (default=any)].. [protocol=0-255|icmpv4|icmpv6|icmpv4:type,code|icmpv6:type,code|.. tcp|udp|any (default=any)].. [interfacetype=wireless|lan|ras|any].. [rmtcomputergrp=<SDDL string>].. [rmtusrgrp=<SDDL string>].. [edge=yes|deferapp|deferuser|no (default=no)].. [security=authenticate|authenc|authdynenc|authnoencap|

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.164848187454738
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	U3E7zMaux2.exe
File size:	294400
MD5:	8362e0f91ae3379c73422bbca7bac493
SHA1:	ec761f77bbe9900aed7ffa0a9303dc6801a9effb
SHA256:	adfea20237be615461c44fea423d6043fc74bf1c5303ee33fcecd8acd201291e
SHA512:	a509f836e79276e35ee721aeb596214550e410753a122ce254cb3943eda371713a9fe597717471bc13d884b497d767c393715c4224777f725c4f3ebed9286cab
SSDEEP:	3072:Uv7CHCUfMX34IHHW1UJNZoVkzUl1V9gALVggjcGkNIVqI:UvByIIW1UJNZo/VV7ITsq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj._.j`.BjRicha.Bj.....PE..L.....`.....

File Icon

Icon Hash:	acec36b6b694c6e2

Static PE Info

General

Entrypoint:	0x403360

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x60A40BAC [Tue May 18 18:47:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	996fe7decbf39b8813e0892e829e72ad

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11fc6	0x12000	False	0.612263997396	data	6.70078106144	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x13000	0x596e	0x5a00	False	0.457204861111	data	5.66671030744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x19000	0x28278	0x22200	False	0.254006410256	data	2.80829340035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x42000	0xdc88	0xde00	False	0.68262598536	data	6.37784764366	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 00:15:08.165779114 CET	192.168.2.4	8.8.8.8	0x1e78	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:08.615135908 CET	192.168.2.4	8.8.8.8	0x7eb5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:09.073154926 CET	192.168.2.4	8.8.8.8	0xbc1c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:09.557881117 CET	192.168.2.4	8.8.8.8	0x8fba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:09.726715088 CET	192.168.2.4	8.8.8.8	0xf7ef	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:10.185842037 CET	192.168.2.4	8.8.8.8	0xdd6e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:11.804354906 CET	192.168.2.4	8.8.8.8	0x4665	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:12.231695890 CET	192.168.2.4	8.8.8.8	0x96b7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:12.427944899 CET	192.168.2.4	8.8.8.8	0x550f	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:14.237322092 CET	192.168.2.4	8.8.8.8	0xcfa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:14.409171104 CET	192.168.2.4	8.8.8.8	0xa3f6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:14.572695971 CET	192.168.2.4	8.8.8.8	0x786b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:15.171166897 CET	192.168.2.4	8.8.8.8	0xe925	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:15.352641106 CET	192.168.2.4	8.8.8.8	0x9efb	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:17.959861994 CET	192.168.2.4	8.8.8.8	0x644f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:18.142793894 CET	192.168.2.4	8.8.8.8	0x60c7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:18.631000996 CET	192.168.2.4	8.8.8.8	0x9905	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:18.719808102 CET	192.168.2.4	8.8.8.8	0x4acb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:19.382601023 CET	192.168.2.4	8.8.8.8	0xa2b4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:19.582433939 CET	192.168.2.4	8.8.8.8	0x1c8c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:20.064352989 CET	192.168.2.4	8.8.8.8	0xc340	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:20.237083912 CET	192.168.2.4	8.8.8.8	0x2005	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.403347015 CET	192.168.2.4	8.8.8.8	0x5113	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.567151070 CET	192.168.2.4	8.8.8.8	0x9be3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.737056971 CET	192.168.2.4	8.8.8.8	0xdd94	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.901120901 CET	192.168.2.4	8.8.8.8	0x4237	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:24.925096989 CET	192.168.2.4	8.8.8.8	0xac12	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.083369970 CET	192.168.2.4	8.8.8.8	0x65db	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.277966976 CET	192.168.2.4	8.8.8.8	0xd16a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.443576097 CET	192.168.2.4	8.8.8.8	0x2be3	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:27.139034986 CET	192.168.2.4	8.8.8.8	0xe05	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:27.313374996 CET	192.168.2.4	8.8.8.8	0xc920	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:27.475970984 CET	192.168.2.4	8.8.8.8	0x45d7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:39.929191113 CET	192.168.2.4	8.8.8.8	0xd04f	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:42.591212988 CET	192.168.2.4	8.8.8.8	0x6af	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:48.683623075 CET	192.168.2.4	8.8.8.8	0x9e4b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 00:15:48.853013992 CET	192.168.2.4	8.8.8.8	0x56ab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.095482111 CET	192.168.2.4	8.8.8.8	0x22c2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.260747910 CET	192.168.2.4	8.8.8.8	0xafe7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.424179077 CET	192.168.2.4	8.8.8.8	0xda2a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.588679075 CET	192.168.2.4	8.8.8.8	0x9b8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.767848015 CET	192.168.2.4	8.8.8.8	0xe42d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.060847998 CET	192.168.2.4	8.8.8.8	0x1ab9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.231005907 CET	192.168.2.4	8.8.8.8	0xbd50	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.394597054 CET	192.168.2.4	8.8.8.8	0x96b5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.560926914 CET	192.168.2.4	8.8.8.8	0xdc5d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.750709057 CET	192.168.2.4	8.8.8.8	0x9e07	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.917156935 CET	192.168.2.4	8.8.8.8	0xee49	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:51.125756979 CET	192.168.2.4	8.8.8.8	0x2dda	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:55.295429945 CET	192.168.2.4	8.8.8.8	0x10d7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:55.453470945 CET	192.168.2.4	8.8.8.8	0x9efd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:55.614363909 CET	192.168.2.4	8.8.8.8	0x8aed	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.026356936 CET	192.168.2.4	8.8.8.8	0xc7d7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.208574057 CET	192.168.2.4	8.8.8.8	0x4298	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.423022985 CET	192.168.2.4	8.8.8.8	0x29f3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.580876112 CET	192.168.2.4	8.8.8.8	0xc73a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.747313023 CET	192.168.2.4	8.8.8.8	0x31e0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.914865971 CET	192.168.2.4	8.8.8.8	0x9952	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:57.103195906 CET	192.168.2.4	8.8.8.8	0xf2c	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:59.355787039 CET	192.168.2.4	8.8.8.8	0x5dfa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:59.521006107 CET	192.168.2.4	8.8.8.8	0x51da	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:59.755677938 CET	192.168.2.4	8.8.8.8	0x9907	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.044022083 CET	192.168.2.4	8.8.8.8	0x5b1b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.223881960 CET	192.168.2.4	8.8.8.8	0xd305	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.390018940 CET	192.168.2.4	8.8.8.8	0x48a5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.591588974 CET	192.168.2.4	8.8.8.8	0x6886	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.824183941 CET	192.168.2.4	8.8.8.8	0x7dc1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:03.016208887 CET	192.168.2.4	8.8.8.8	0xcdf3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:03.189146996 CET	192.168.2.4	8.8.8.8	0xd2ab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:03.358738899 CET	192.168.2.4	8.8.8.8	0x10e6	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:06.475105047 CET	192.168.2.4	8.8.8.8	0x1d04	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:06.636070967 CET	192.168.2.4	8.8.8.8	0x47a2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:06.801625967 CET	192.168.2.4	8.8.8.8	0xd460	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 00:16:08.337502003 CET	192.168.2.4	8.8.8.8	0xd5ff	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:08.555936098 CET	192.168.2.4	8.8.8.8	0xb8a9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:08.839423895 CET	192.168.2.4	8.8.8.8	0xa9f5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:09.013679981 CET	192.168.2.4	8.8.8.8	0xc4ec	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:11.631227970 CET	192.168.2.4	8.8.8.8	0xb620	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:12.475086927 CET	192.168.2.4	8.8.8.8	0x824c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:12.673590899 CET	192.168.2.4	8.8.8.8	0xce37	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:13.988838911 CET	192.168.2.4	8.8.8.8	0xe413	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:14.287476063 CET	192.168.2.4	8.8.8.8	0xb20f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:14.658121109 CET	192.168.2.4	8.8.8.8	0x165	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:18.495066881 CET	192.168.2.4	8.8.8.8	0x185	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:18.692121983 CET	192.168.2.4	8.8.8.8	0x7768	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:21.204607964 CET	192.168.2.4	8.8.8.8	0xcd02	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:21.791950941 CET	192.168.2.4	8.8.8.8	0x670c	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:22.426749945 CET	192.168.2.4	8.8.8.8	0xd3fe	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.147851944 CET	192.168.2.4	8.8.8.8	0x3019	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.197062969 CET	192.168.2.4	8.8.8.8	0xdbf8	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.203850031 CET	192.168.2.4	8.8.8.8	0x8de8	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.748819113 CET	192.168.2.4	8.8.8.8	0xa426	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:31.828166962 CET	192.168.2.4	8.8.8.8	0x8a9	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:33.387123108 CET	192.168.2.4	8.8.8.8	0x22e	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:51.736057043 CET	192.168.2.4	8.8.8.8	0xdb81	Standard query (0)	pool.supportxmr.com	A (IP address)	IN (0x0001)
Jan 14, 2022 00:17:13.778686047 CET	192.168.2.4	8.8.8.8	0x5e1	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 00:15:08.466722965 CET	8.8.8.8	192.168.2.4	0x1e78	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:08.926810026 CET	8.8.8.8	192.168.2.4	0x7eb5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:09.401787996 CET	8.8.8.8	192.168.2.4	0xbc1c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:09.575335979 CET	8.8.8.8	192.168.2.4	0x8fba	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:10.039287090 CET	8.8.8.8	192.168.2.4	0xf7ef	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:10.473891973 CET	8.8.8.8	192.168.2.4	0xdd6e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:12.090094090 CET	8.8.8.8	192.168.2.4	0x4665	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:12.250962019 CET	8.8.8.8	192.168.2.4	0x96b7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 00:15:12.447144985 CET	8.8.8.8	192.168.2.4	0x550f	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:14.257040977 CET	8.8.8.8	192.168.2.4	0xcfa	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:14.427084923 CET	8.8.8.8	192.168.2.4	0xa3f6	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:14.904640913 CET	8.8.8.8	192.168.2.4	0x786b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:15.190542936 CET	8.8.8.8	192.168.2.4	0xe925	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:15.666140079 CET	8.8.8.8	192.168.2.4	0x9efb	No error (0)	privacy-tools-for-you-780.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:17.977097034 CET	8.8.8.8	192.168.2.4	0x644f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:18.161992073 CET	8.8.8.8	192.168.2.4	0x60c7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:18.650316000 CET	8.8.8.8	192.168.2.4	0x9905	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:18.739072084 CET	8.8.8.8	192.168.2.4	0x4acb	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:19.402050972 CET	8.8.8.8	192.168.2.4	0xa2b4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:19.897456884 CET	8.8.8.8	192.168.2.4	0x1c8c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:20.083414078 CET	8.8.8.8	192.168.2.4	0xc340	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:20.562536001 CET	8.8.8.8	192.168.2.4	0x2005	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.423297882 CET	8.8.8.8	192.168.2.4	0x5113	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.586868048 CET	8.8.8.8	192.168.2.4	0x9be3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.754504919 CET	8.8.8.8	192.168.2.4	0xdd94	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:22.920911074 CET	8.8.8.8	192.168.2.4	0x4237	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:24.943259954 CET	8.8.8.8	192.168.2.4	0xac12	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.101136923 CET	8.8.8.8	192.168.2.4	0x65db	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.297411919 CET	8.8.8.8	192.168.2.4	0xd16a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.463532925 CET	8.8.8.8	192.168.2.4	0x2be3	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.463532925 CET	8.8.8.8	192.168.2.4	0x2be3	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.463532925 CET	8.8.8.8	192.168.2.4	0x2be3	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.463532925 CET	8.8.8.8	192.168.2.4	0x2be3	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:25.463532925 CET	8.8.8.8	192.168.2.4	0x2be3	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 00:15:27.160053968 CET	8.8.8.8	192.168.2.4	0xe05	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:27.333893061 CET	8.8.8.8	192.168.2.4	0xc920	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:27.495369911 CET	8.8.8.8	192.168.2.4	0x45d7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:39.956341028 CET	8.8.8.8	192.168.2.4	0xd04f	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:39.956341028 CET	8.8.8.8	192.168.2.4	0xd04f	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:39.956341028 CET	8.8.8.8	192.168.2.4	0xd04f	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:39.956341028 CET	8.8.8.8	192.168.2.4	0xd04f	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:39.956341028 CET	8.8.8.8	192.168.2.4	0xd04f	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:42.897193909 CET	8.8.8.8	192.168.2.4	0x6af	No error (0)	patmushta.info		8.209.67.104	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:48.703727007 CET	8.8.8.8	192.168.2.4	0x9e4b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:48.873003960 CET	8.8.8.8	192.168.2.4	0x56ab	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.115181923 CET	8.8.8.8	192.168.2.4	0x22c2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.279900074 CET	8.8.8.8	192.168.2.4	0xafe7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.443753004 CET	8.8.8.8	192.168.2.4	0xda2a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.610033989 CET	8.8.8.8	192.168.2.4	0x9b8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:49.790723085 CET	8.8.8.8	192.168.2.4	0xe42d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.081588984 CET	8.8.8.8	192.168.2.4	0x1ab9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.252104998 CET	8.8.8.8	192.168.2.4	0xbd50	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.413388014 CET	8.8.8.8	192.168.2.4	0x96b5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.582348108 CET	8.8.8.8	192.168.2.4	0xdc5d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.770617008 CET	8.8.8.8	192.168.2.4	0x9e07	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:50.936686993 CET	8.8.8.8	192.168.2.4	0xee49	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:51.145322084 CET	8.8.8.8	192.168.2.4	0x2dda	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:55.314858913 CET	8.8.8.8	192.168.2.4	0x10d7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 00:15:55.472961903 CET	8.8.8.8	192.168.2.4	0x9efd	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:55.635926008 CET	8.8.8.8	192.168.2.4	0x8aed	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:55.635926008 CET	8.8.8.8	192.168.2.4	0x8aed	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.045312881 CET	8.8.8.8	192.168.2.4	0xc7d7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.225570917 CET	8.8.8.8	192.168.2.4	0x4298	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.442231894 CET	8.8.8.8	192.168.2.4	0x29f3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.600402117 CET	8.8.8.8	192.168.2.4	0xc73a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.764776945 CET	8.8.8.8	192.168.2.4	0x31e0	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:56.934189081 CET	8.8.8.8	192.168.2.4	0x9952	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:57.123147011 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:59.375186920 CET	8.8.8.8	192.168.2.4	0x5dfa	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:59.541596889 CET	8.8.8.8	192.168.2.4	0x51da	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:15:59.774959087 CET	8.8.8.8	192.168.2.4	0x9907	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.064773083 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.243716002 CET	8.8.8.8	192.168.2.4	0xd305	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.410080910 CET	8.8.8.8	192.168.2.4	0x48a5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.609232903 CET	8.8.8.8	192.168.2.4	0x6886	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:02.845551968 CET	8.8.8.8	192.168.2.4	0x7dc1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:03.037575960 CET	8.8.8.8	192.168.2.4	0xcdf3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:03.209789038 CET	8.8.8.8	192.168.2.4	0xd2ab	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:03.380450010 CET	8.8.8.8	192.168.2.4	0x10e6	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:06.494786978 CET	8.8.8.8	192.168.2.4	0x1d04	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:06.655414104 CET	8.8.8.8	192.168.2.4	0x47a2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:06.821372032 CET	8.8.8.8	192.168.2.4	0xd460	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:08.358143091 CET	8.8.8.8	192.168.2.4	0xd5ff	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:08.573673010 CET	8.8.8.8	192.168.2.4	0xb8a9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 00:16:08.859005928 CET	8.8.8.8	192.168.2.4	0xa9f5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:09.300795078 CET	8.8.8.8	192.168.2.4	0xc4ec	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:11.650517941 CET	8.8.8.8	192.168.2.4	0xb620	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:12.494309902 CET	8.8.8.8	192.168.2.4	0x824c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:12.692929983 CET	8.8.8.8	192.168.2.4	0xce37	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:14.010508060 CET	8.8.8.8	192.168.2.4	0xe413	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:14.304579020 CET	8.8.8.8	192.168.2.4	0xb20f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:14.678030968 CET	8.8.8.8	192.168.2.4	0x165	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:18.515554905 CET	8.8.8.8	192.168.2.4	0x185	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:18.712820053 CET	8.8.8.8	192.168.2.4	0x7768	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:21.225965977 CET	8.8.8.8	192.168.2.4	0xcd02	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:21.818962097 CET	8.8.8.8	192.168.2.4	0x670c	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:22.446170092 CET	8.8.8.8	192.168.2.4	0xd3fe	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.220061064 CET	8.8.8.8	192.168.2.4	0xdbf8	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.220061064 CET	8.8.8.8	192.168.2.4	0xdbf8	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.220061064 CET	8.8.8.8	192.168.2.4	0xdbf8	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.220061064 CET	8.8.8.8	192.168.2.4	0xdbf8	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.220061064 CET	8.8.8.8	192.168.2.4	0xdbf8	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.226542950 CET	8.8.8.8	192.168.2.4	0x8de8	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.226542950 CET	8.8.8.8	192.168.2.4	0x8de8	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.226542950 CET	8.8.8.8	192.168.2.4	0x8de8	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.226542950 CET	8.8.8.8	192.168.2.4	0x8de8	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.226542950 CET	8.8.8.8	192.168.2.4	0x8de8	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.253052950 CET	8.8.8.8	192.168.2.4	0x3019	No error (0)	patmushta.info		8.209.67.104	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:23.767479897 CET	8.8.8.8	192.168.2.4	0xa426	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:31.850064993 CET	8.8.8.8	192.168.2.4	0x8a9	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 00:16:31.850064993 CET	8.8.8.8	192.168.2.4	0x8a9	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:31.850064993 CET	8.8.8.8	192.168.2.4	0x8a9	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:31.850064993 CET	8.8.8.8	192.168.2.4	0x8a9	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:31.850064993 CET	8.8.8.8	192.168.2.4	0x8a9	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:33.406083107 CET	8.8.8.8	192.168.2.4	0x22e	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:33.406083107 CET	8.8.8.8	192.168.2.4	0x22e	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:33.406083107 CET	8.8.8.8	192.168.2.4	0x22e	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:33.406083107 CET	8.8.8.8	192.168.2.4	0x22e	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:33.406083107 CET	8.8.8.8	192.168.2.4	0x22e	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:51.757019043 CET	8.8.8.8	192.168.2.4	0xdb81	No error (0)	pool.supportxmr.com	pool-fr.supportxmr.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 00:16:51.757019043 CET	8.8.8.8	192.168.2.4	0xdb81	No error (0)	pool-fr.supportxmr.com		91.121.140.167	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:51.757019043 CET	8.8.8.8	192.168.2.4	0xdb81	No error (0)	pool-fr.supportxmr.com		149.202.83.171	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:51.757019043 CET	8.8.8.8	192.168.2.4	0xdb81	No error (0)	pool-fr.supportxmr.com		37.187.95.110	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:51.757019043 CET	8.8.8.8	192.168.2.4	0xdb81	No error (0)	pool-fr.supportxmr.com		94.23.23.52	A (IP address)	IN (0x0001)
Jan 14, 2022 00:16:51.757019043 CET	8.8.8.8	192.168.2.4	0xdb81	No error (0)	pool-fr.supportxmr.com		94.23.247.226	A (IP address)	IN (0x0001)
Jan 14, 2022 00:17:13.884191990 CET	8.8.8.8	192.168.2.4	0x5e1	No error (0)	patmushta.info		8.209.67.104	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- lkoyuevdx.net
  - host-data-coin-11.com
- secxfi.net
- vuafh.org
- psxblf.com
- dsdofcnp.com
- obbsps.com
- ttkljrkl.com
- fvjjmgnhpi.org

- data-host-coin-8.com
- giblvuodn.org
- unjilfapdr.net
- bnrfjahkht.net
- epntadtm.net
- privacy-tools-for-you-780.com
- yevvbkvx.org
- psfbiu.com
- unicupload.top
- phnfrhmjav.com
- etxdniy.com
- tlotvuqfn.net
- bjfnimnu.org
- mkbyakqqj.com
- reeitd.net
- vnmaltjgi.net
- fmegeducg.org
- 185.7.214.171:8080
- ghiodndfpo.com
- njpun.net
- rmhfrtkprf.net
- ynkqvnpya.com
- pnfnlpnysf.com
- mosjbuj.net
- oytdv.net
- rljjkyrr.net
- jpqcmep.com
- fosbja.com
- rcjgja.net
- yivbbwxtct.com

- dqwogmqhb.com
- cvhsbw.com
- oyghbp.com
- yuvwrs.com
- xkujdf.net
- fyyanes.com
- tyjpjf.org
- rsxrkuta.org
- jlgqjcjkdy.net
- avcxisfo.org
- mvsed.org
- pgctyuwy.net
- surulybuu.org
- thylpwqt.org
- rhglrb.org
- dbxsgfe.org
- a0621298.xsph.ru
- aoavvcteey.com
- tqnyuoui.net
- nqlstnrw.org
- cbwqss.org
- toosx.com
- dokqsat.net
- pipoxpya.com
- wbrirc.com
- 185.215.113.35
- dwskrgjp.com
- pwahu.net
- xnfmckfat.org
- 185.163.204.22

- htagjvn.org
- 185.163.204.24
- nadbxcytci.net
- wvnyptv.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: U3E7zMaux2.exe PID: 6688 Parent PID: 3512

General

Start time:	00:14:26
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\U3E7zMaux2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\U3E7zMaux2.exe"
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	8362E0F91AE3379C73422BBCA7BAC493
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: U3E7zMaux2.exe PID: 6728 Parent PID: 6688

General

Start time:	00:14:28
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\U3E7zMaux2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\U3E7zMaux2.exe"
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	8362E0F91AE3379C73422BBCA7BAC493
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: 00000001.00000002.713149753.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.713456716.0000000002301000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 6728

General

Start time:	00:14:35
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000007.00000000.700489251.00000000044E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 2480 Parent PID: 568

General

Start time:	00:14:36
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6140 Parent PID: 568

General

Start time:	00:14:56
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: uufaeea PID: 2804 Parent PID: 968

General

Start time:	00:15:09
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\uufaeea
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\uufaeea
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	8362E0F91AE3379C73422BBCA7BAC493
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: uufaeea PID: 6944 Parent PID: 2804

General

Start time:	00:15:12
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\uufaeea
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\uufaeea
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	8362E0F91AE3379C73422BBCA7BAC493
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: 0000000C.00000002.766896131.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000C.00000002.766831607.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 5444 Parent PID: 568

General

Start time:	00:15:12
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: D984.exe PID: 5756 Parent PID: 3424

General

Start time:	00:15:12
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\D984.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D984.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 5680 Parent PID: 568

General

Start time:	00:15:15
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5788 Parent PID: 5680

General

Start time:	00:15:16
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 5756 -ip 5756
Imagebase:	0x1240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: E666.exe PID: 4780 Parent PID: 3424

General

Start time:	00:15:16
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E666.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E666.exe
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	8362E0F91AE3379C73422BBCA7BAC493
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 6712 Parent PID: 5756

General

Start time:	00:15:19
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5756 -s 520
Imagebase:	0x1240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: E666.exe PID: 4388 Parent PID: 4780

General

Start time:	00:15:20
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E666.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E666.exe
Imagebase:	0x400000
File size:	294400 bytes
MD5 hash:	8362E0F91AE3379C73422BBCA7BAC493
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: 00000013.00000002.784101177.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.783879616.0000000000530000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 7CA1.exe PID: 5352 Parent PID: 3424

General

Start time:	00:15:21
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7CA1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\7CA1.exe
Imagebase:	0x400000
File size:	327680 bytes
MD5 hash:	3754DB9964B0177B6E905999B6F18FD7
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: 00000014.00000002.775878501.0000000000622000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000014.00000002.775878501.0000000000622000.00000004.00000020.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 86C4.exe PID: 1368 Parent PID: 3424

General

Start time:	00:15:23
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\86C4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\86C4.exe

Imagebase:	0x400000
File size:	313344 bytes
MD5 hash:	B11C5DEFDBA76C2B3EE67EE1B474389D
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: 00000015.00000002.797378726.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000015.00000003.780018628.0000000000560000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000015.00000002.797152271.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 8EC4.exe PID: 6024 Parent PID: 3424

General

Start time:	00:15:25
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8EC4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8EC4.exe
Imagebase:	0xfa0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000002.828481056.0000000004401000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 5208 Parent PID: 1368

General

Start time:	00:15:28
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\shayesoq\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 6000 Parent PID: 5208

General

Start time:	00:15:28
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6392 Parent PID: 1368

General

Start time:	00:15:29
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\lagavljy.exe" C:\Windows\SysWOW64\shayesoq\
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6916 Parent PID: 6392

General

Start time:	00:15:29
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: sc.exe PID: 3496 Parent PID: 1368

General

Start time:	00:15:30
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create shayesoq binPath= "C:\Windows\SysWOW64\shayesoq\lagavljy.exe /d\"C:\Users\user\AppData\Local\Temp\86C4.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x150000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4936 Parent PID: 568

General

Start time:	00:15:30
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1496 Parent PID: 3496

General

Start time:	00:15:30
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 1716 Parent PID: 1368

General

Start time:	00:15:31
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description shayesoq "wifi internet conection
Imagebase:	0x150000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5416 Parent PID: 1716

General

Start time:	00:15:32
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 4728 Parent PID: 1368

General

Start time:	00:15:32
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start shayesoq
Imagebase:	0x150000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5236 Parent PID: 4728

General

Start time:	00:15:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: lagavljy.exe PID: 4544 Parent PID: 568

General

Start time:	00:15:33
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\shayesoq\lagavljy.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\shayesoq\lagavljy.exe /d"C:\Users\user\AppData\Local\Temp\86C4.exe"
Imagebase:	0x400000
File size:	10543104 bytes
MD5 hash:	7A36C0AD3083A1519CCE3A67BB377D18
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: 00000024.00000002.806559980.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000024.00000002.807575070.0000000000650000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000024.00000002.807182784.0000000000470000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000024.00000003.803811514.0000000000490000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: netsh.exe PID: 5988 Parent PID: 1368

General

Start time:	00:15:33
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5560 Parent PID: 5988

General

Start time:	00:15:34
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5940 Parent PID: 4544

General

Start time:	00:15:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xfc0000
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: 00000027.00000002.922686278.0000000000320000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 8EC4.exe PID: 6240 Parent PID: 6024

General

Start time:	00:15:40
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8EC4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8EC4.exe
Imagebase:	0x610000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000002.923336327.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.820733997.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.819245011.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.820186557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.819693926.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 7801.exe PID: 7032 Parent PID: 3424

General

Start time:	00:15:51
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7801.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\7801.exe
Imagebase:	0x400000
File size:	905216 bytes
MD5 hash:	852D86F5BC34BF4AF7FA89C60569DF13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000002B.00000003.856737411.0000000004E00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000002B.00000002.922477314.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis