ID: 552945
Sample Name: 0Cjy7Lkv1A.exe
Cookbook: default.jbs
Time: 23:27:23
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

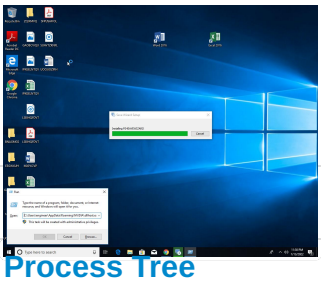
Windows Analysis Report 0Cjy7Lkv1A.exe

Overview

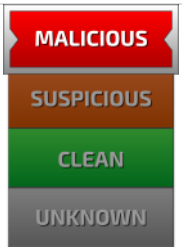
General Information

Sample Name:	0Cjy7Lkv1A.exe
Analysis ID:	552945
MD5:	eb023c854d3c8a..
SHA1:	699eb8e25fcd583.
SHA256:	b602afd3f94c582..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



Amadey Raccoon RedLine SmokeLoader Tofsee Vidar

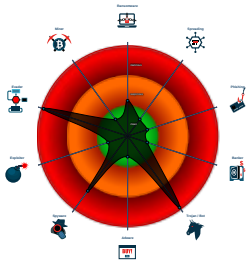
Score: 100
Range: 0 - 100

Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- 0Cjy7Lkv1A.exe (PID: 4440 cmdline: "C:\Users\user\Desktop\0Cjy7Lkv1A.exe" MD5: EB023C854D3C8A24589E9294FD5D346E)
  - 0Cjy7Lkv1A.exe (PID: 6452 cmdline: "C:\Users\user\Desktop\0Cjy7Lkv1A.exe" MD5: EB023C854D3C8A24589E9294FD5D346E)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 60C2.exe (PID: 6188 cmdline: C:\Users\user\AppData\Local\Temp\60C2.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 2784 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6188 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 7063.exe (PID: 7052 cmdline: C:\Users\user\AppData\Local\Temp\7063.exe MD5: 3754DB9964B0177B6E905999B6F18FD7)
      - A8FB.exe (PID: 4692 cmdline: C:\Users\user\AppData\Local\Temp\A8FB.exe MD5: 2650E6FA017E57264E55CB0078639A13)
        - cmd.exe (PID: 7092 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\uuqefjyt\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 3496 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\szdcdkt.exe" C:\Windows\SysWOW64\uuqefjyt\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 3220 cmdline: C:\Windows\System32\sc.exe" create uuqefjyt binPath= "C:\Windows\SysWOW64\uuqefjyt\szdcdkt.exe /d\"C:\Users\user\AppData\Local\Temp\A8FB.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5324 cmdline: C:\Windows\System32\sc.exe" description uuqefjyt "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2192 cmdline: "C:\Windows\System32\sc.exe" start uuqefjyt MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 4388 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: 4820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - B3BA.exe (PID: 6964 cmdline: C:\Users\user\AppData\Local\Temp\B3BA.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - B3BA.exe (PID: 4264 cmdline: C:\Users\user\AppData\Local\Temp\B3BA.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - B3BA.exe (PID: 1756 cmdline: C:\Users\user\AppData\Local\Temp\B3BA.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - 1BCC.exe (PID: 6684 cmdline: C:\Users\user\AppData\Local\Temp\1BCC.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - 382E.exe (PID: 6140 cmdline: C:\Users\user\AppData\Local\Temp\382E.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
      - 5126.exe (PID: 6132 cmdline: C:\Users\user\AppData\Local\Temp\5126.exe MD5: 6E7430832C1C24C2BF8BE746F2FE583C)
        - conhost.exe (PID: 5432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6492 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1520 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5036 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- ujhcrda (PID: 5724 cmdline: C:\Users\user\AppData\Roaming\ujhcrda MD5: EB023C854D3C8A24589E9294FD5D346E)
  - ujhcrda (PID: 5416 cmdline: C:\Users\user\AppData\Roaming\ujhcrda MD5: EB023C854D3C8A24589E9294FD5D346E)
- svchost.exe (PID: 4192 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5668 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6188 -ip 6188 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 3252 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- szdcdkt.exe (PID: 2972 cmdline: C:\Windows\SysWOW64\uuqefjyt\szdcdkt.exe /d"C:\Users\user\AppData\Local\Temp\A8FB.exe" MD5: F23C1D7C6806E4BFAA8ABAD7CCC77AC1)
  - svchost.exe (PID: 6780 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 1624 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- ujhcrda (PID: 6104 cmdline: C:\Users\user\AppData\Roaming\ujhcrda MD5: EB023C854D3C8A24589E9294FD5D346E)
- **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
00000024.00000003.507342269.000000000690000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000011.00000002.474690379.000000000571000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000011.00000002.474690379.000000000571000.00000004.00000020.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Source	Rule	Description	Author	Strings
0000002F.00000003.564856564.00000000006B0000.00000004.00000001.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0000002C.00000002.748388079.000000000511 4000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.0Cjy7Lkv1A.exe.4615a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
36.2.szdcdkt.exe.400000.0.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
39.2.svchost.exe.a50000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
1.2.0Cjy7Lkv1A.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
13.1.ujhcrda.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 26 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 dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Yara detected BatToExe compiled binary

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

Persistence and Installation Behavior:

Yara detected Amadey bot

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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

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

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

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Raccoon Stealer

Yara detected Vidar stealer

Yara detected Tofsee

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Raccoon Stealer

Yara detected Vidar stealer

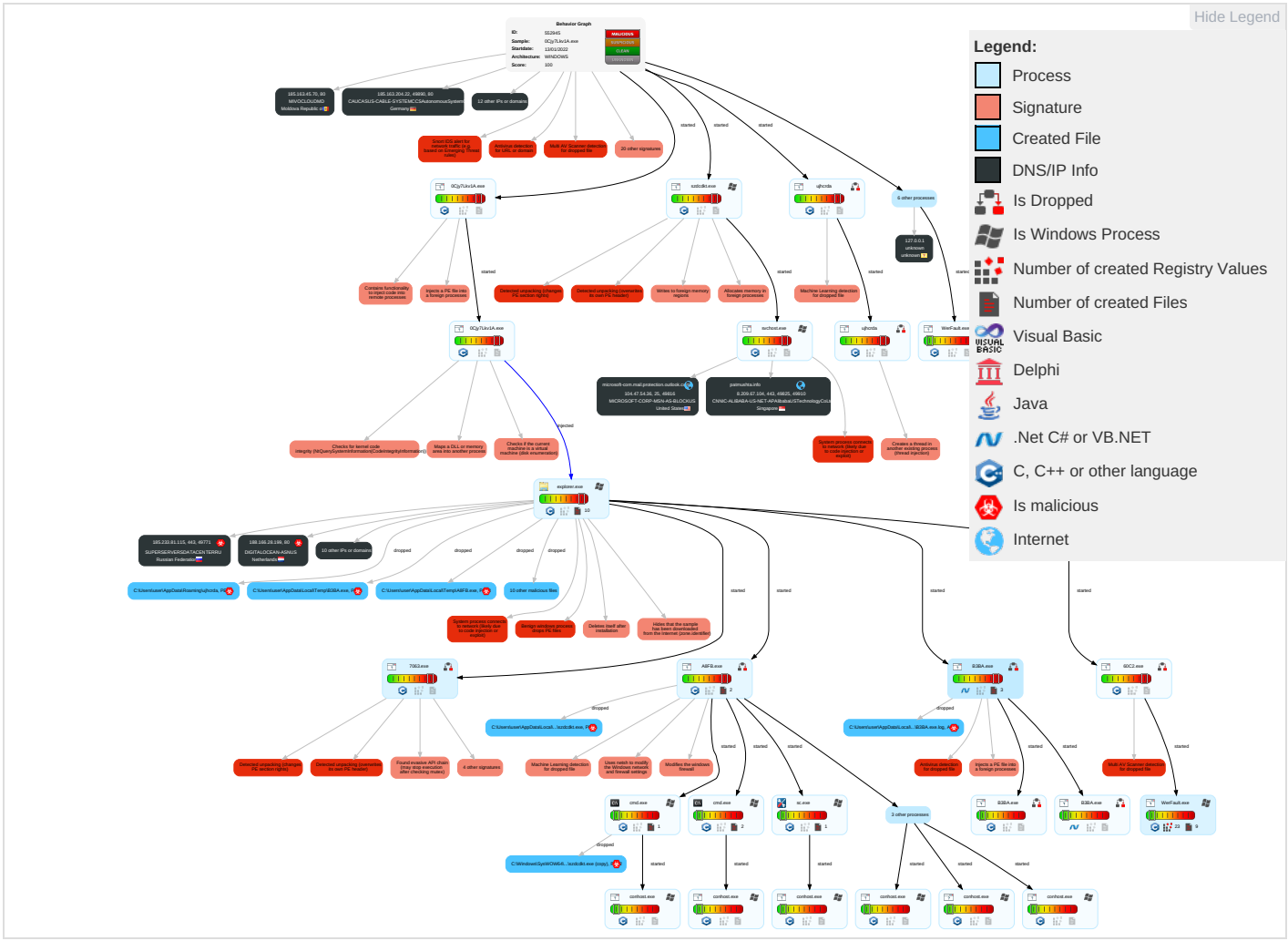
Yara detected Tofsee

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 4 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 4 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Proto
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 3	Keylogging	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

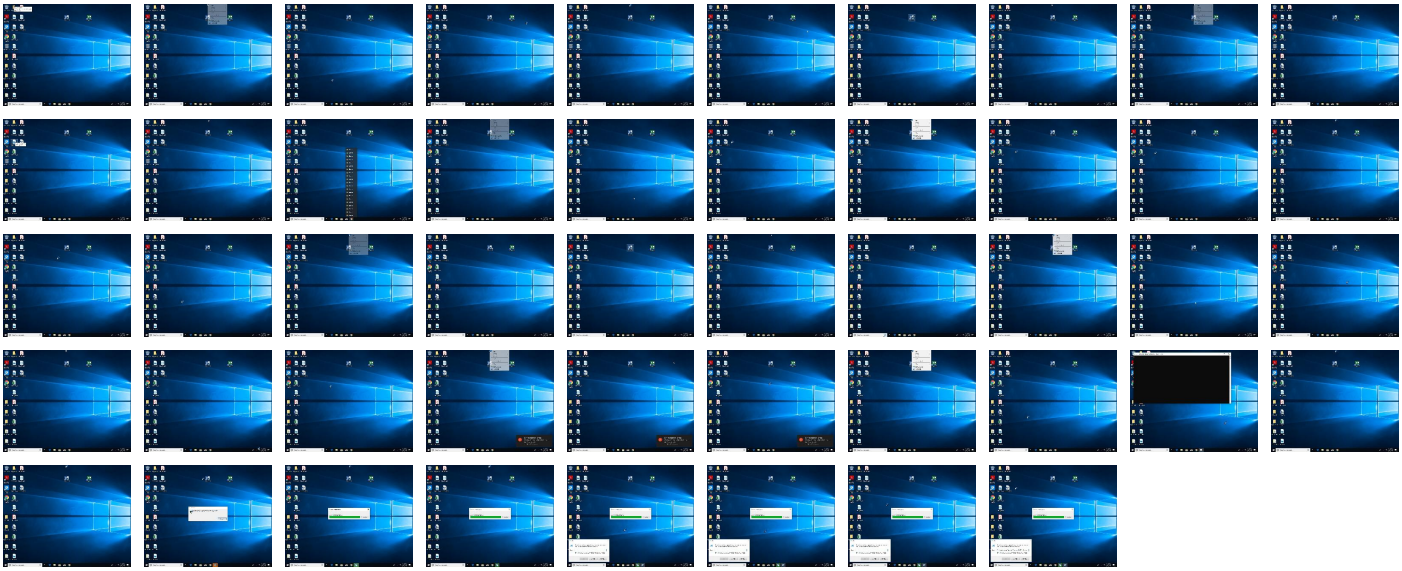
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0Cjy7Lkv1A.exe	38%	Virustotal		Browse
0Cjy7Lkv1A.exe	54%	ReversingLabs	Win32.Trojan.DllCheck	
0Cjy7Lkv1A.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\B3BA.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\8008.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A8FB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9874.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7063.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\382E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\szdcdkt.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B3BA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\60C2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8B25.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6674.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5126.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1BCC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ujhcrda	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1BCC.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\382E.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\382E.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Local\Temp\60C2.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\60C2.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\6674.exe	46%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\8008.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.3.7063.exe.4a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.60C2.exe.2080e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.szdcdkt.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
42.0.B3BA.exe.9b0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.3.60C2.exe.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.ujhcrda.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.2.B3BA.exe.250000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.0.B3BA.exe.370000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
36.2.szdcdkt.exe.670e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.0Cjy7Lkv1A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.1.ujhcrda.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.B3BA.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
1.0.0Cjy7Lkv1A.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.B3BA.exe.9b0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.0.B3BA.exe.370000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.0.B3BA.exe.370000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
42.0.B3BA.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
42.0.B3BA.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
20.2.B3BA.exe.370000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
42.0.B3BA.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
42.0.B3BA.exe.9b0000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.0.60C2.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.7063.exe.480e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
42.0.B3BA.exe.9b0000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
42.0.B3BA.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
42.0.B3BA.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
42.0.B3BA.exe.9b0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
41.0.B3BA.exe.250000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
13.0.ujhcrda.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.B3BA.exe.370000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
13.0.ujhcrda.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
36.3.szdcdkt.exe.690000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.ujhcrda.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.60C2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.B3BA.exe.9b0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
36.2.szdcdkt.exe.eb0000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
14.0.60C2.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.60C2.exe.2080e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.B3BA.exe.9b0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.2.A8FB.exe.550e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.0.B3BA.exe.250000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
39.2.svchost.exe.a50000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
41.0.B3BA.exe.250000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.0Cjy7Lkv1A.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.0.B3BA.exe.9b0000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.2.ujhcrda.5315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.0Cjy7Lkv1A.exe.4615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.B3BA.exe.250000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
42.0.B3BA.exe.9b0000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.0.60C2.exe.2080e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.3.A8FB.exe.570000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
42.0.B3BA.exe.9b0000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.1.0Cjy7Lkv1A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.0Cjy7Lkv1A.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.7063.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.A8FB.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.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://185.163.204.24/	4%	Virustotal		Browse
http://185.163.204.24/	0%	Avira URL Cloud	safe	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/4457553c06dee2e98e4f451cad0abfa16d7760a4	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/e946ea03b0a56043b0189e637403106a5b3aad8e	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18Response	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id3Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3-w.us-east-1.amazonaws.com	54.231.194.41	true	false		high
bitbucket.org	104.192.141.1	true	false		high
pool-fr.supportxmr.com	149.202.83.171	true	false		high
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	93.189.42.167	true	false		high
patmushta.info	8.209.67.104	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
microsoft-com.mail.protection.outlook.com	104.47.54.36	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
bbuseruploads.s3.amazonaws.com	unknown	unknown	false		high
pool.supportxmr.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://185.163.204.24/	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://a0621298.xsph.ru/advert.msi	false		high
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/4457553c06dee2e98e4f451cad0abfa16d7760a4	false	• Avira URL Cloud: safe	unknown
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/e946ea03b0a56043b0189e637403106a5b3aad8e	false	• Avira URL Cloud: safe	unknown
http://a0621298.xsph.ru/9.exe	false		high
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• 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/443.exe	false		high
http://a0621298.xsph.ru/File.exe	false		high

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
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
54.38.220.85	unicupload.top	France		16276	OVHFR	false
104.47.54.36	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
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	false
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552945
Start date:	13.01.2022
Start time:	23:27:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0Cjy7Lkv1A.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	50
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@56/31@94/17
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 29.6% (good quality ratio 24.7%) • Quality average: 67.8% • Quality standard deviation: 37%
HCA Information:	• Successful, ratio: 96% • 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
23:29:09	Task Scheduler	Run new task: Firefox Default Browser Agent EDCB7C3654C5C579 path: C:\Users\user\AppData\Roaming\ujhcrda
23:29:21	API Interceptor	1x Sleep call for process: 7063.exe modified
23:29:32	API Interceptor	10x Sleep call for process: svchost.exe modified
23:29:41	API Interceptor	1x Sleep call for process: WerFault.exe modified
23:30:08	API Interceptor	3x Sleep call for process: 1BCC.exe modified
23:30:10	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
23:30:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
23:30:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_s.exe

Time	Type	Description
23:30:42	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
23:30:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_s.exe
23:31:06	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\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24859360587628684
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU46:BJiRdwfu2SRU46
MD5:	A83E0A729D4A1F55166CB05328B01B69
SHA1:	CB9E63E045059073AC31F4A4630B1228444D4015
SHA-256:	E390FCBF4FF541845B1C55FBA10CBDCEA0C364620A90280EA1BD75E27BD118B1
SHA-512:	E779E06BA24BD4409354222DF3E22C31250BCC279157F7020BFBA3259A985506DCDD3B3178F068C2E9DD1AE65E56247F1EAFA1A89649C1ACC46A9517D1E4424
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x81ef5937, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25071192802551023
Encrypted:	false
SSDEEP:	384:c+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:DSB2nSB2RSjlK/+mLesOj1J2

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
MD5:	18F46E54AD0F6D90BAA6DD6ADDBB5B06
SHA1:	02A2CD28172475401FA0EB4DEFED4116A27C504B
SHA-256:	635C3E6F66EC0E3AE0A794FE3F336039F8D3FDB65269E216051F6844B6293FD2
SHA-512:	C50F160F2B9676EFE8C3C13EA911A3C8B9AD5132D8214CBCF605B4984C1AA77AAF28DE98CFF0B6880B79B4BC16FC734B62BFAC4D04465AEEBA4F19D976C66BCC
Malicious:	false
Reputation:	unknown
Preview:	..Y7... .....e.f.3...w.....&.....w..*....z..h.(.....3...w.....B.....@..... ....3...w..... .....k.#.*....z.u.....*....z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07743634763724366
Encrypted:	false
SSDEEP:	3:Gwlt1EvPzghl/bJdAtiSPzW01oll3VkttlmlnI:GQysht4rzK3
MD5:	6C5620A22A87F1FAA1C600661C7FB193
SHA1:	BF2C1E30D2423E49777823EBF419C0B070BE65CC
SHA-256:	F2EAB83FE956D6CCAA66597AC764992AFAFDF32BC472C16C17721711685E9E23
SHA-512:	7308CFE4C3AF2F52388AD915E55AFDEC057B4146DF2CC342335821EDEBC20FEFECBBBF5ED636F3B8AFB238A048859A189C3574B03127E23B013CB1330EC23DC2
Malicious:	false
Reputation:	unknown
Preview:	.....3...w..*....z.....w.....w.....w....:O.....w.....*....z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_60C2.exe_b994e4a82aa011c06f96cb901a89f64e833a6a1c_f737e9d6_0beefd4a\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):	0.8141362247109446
Encrypted:	false
SSDEEP:	96:f8NFFznbXSGLzCHyA+9OQoJ7R3V6tpXIQcQec6tycEfcw3WFz+HbHg/8BRTf3o8e:UnznW4eSo8HQ0l7jIq/u7syS274Itf
MD5:	8E70A2A7A41C0DAA597D4DE569DD1103
SHA1:	1DC0A1EDC935BF48C2ABC3EFB1E9718ADDFEEFE8
SHA-256:	923DFEF1785F738691F6ADB632C2765D66DDD11CEC802678AAD12CD9196B6D7F
SHA-512:	04CB2EE6D8F3461987DCA542929C8E5DFC379DB932E069FB6DEC4750A8BBBD28ADD933DB651CB39E7516F0FC5B48A939E75A02247CE56649152AB3E526B3923
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.1.8.9.6.3.4.5.8.2.3.5.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.1.8.9.7.9.5.5.1.9.0.8.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.8.a.e.7.f.1.f.-.b.0.1.6.-.4.d.e.7.-.9.f.5.8.-.f.3.a.d.b.3.4.3.a.3.2.4.....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.=.4.a.a.5.1.d.c.e.-.6.8.7.3.-.4.5.c.b.-.8.6.9.9.-.1.3.b.8.8.e.b.4.d.4.a.8.....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.=.6.0.C.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.2.c.-.0.0.0.1.-.0.0.1.7.-.6.8.6.3.-.9.6.6.d.1.8.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.6.1.c.4.3.d.4.6.5.8.4.5.6.a.1.b.f.3.a.c.1.6.0.4.f.5.5.1.8.b.1.0.0.0.0.2.9.0.1.!.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.!.6.0.C.2...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\WER27C7.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53092
Entropy (8bit):	3.0504300134413387
Encrypted:	false
SSDEEP:	1536:6gHzsgnsrlS1jO9AEojWxfbWIwtt0IbRpvuCPYq:6gHzsgnsrlS1jO9AEojWxfSIwtt0IbR5
MD5:	C011905D2C70667B9C517B4D7E3ACDA2
SHA1:	B70D4DDD72CBCCE688B3B3AD22BCD006D123C096
SHA-256:	93E4F641A0328CD61DDFA891D41D5970476DC6C7B63A47FECF0C11967BDF950B

C:\ProgramData\Microsoft\Windows\WER\Temp\WER27C7.tmp.csv	
SHA-512:	2C90438FABB46A25AC6441A602BE70EF872A4951D17F8D0215724158844CDD9E2450644DAD757214167F5AD2BCDA2707BEE7C7B2753F6F6CC5E5A96A10767A0
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\WER2AD2.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6994209673274248
Encrypted:	false
SSDEEP:	96:9GiZYWJ0G7p9WYXY6W18eziHdYEZ7xtYiAkwvjOwdSCaAcEtqhXg7IV713:9jZDJ0vAOXCIXharEqhXpV713
MD5:	4C6B1B2C012A457482F8CBB38B75888D
SHA1:	F7DB80090AEE55660CC28A073F1F4AED0F332D26
SHA-256:	42B29C438F9A38548D3C5BF4C662069D6C2D102DED5E97EB15FA4787DD0B9E2E
SHA-512:	896FAC6BB53B169ECF864947ACD1C5B9CE74C1BE65FCC953C961259473C97A7C5A9FFB7AC63A46B417E50CB46C47BD80D53C53A553B07E6E16C35E2F747E3EC7
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\WER2C4C.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696610353143529
Encrypted:	false
SSDEEP:	96:9GiZYWGPcKi3YuYkWazH6nYEZgAtPiTFK+6wR56aW0pMBi4yENIv0B3:9jZDbpIeBkaW0iBi4yzsB3
MD5:	FF0B8841B96BCFC15D8534442B4DB606
SHA1:	5210CF5DD5921B479EFFDE18E5AC82F0F852D0AD
SHA-256:	2BA90252B066DDBB6E4C60E984E3B6A20473D208CEDBCC55E6C81811B491074B
SHA-512:	582AC00D42F0D4E0CD6B704707920CA0596211B54BA1E0EF6D4D9C942FF3AD70908B672D0FCBAFB285A80CA7628E184297661CE9B2D7136E31BA36BE9F3DE60
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\WER4237.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 07:29:24 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.1215398826650915
Encrypted:	false
SSDEEP:	96:5JS888//qUNJHeuuoi7ehEnus9D5a5aiqQ9E+5RVhTugZM2rgGosz30k2WInWIXH:RXRrNHOeh0k6+nrrfos4k7SkcEIJ
MD5:	AB57E822444B815F1AE1D46462953A26
SHA1:	09B089DC757DE5244BD68A45D68D87805D2B7E17
SHA-256:	FF1E2FCAA91C87802E5154F2C9157BDDCA188F5F954E634237B0BD485EBA13AA
SHA-512:	80348AD1738352FC2C7643AE5557ABA684DB91D71C0CC7880CD5A79AB975160D37342124C70854AE02BCE6A68AD1043FBD08960B0E67CC67096DC3E42D16766
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4237.tmp.dmp	
Preview:	MDMP..... .....T&.a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....,...H&.a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER44E.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	61464
Entropy (8bit):	3.0333924723012595
Encrypted:	false
SSDEEP:	1536:pPHmopTW2gAbslRhHVAEFh5e8vATrKVNB/9KJxs/fwe:pPHmopTW2gAbslRhHVpFh5e8vATrKVNF
MD5:	C69B0E4857750FCCC49E90AE82BFDA7B
SHA1:	749AC3C4FA1376349529E79466D165F7C9C9B071
SHA-256:	F8056552462B214AB6E2015013FFAEB9D8EF71B7F19EC19F166418E062799006
SHA-512:	4368B704EE08A61D5D68BA8C798E3AAC30EA05468AE3CE6EA80DD2D45856F298FEFBE70DA2F2D3C33BE125E34C2A468FB4AB77D4431386591E2B07B9B34FD3E8
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\WER48A1.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.698995042194666
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJs67sQ6YJtSUggmfcRSgCpD389bfEYsfcj1m:RrlsNiC67sQ6YDSUggmfcRSYfELfcM
MD5:	F8B49D24DAB61629DBB4C193F37A628D
SHA1:	036A1F7B6B1C50D44714BD3D54A89357CD23EBF1
SHA-256:	8E3897A6926F9A21310DB0B023C9BF2CDD9BF393D5E7ED0D968DD9D5652C21C1
SHA-512:	D6434F1E91ACA6EAA4600FBB2BD67EEB6CDB4209795E9576EB54042B1FEDE8BF42C62B6B881F667D5D92F7B96401B35FC7C52BE70622D45A2DD2CC130A8A8754
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D84.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):	4.47237264790422
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9LDWSC8Br/8fm8M4Jd8qFR+q8v58u1E/EnaMd:uITfjcySNuJzKFRnaMd
MD5:	2B73F70467BA437B411066239627D3AD
SHA1:	9F2057968FC910968C129DA384900FF9B167D6E5
SHA-256:	705A61F9FACB547638362C1C7E8C2F85ABA41AEF45802B1AB66772BABBA3A898
SHA-512:	181E3D7715D468E483C43E84C40A980D78FF7C9408F7463BB3DA051463D3F432CDF1408B1C89265731964259CC955500E1BF8389E132F8B497C9BFAABDF1B1CE
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D84.tmp.xml	
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="1341640" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B3BA.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\B3BA.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\1BCC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata.."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\382E.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427D
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\382E.exe

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

C:\Users\user\AppData\Local\Temp\5126.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\60C2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:lls8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i.hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@.....e..P.....2..... Y..@.....0.....text..... ..`.rdata..D?...0...@..."....@..@.data...X....p...$...b.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\6674.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

C:\Users\user\AppData\Local\Temp\6674.exe

SHA-512:	E35DBE56828E804AA78FE436E1717C3A09C416DBE2873FFFC9B44393E7EC2336CE9C544E4D6011C58E7E706819AEABC027AF9A85AA2A2509BDFC39699560ABD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... T.....b.6.....||O. .....M..... ....&....@.....@.....0.....@.....1...P.....@.....02...../.....@....rsrc.....M.....40.....@....T3QbYgM.....`O.....1..... ..@....adata.....T.....z6.....@.....

C:\Users\user\AppData\Local\Temp\7063.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:QOWFvVSz4X34ToHWGPOeh20XTF2xi69YPUy0ZPv4J3vfrhVggjcGkNlVqI:QO0sMITBsh20XTIp6M5Pv4tX7ITsq
MD5:	3754DB9964B0177B6E905999B6F18FD7
SHA1:	F47B3FCF01C76AF3B174792519D44171413D25AE
SHA-256:	F56B4C870E0B40ED1BF4F1019346F14443BBE8608D6F75ACB92B176D138F74B7
SHA-512:	8BF6439AD6FDC8A8F48F4520FB33A4D69E014BFB70EE3E691DBC611ACA11F1FE2C4B0D3901176455E6D46B8AA661B21C93069E0ABAF78DC93284935E866B29FA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj._.j`.BjRicha.Bj.....PE..L....,_.....\.....`3.....0....@.....w.....(.....1.....s..@... .....0.....text..... ....`.rdata..nY...0...Z...$.....@..@.data.....~.....@....rsrc.....".....@..@.....

C:\Users\user\AppData\Local\Temp\8008.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..''?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\8B25.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

C:\Users\user\AppData\Local\Temp\8B25.exe	
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3ED CD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$...*..... ...`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...",..

C:\Users\user\AppData\Local\Temp\9874.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:	96A495E5D30E66A236C0AEA19DAEDF95B31F254E457647B6553F2D6CAE117F0A6DA2468550333FBAE3FFA94D0960E2459D2259D3B4C2598EFE49FC03E6C36F1 A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....^..... ....@..... .....ta.....4.....hd.,.....code....7.....8..... ..`.text.....P.....<..... ..`.rdata...3... ...4.....@..@.data...$...`.....@.....@....rsrc...4.....R.....@..@..... ....

C:\Users\user\AppData\Local\Temp\A8FB.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	313344
Entropy (8bit):	5.397613918503412
Encrypted:	false
SSDEEP:	3072:ioeQ4Ktj7h8X34vZHWVMC5QNPoT7iilkIexZ41BorVggjcGkNIVqI:recF4Iv0VM457i6E7ITsq
MD5:	2650E6FA017E57264E55CB0078639A13
SHA1:	8677721B6968EA494C69DFFE61E0E34FAF166EB6
SHA-256:	A004E459F0B6F2103369F14E80E3BCD7B16098AFAC311A5C42B5C72E61492475
SHA-512:	1D793F7CAF1AEC58EA24F173984C8BDC4891E93B5F07FC743C4921EF553520CCE80DDC8AC10E0F8A36CFBE190EEAE012C8FA8A9FB8963BF4EB666469C3049C 63
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj ._.j`.BjRicha.Bj.....PE..L....H._..... ...$.....`3.....0....@.....@.....?.....(...`.....1.....s..@... .....0.....text..... ..... ..`.rdata..nY...0...Z...$.....@..@.data...8.....l..~.....@....rsrc.....`.....@..@..... ....

C:\Users\user\AppData\Local\Temp\B3BA.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

C:\Users\user\AppData\Local\Temp\B3BA.exe

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..*.....l... ...`....@.. ..... ..@.....`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\szdcdkt.exe

Process:	C:\Users\user\AppData\Local\Temp\A8FB.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14635008
Entropy (8bit):	6.362637600237045
Encrypted:	false
SSDEEP:	12288:2JF4Iv4Ni6E70707070707070707070707070707070707070707070707070707070j:eF4Iv4Ni
MD5:	F23C1D7C6806E4BFAA8ABAD7CCC77AC1
SHA1:	2EC703653583A824814910985FA858CE464A1847
SHA-256:	77910D7DDF21BEB55CEABBAA66733A0AB89E7A6ACCD1474207F38AE7E793EFCE
SHA-512:	8DD2A8421137E98CD1C64EC1FF1E54D247A93D6573D1CADFAF332693481ECFF5E48021CB3623FF801366D4763DC20E2A4F93ECF72F90198CB04D8B4A1DE5A6B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.jl.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj.._.j`.BjRicha.Bj.....PE..L....H._..... ...$.....`3.....0....@.....@.....?.....(...`.....1.....s..@... .....0.....text..... ....`.rdata..nY...0...Z...$.....@..@.data...8.....l...~.....@....rsrc.....`...f.....@..@..... .....

C:\Users\user\AppData\Roaming\ujhcrda

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	284672
Entropy (8bit):	5.09851739034015
Encrypted:	false
SSDEEP:	3072:AbxI6T6jY7wdRLjumseo44+9acMUpK5XVFR5+zcXXGO1Z6S9daWrxpzbgqru:AbxRx4d8XVFn7W6/muzbgwu
MD5:	EB023C854D3C8A24589E9294FD5D346E
SHA1:	699EB8E25FCD583774381B9FF554C7E8442C8C43
SHA-256:	B602AFD3F94C5820291F8319B23F20E5254212BA6AAB49BE0238D7067CACA7B8
SHA-512:	9D20183622A2BA8E59FD6FC3F8F361DA2C258D040EDE68844ED65303E3EE1AAA5B4DF1C6A2AF13A1A0162FAAB9C23C4577963EF4B5F2601AE8516D26B0E96B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....._. .....$.....4.....@....@.....hv..(..... .....A.....@i..@.....@.....text...#".... ..$..... ..`.rdata..2?...@...@...(.....@..@.data...x.....".."...h.....@....rsrc.. .....@..@.....

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

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Roaming\ujhcrda:Zone.Identifier	
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

C:\Windows\SysWOW64\uuqefjyt\szdcdkt.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14635008
Entropy (8bit):	6.362637600237045
Encrypted:	false
SSDEEP:	12288:2JF4Iv4Ni6E70707070707070707070707070707070707070707070707070j:eF4Iv4Ni
MD5:	F23C1D7C6806E4BFAA8ABAD7CCC77AC1
SHA1:	2EC703653583A824814910985FA858CE464A1847
SHA-256:	77910D7DDF21BEB55CEABBAA66733A0AB89E7A6ACCD1474207F38AE7E793EFCE
SHA-512:	8DD2A8421137E98CD1C64EC1FF1E54D247A93D6573D1CADFAF332693481ECFF5E48021CB3623FF801366D4763DC20E2A4F93ECF72F90198CB04D8B4A1DE5A6 B
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj ._.j`.BjRicha.Bj.....PE..L....H._..... ...$.....`3.....0....@.....@.....?.....(...`.....1.....s..@... .....0.....text..... ..... ..`.rdata..nY...0...Z...$.....@..@.data...8.....l...~.....@....rsrc.....`...f.....@..@..... ....

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):	4.213486179721548
Encrypted:	false
SSDEEP:	12288:7dZYndbynSGWE6tqcojKt2Mr94xHkZIxa7V7v2E1IcBnKiJQqwz8ku:BZYndbynSGB6tq41h2aK
MD5:	313CF8C27BC5DDA4CB242376B4732F0E
SHA1:	D7F171568C1E393961C0C1FF820DDA9FE9AF79D9
SHA-256:	53C6C4ADCAD4E2B98FB4573938E6DE0E9EBA3D6C95ED53968CD315B91B682540
SHA-512:	E38AD7E812012D9695AACEC8DAAF8499113A37D2D28F320495B8D6D025932A495A7E6ABCC02EBE245CAC9A9779A6A45D0F6EF08D5CF041F34C8187DBCEDF7 8C
Malicious:	false
Reputation:	unknown
Preview:	regfV...V...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmz@~r..... ....".u/..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.45981995129144
Encrypted:	false
SSDEEP:	384:9215sxIpnc8fTVgGUKZX7mnnOpuvU87WK:ULCSc8bVgG/ZXSnnO187W
MD5:	7C72645B82F488776CDCB444EC1BA98B
SHA1:	33E6AF1234407B8B26FD75643CE2E9A0E94948EF
SHA-256:	EE26950F8539C166BB61C27B24CE62EB70A9AF98E6256470BECFA13B56AC4248
SHA-512:	F5EF0ECB503B9DAD19EDAAB4DD1B1982CF29343B214CFED9E7CA966CC83B29CD8D4B1CE33C0EED8F4005870D2DCE33E469131D76E5CFA3882C55C9ACB10F6388
Malicious:	false
Reputation:	unknown
Preview:	regfU...U...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmz@~r..... .....$.u/HvLE.N.....U.....mj....T_.N.....`... ..hbin.....p.\..,.....nk,...r..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...r..... ....Z.....Root.....lf.....Root....nk ...r.....}..... .....*.....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):	5.09851739034015
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:	0Cjy7Lkv1A.exe
File size:	284672
MD5:	eb023c854d3c8a24589e9294fd5d346e
SHA1:	699eb8e25fcd583774381b9ff554c7e8442c8c43
SHA256:	b602afd3f94c5820291f8319b23f20e5254212ba6aab49be0238d7067caca7b8
SHA512:	9d20183622a2ba8e59fd6fc3f8f361da2c258d040ede68844ed65303e3ee1aaa5b4df1c6a2af13a1a0162faab9c23c4577963ef4b5f2601ae8516d26b0e96b17
SSDEEP:	3072:AbxI6T6jY7wdRLjumseo44+9acMUpK5XVFR5+zcXXGO1Z6S9daWrxpzbgqru:AbxRx4d8XVFn7W6/muzbgwu

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I.....v.....h.....E.....x.....f.....c.....Rich.....PE..L....._.....

File Icon

Icon Hash:	a4fc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x403410
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:	0x5F8E9300 [Tue Oct 20 07:34:24 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6d4af36ccbaddaffd179ef41d42df9cf

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12223	0x12400	False	0.611488655822	data	6.67194983583	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x14000	0x3f32	0x4000	False	0.366027832031	data	5.43383883533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x18000	0x28178	0x22200	False	0.252253605769	data	2.7902507697	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x41000	0xcd20	0xce00	False	0.65973907767	data	6.33812987137	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 23:29:09.381481886 CET	192.168.2.6	8.8.8.8	0xae58	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:09.843453884 CET	192.168.2.6	8.8.8.8	0xd607	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:10.277985096 CET	192.168.2.6	8.8.8.8	0xf5fc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:10.710042000 CET	192.168.2.6	8.8.8.8	0x7b7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:10.869241953 CET	192.168.2.6	8.8.8.8	0xc752	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:11.345701933 CET	192.168.2.6	8.8.8.8	0x548	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:12.738148928 CET	192.168.2.6	8.8.8.8	0x9370	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:12.902550936 CET	192.168.2.6	8.8.8.8	0x3119	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:13.064692020 CET	192.168.2.6	8.8.8.8	0x1268	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:14.813620090 CET	192.168.2.6	8.8.8.8	0x3c85	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.245038033 CET	192.168.2.6	8.8.8.8	0x9861	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.407557964 CET	192.168.2.6	8.8.8.8	0x48b1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.683904886 CET	192.168.2.6	8.8.8.8	0x5ab0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.836492062 CET	192.168.2.6	8.8.8.8	0x8b66	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.995913982 CET	192.168.2.6	8.8.8.8	0x59b9	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.341053009 CET	192.168.2.6	8.8.8.8	0x1dbc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.495242119 CET	192.168.2.6	8.8.8.8	0x81be	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.675658941 CET	192.168.2.6	8.8.8.8	0xe044	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.838521004 CET	192.168.2.6	8.8.8.8	0xa2d1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:17.027964115 CET	192.168.2.6	8.8.8.8	0xfa97	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:20.687021017 CET	192.168.2.6	8.8.8.8	0x8f92	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:20.852571964 CET	192.168.2.6	8.8.8.8	0x5119	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:21.034580946 CET	192.168.2.6	8.8.8.8	0x5a1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:21.496798038 CET	192.168.2.6	8.8.8.8	0x173	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:23.839807987 CET	192.168.2.6	8.8.8.8	0x2424	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.006145954 CET	192.168.2.6	8.8.8.8	0x632a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.169416904 CET	192.168.2.6	8.8.8.8	0x4aa9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.671953917 CET	192.168.2.6	8.8.8.8	0x80a3	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:26.515676022 CET	192.168.2.6	8.8.8.8	0xf16	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:26.704545975 CET	192.168.2.6	8.8.8.8	0x805b	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 13, 2022 23:29:26.866780996 CET	192.168.2.6	8.8.8.8	0x2c4a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:41.571877003 CET	192.168.2.6	8.8.8.8	0x21c0	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:44.258790970 CET	192.168.2.6	8.8.8.8	0xd574	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.408039093 CET	192.168.2.6	8.8.8.8	0x5e27	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.602161884 CET	192.168.2.6	8.8.8.8	0x404f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.759782076 CET	192.168.2.6	8.8.8.8	0x34f7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.929415941 CET	192.168.2.6	8.8.8.8	0x7f29	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.090981960 CET	192.168.2.6	8.8.8.8	0x75	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.262195110 CET	192.168.2.6	8.8.8.8	0xb816	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.425590038 CET	192.168.2.6	8.8.8.8	0x8551	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.584451914 CET	192.168.2.6	8.8.8.8	0xcef6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.750351906 CET	192.168.2.6	8.8.8.8	0x637f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.907294035 CET	192.168.2.6	8.8.8.8	0xe70f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.363436937 CET	192.168.2.6	8.8.8.8	0x6d8e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.523484945 CET	192.168.2.6	8.8.8.8	0x9540	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.684974909 CET	192.168.2.6	8.8.8.8	0xb436	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.852371931 CET	192.168.2.6	8.8.8.8	0xfc3	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.346960068 CET	192.168.2.6	8.8.8.8	0x61ce	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.549402952 CET	192.168.2.6	8.8.8.8	0x2c1a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.737508059 CET	192.168.2.6	8.8.8.8	0x708b	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.186666012 CET	192.168.2.6	8.8.8.8	0x5d64	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.362607956 CET	192.168.2.6	8.8.8.8	0xe9bc	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.553836107 CET	192.168.2.6	8.8.8.8	0x2622	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.717216969 CET	192.168.2.6	8.8.8.8	0x76e9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.915946960 CET	192.168.2.6	8.8.8.8	0x1d4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:58.091353893 CET	192.168.2.6	8.8.8.8	0xc4e7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:58.271456957 CET	192.168.2.6	8.8.8.8	0x8162	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:04.255681038 CET	192.168.2.6	8.8.8.8	0xe801	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:04.428649902 CET	192.168.2.6	8.8.8.8	0x644f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:04.612395048 CET	192.168.2.6	8.8.8.8	0x337d	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.153584003 CET	192.168.2.6	8.8.8.8	0x1480	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.313498974 CET	192.168.2.6	8.8.8.8	0x12c4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.470238924 CET	192.168.2.6	8.8.8.8	0x792f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.633542061 CET	192.168.2.6	8.8.8.8	0xb05b	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.855351925 CET	192.168.2.6	8.8.8.8	0x1c03	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:08.050093889 CET	192.168.2.6	8.8.8.8	0x7dd8	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 13, 2022 23:30:08.216840982 CET	192.168.2.6	8.8.8.8	0xe947	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:08.382360935 CET	192.168.2.6	8.8.8.8	0x1d12	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:10.574676037 CET	192.168.2.6	8.8.8.8	0xdd13	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:12.392607927 CET	192.168.2.6	8.8.8.8	0x3462	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:14.302822113 CET	192.168.2.6	8.8.8.8	0x69b2	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:15.189268112 CET	192.168.2.6	8.8.8.8	0x5615	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:15.711497068 CET	192.168.2.6	8.8.8.8	0x3ce5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:15.904176950 CET	192.168.2.6	8.8.8.8	0x4628	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:16.051207066 CET	192.168.2.6	8.8.8.8	0xeb08	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.567692995 CET	192.168.2.6	8.8.8.8	0x1	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.798347950 CET	192.168.2.6	8.8.8.8	0x1113	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:19.158591032 CET	192.168.2.6	8.8.8.8	0x64a3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:19.324814081 CET	192.168.2.6	8.8.8.8	0x2406	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:19.491065025 CET	192.168.2.6	8.8.8.8	0x35e3	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:22.573787928 CET	192.168.2.6	8.8.8.8	0xc9d2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:22.883111954 CET	192.168.2.6	8.8.8.8	0x4664	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:24.475070000 CET	192.168.2.6	8.8.8.8	0xb01c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:25.396651030 CET	192.168.2.6	8.8.8.8	0x53f7	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:28.579149008 CET	192.168.2.6	8.8.8.8	0x15f	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:39.841985941 CET	192.168.2.6	8.8.8.8	0x9e17	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:42.829236984 CET	192.168.2.6	8.8.8.8	0xb5eb	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.347338915 CET	192.168.2.6	8.8.8.8	0x8366	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.445586920 CET	192.168.2.6	8.8.8.8	0xd51b	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.520307064 CET	192.168.2.6	8.8.8.8	0xf56e	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.742400885 CET	192.168.2.6	8.8.8.8	0xd2b2	Standard query (0)	pool.supportxmr.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:51.994684935 CET	192.168.2.6	8.8.8.8	0xba00	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.390553951 CET	192.168.2.6	8.8.8.8	0x9ec1	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:18.783371925 CET	192.168.2.6	8.8.8.8	0x2c4b	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 13, 2022 23:29:09.697674036 CET	8.8.8.8	192.168.2.6	0xae58	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:10.131162882 CET	8.8.8.8	192.168.2.6	0xd607	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:10.563831091 CET	8.8.8.8	192.168.2.6	0xf5fc	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 13, 2022 23:29:10.727297068 CET	8.8.8.8	192.168.2.6	0x7b7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:11.180031061 CET	8.8.8.8	192.168.2.6	0xc752	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:11.364842892 CET	8.8.8.8	192.168.2.6	0x548	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:12.757402897 CET	8.8.8.8	192.168.2.6	0x9370	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:12.919792891 CET	8.8.8.8	192.168.2.6	0x3119	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:13.084080935 CET	8.8.8.8	192.168.2.6	0x1268	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.101315022 CET	8.8.8.8	192.168.2.6	0x3c85	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.262005091 CET	8.8.8.8	192.168.2.6	0x9861	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.424645901 CET	8.8.8.8	192.168.2.6	0x48b1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.701661110 CET	8.8.8.8	192.168.2.6	0x5ab0	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:15.853955984 CET	8.8.8.8	192.168.2.6	0x8b66	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.283864021 CET	8.8.8.8	192.168.2.6	0x59b9	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.360713959 CET	8.8.8.8	192.168.2.6	0x1dbc	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.514317036 CET	8.8.8.8	192.168.2.6	0x81be	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.692796946 CET	8.8.8.8	192.168.2.6	0xe044	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:16.858153105 CET	8.8.8.8	192.168.2.6	0xa2d1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:17.046593904 CET	8.8.8.8	192.168.2.6	0xfa97	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:20.704349041 CET	8.8.8.8	192.168.2.6	0x8f92	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:20.871716976 CET	8.8.8.8	192.168.2.6	0x5119	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:21.347768068 CET	8.8.8.8	192.168.2.6	0x5a1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:21.516134977 CET	8.8.8.8	192.168.2.6	0x173	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:23.859105110 CET	8.8.8.8	192.168.2.6	0x2424	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.025132895 CET	8.8.8.8	192.168.2.6	0x632a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.487891912 CET	8.8.8.8	192.168.2.6	0x4aa9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.694325924 CET	8.8.8.8	192.168.2.6	0x80a3	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.694325924 CET	8.8.8.8	192.168.2.6	0x80a3	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 13, 2022 23:29:24.694325924 CET	8.8.8.8	192.168.2.6	0x80a3	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.694325924 CET	8.8.8.8	192.168.2.6	0x80a3	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:24.694325924 CET	8.8.8.8	192.168.2.6	0x80a3	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:26.533840895 CET	8.8.8.8	192.168.2.6	0xf16	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:26.723767996 CET	8.8.8.8	192.168.2.6	0x805b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:26.886517048 CET	8.8.8.8	192.168.2.6	0x2c4a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:41.589410067 CET	8.8.8.8	192.168.2.6	0x21c0	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:41.589410067 CET	8.8.8.8	192.168.2.6	0x21c0	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:41.589410067 CET	8.8.8.8	192.168.2.6	0x21c0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:41.589410067 CET	8.8.8.8	192.168.2.6	0x21c0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:41.589410067 CET	8.8.8.8	192.168.2.6	0x21c0	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:44.278407097 CET	8.8.8.8	192.168.2.6	0xd574	No error (0)	patmushta.info		8.209.67.104	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.427587986 CET	8.8.8.8	192.168.2.6	0x5e27	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.619612932 CET	8.8.8.8	192.168.2.6	0x404f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.777292013 CET	8.8.8.8	192.168.2.6	0x34f7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:48.948421955 CET	8.8.8.8	192.168.2.6	0x7f29	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.110455036 CET	8.8.8.8	192.168.2.6	0x75	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.279872894 CET	8.8.8.8	192.168.2.6	0xb816	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.444879055 CET	8.8.8.8	192.168.2.6	0x8551	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.602030039 CET	8.8.8.8	192.168.2.6	0xcef6	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:49.769073963 CET	8.8.8.8	192.168.2.6	0x637f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.219671011 CET	8.8.8.8	192.168.2.6	0xe70f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.382039070 CET	8.8.8.8	192.168.2.6	0x6d8e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.543113947 CET	8.8.8.8	192.168.2.6	0x9540	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 13, 2022 23:29:50.702033997 CET	8.8.8.8	192.168.2.6	0xb436	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:50.871994972 CET	8.8.8.8	192.168.2.6	0xfc3	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.366504908 CET	8.8.8.8	192.168.2.6	0x61ce	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.566884041 CET	8.8.8.8	192.168.2.6	0x2c1a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.761998892 CET	8.8.8.8	192.168.2.6	0x708b	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:56.761998892 CET	8.8.8.8	192.168.2.6	0x708b	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.206146002 CET	8.8.8.8	192.168.2.6	0x5d64	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.382162094 CET	8.8.8.8	192.168.2.6	0xe9bc	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.573051929 CET	8.8.8.8	192.168.2.6	0x2622	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.736783981 CET	8.8.8.8	192.168.2.6	0x76e9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:57.935136080 CET	8.8.8.8	192.168.2.6	0x1d4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:58.109098911 CET	8.8.8.8	192.168.2.6	0xc4e7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:29:58.288562059 CET	8.8.8.8	192.168.2.6	0x8162	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:04.275192022 CET	8.8.8.8	192.168.2.6	0xe801	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:04.447892904 CET	8.8.8.8	192.168.2.6	0x644f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:04.635010958 CET	8.8.8.8	192.168.2.6	0x337d	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.170701981 CET	8.8.8.8	192.168.2.6	0x1480	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.333105087 CET	8.8.8.8	192.168.2.6	0x12c4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.491004944 CET	8.8.8.8	192.168.2.6	0x792f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.651065111 CET	8.8.8.8	192.168.2.6	0xb05b	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:07.874785900 CET	8.8.8.8	192.168.2.6	0x1c03	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:08.069142103 CET	8.8.8.8	192.168.2.6	0x7dd8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:08.235975027 CET	8.8.8.8	192.168.2.6	0xe947	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:08.401951075 CET	8.8.8.8	192.168.2.6	0x1d12	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:10.677889109 CET	8.8.8.8	192.168.2.6	0xdd13	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:12.421346903 CET	8.8.8.8	192.168.2.6	0x3462	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 23:30:14.320513964 CET	8.8.8.8	192.168.2.6	0x69b2	No error (0)	a0621298.x sph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:15.208156109 CET	8.8.8.8	192.168.2.6	0x5615	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:15.729043007 CET	8.8.8.8	192.168.2.6	0x3ce5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:15.923553944 CET	8.8.8.8	192.168.2.6	0x4628	No error (0)	a0621298.x sph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:16.341681957 CET	8.8.8.8	192.168.2.6	0xeb08	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.590646029 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.590646029 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.590646029 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.590646029 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.590646029 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:17.815614939 CET	8.8.8.8	192.168.2.6	0x1113	No error (0)	a0621298.x sph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:19.175718069 CET	8.8.8.8	192.168.2.6	0x64a3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:19.343470097 CET	8.8.8.8	192.168.2.6	0x2406	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:19.510390043 CET	8.8.8.8	192.168.2.6	0x35e3	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:22.593178988 CET	8.8.8.8	192.168.2.6	0xc9d2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:22.902317047 CET	8.8.8.8	192.168.2.6	0x4664	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:24.494168997 CET	8.8.8.8	192.168.2.6	0xb01c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:25.417500973 CET	8.8.8.8	192.168.2.6	0x53f7	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:25.417500973 CET	8.8.8.8	192.168.2.6	0x53f7	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:25.417500973 CET	8.8.8.8	192.168.2.6	0x53f7	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:25.417500973 CET	8.8.8.8	192.168.2.6	0x53f7	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:25.417500973 CET	8.8.8.8	192.168.2.6	0x53f7	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:28.691292048 CET	8.8.8.8	192.168.2.6	0x15f	No error (0)	patmushta.info		8.209.67.104	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:39.859559059 CET	8.8.8.8	192.168.2.6	0x9e17	No error (0)	a0621298.x sph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:42.850610971 CET	8.8.8.8	192.168.2.6	0xb5eb	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.375211000 CET	8.8.8.8	192.168.2.6	0x8366	No error (0)	a0621298.x sph.ru		141.8.194.74	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 23:30:43.463148117 CET	8.8.8.8	192.168.2.6	0xd51b	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 23:30:43.463148117 CET	8.8.8.8	192.168.2.6	0xd51b	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 23:30:43.463148117 CET	8.8.8.8	192.168.2.6	0xd51b	No error (0)	s3-w.us-east-1.amazonaws.com		54.231.194.41	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.539891005 CET	8.8.8.8	192.168.2.6	0xf56e	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 23:30:43.539891005 CET	8.8.8.8	192.168.2.6	0xf56e	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 23:30:43.539891005 CET	8.8.8.8	192.168.2.6	0xf56e	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.203.217	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.761686087 CET	8.8.8.8	192.168.2.6	0xd2b2	No error (0)	pool.supportxmr.com	pool-fr.supportxmr.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 23:30:43.761686087 CET	8.8.8.8	192.168.2.6	0xd2b2	No error (0)	pool-fr.supportxmr.com		149.202.83.171	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.761686087 CET	8.8.8.8	192.168.2.6	0xd2b2	No error (0)	pool-fr.supportxmr.com		94.23.23.52	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.761686087 CET	8.8.8.8	192.168.2.6	0xd2b2	No error (0)	pool-fr.supportxmr.com		94.23.247.226	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.761686087 CET	8.8.8.8	192.168.2.6	0xd2b2	No error (0)	pool-fr.supportxmr.com		37.187.95.110	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:43.761686087 CET	8.8.8.8	192.168.2.6	0xd2b2	No error (0)	pool-fr.supportxmr.com		91.121.140.167	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:52.014040947 CET	8.8.8.8	192.168.2.6	0xba00	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.418649912 CET	8.8.8.8	192.168.2.6	0x9ec1	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.418649912 CET	8.8.8.8	192.168.2.6	0x9ec1	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.418649912 CET	8.8.8.8	192.168.2.6	0x9ec1	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.418649912 CET	8.8.8.8	192.168.2.6	0x9ec1	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 13, 2022 23:30:59.418649912 CET	8.8.8.8	192.168.2.6	0x9ec1	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 13, 2022 23:31:19.102844000 CET	8.8.8.8	192.168.2.6	0x2c4b	No error (0)	patmushta.info		8.209.67.104	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- qsmgbhufo.net
  - host-data-coin-11.com
- asruhu.org
- jcgov.net
- obmpjgr.org
- sstfqxq.net

- jlldr.org
- voqqwvg.net
- lmkns.org
- data-host-coin-8.com
- qhgexnr.com
- yhmjbvbr.net
- hyjsal.org
- dgxouben.org
- bculwb.com
- unicupload.top
- qfpwti.com
- xvnibudur.org
- wmvxxhaln.net
- ogoctcljqs.com
- ioktb.net
- dukmi.com
- mcwxjjc.org
- ohvdekeqkm.org
- 185.7.214.171:8080
- mlhkcu.org
- vevlc.com
- ohlut.com
- omhdbkt.net
- mfconnslgq.com
- pubhrhxb.com
- ajgkqwkg.org
- xrbspm.com
- epcciphsoh.org
- tbqbqbxaj.net
- yedkq.org

- nekvodf.com
- ywykfwn.net
- qfbgcss.net
- lxjysfgjrh.org
- qxnyvqdps.net
- wcdhabii.org
- ynptmns.com
- yjoyannoc.org
- vsnokv.org
- wlmasccc.com
- qalbmnobc.org
- qmvwr.net
- fhfjy.com
- krgodthiqk.net
- fpepckdf.org
- ovhmquitm.com
- jbmqdifhe.com
- a0621298.xsph.ru
- fkgaaiey.net
- kebbk.net
- hoircbi.org
- aglrl.com
- ivytp.com
- rbokhamk.net
- 185.163.204.22
- 185.163.204.24
- molmwvfdsj.org
- uqmibnvyi.org
- cmmwfel.org
- voeiplb.com

- xivyfkgciu.net
- ydjicveig.com
- mtcpl.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 0Cjy7Lkv1A.exe PID: 4440 Parent PID: 3036

General

Start time:	23:28:25
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\0Cjy7Lkv1A.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\0Cjy7Lkv1A.exe"
Imagebase:	0x400000
File size:	284672 bytes
MD5 hash:	EB023C854D3C8A24589E9294FD5D346E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 0Cjy7Lkv1A.exe PID: 6452 Parent PID: 4440

General

Start time:	23:28:28
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\0Cjy7Lkv1A.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\0Cjy7Lkv1A.exe"
Imagebase:	0x400000
File size:	284672 bytes
MD5 hash:	EB023C854D3C8A24589E9294FD5D346E
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: 00000001.00000002.419458917.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.419524662.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3440 Parent PID: 6452

General

Start time:	23:28:35
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000000.404651747.0000000004151000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6492 Parent PID: 560

General

Start time:	23:28:40
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 1520 Parent PID: 560

General

Start time:	23:28:52
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5036 Parent PID: 560

General

Start time:	23:29:07
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: ujhcrda PID: 5724 Parent PID: 936

General

Start time:	23:29:09
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\ujhcrda
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ujhcrda
Imagebase:	0x400000
File size:	284672 bytes
MD5 hash:	EB023C854D3C8A24589E9294FD5D346E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: ujhcrda PID: 5416 Parent PID: 5724

General

Start time:	23:29:12

Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\ujhcrda
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ujhcrda
Imagebase:	0x400000
File size:	284672 bytes
MD5 hash:	EB023C854D3C8A24589E9294FD5D346E
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: 0000000D.00000002.471381402.0000000000460000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.471483923.0000000000491000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 60C2.exe PID: 6188 Parent PID: 3440

General

Start time:	23:29:13
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\60C2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\60C2.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs
Reputation:	moderate

Analysis Process: svchost.exe PID: 4192 Parent PID: 560

General

Start time:	23:29:16
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5668 Parent PID: 4192

General

Start time:	23:29:16
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6188 -ip 6188
Imagebase:	0x200000
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: 7063.exe PID: 7052 Parent PID: 3440

General

Start time:	23:29:18
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7063.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\7063.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: 00000011.00000002.474690379.0000000000571000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000011.00000002.474690379.0000000000571000.00000004.00000020.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: 2784 Parent PID: 6188

General

Start time:	23:29:19
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6188 -s 520
Imagebase:	0x200000
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: A8FB.exe PID: 4692 Parent PID: 3440

General

Start time:	23:29:21
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\A8FB.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A8FB.exe
Imagebase:	0x400000
File size:	313344 bytes
MD5 hash:	2650E6FA017E57264E55CB0078639A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000013.00000002.499421318.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000013.00000003.480122610.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000013.00000002.501018079.0000000000550000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Analysis Process: B3BA.exe PID: 6964 Parent PID: 3440

General

Start time:	23:29:24
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B3BA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B3BA.exe
Imagebase:	0x370000
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: 00000014.00000002.565709295.0000000003881000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000014.00000002.566907931.00000000039F1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 7092 Parent PID: 4692

General

Start time:	23:29:27
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\uuqefjyt\
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 2968 Parent PID: 7092

General

Start time:	23:29:28
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 3496 Parent PID: 4692

General

Start time:	23:29:28
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\szdcdkt.exe" C:\Windows\SysWOW64\uuqefjyt\
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 1312 Parent PID: 3496

General

Start time:	23:29:29
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 3220 Parent PID: 4692

General

Start time:	23:29:29
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create uuqefjyt binPath= "C:\Windows\SysWOW64\uuqefjyt\szdcdkt.exe /d\"C:\Users\user\AppData\Local\Temp\A8FB.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x13c0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3252 Parent PID: 560

General

Start time:	23:29:29

Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5004 Parent PID: 3220

General

Start time:	23:29:30
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5324 Parent PID: 4692

General

Start time:	23:29:31
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description uuqefjyt "wifi internet conection
Imagebase:	0x13c0000
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: 5432 Parent PID: 5324

General

Start time:	23:29:31
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

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

Analysis Process: sc.exe PID: 2192 Parent PID: 4692

General

Start time:	23:29:32
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start uuqefjyt
Imagebase:	0x13c0000
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: 6112 Parent PID: 2192

General

Start time:	23:29:32
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 4388 Parent PID: 4692

General

Start time:	23:29:33
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x9e0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: szdcdkt.exe PID: 2972 Parent PID: 560

General

Start time:	23:29:33
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\uuqefjyt\szdcdkt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\uuqefjyt\szdcdkt.exe /d"C:\Users\user\AppData\Local\Temp\A8FB.exe"
Imagebase:	0x400000
File size:	14635008 bytes
MD5 hash:	F23C1D7C6806E4BFAA8ABAD7CCC77AC1
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: 00000024.00000003.507342269.0000000000690000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000024.00000002.511069227.0000000000EB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000024.00000002.510317453.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000024.00000002.510779082.0000000000670000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4820 Parent PID: 4388

General

Start time:	23:29:33
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6780 Parent PID: 2972

General

Start time:	23:29:38
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0xf20000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000027.00000002.631897455.0000000000A50000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 1624 Parent PID: 560

General

Start time:	23:29:41
Start date:	13/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: B3BA.exe PID: 4264 Parent PID: 6964

General

Start time:	23:29:41
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B3BA.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\B3BA.exe
Imagebase:	0x250000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: B3BA.exe PID: 1756 Parent PID: 6964

General

Start time:	23:29:46
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B3BA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B3BA.exe
Imagebase:	0x9b0000
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: 0000002A.00000000.537971963.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002A.00000002.629733104.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002A.00000000.539310965.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002A.00000000.538607329.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002A.00000000.537161217.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis