ID: 800784
Sample Name: file.exe
Cookbook: default.jbs
Time: 19:42:59
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

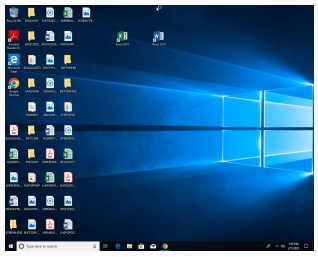
Windows Analysis Report

file.exe

Overview

General Information

Sample Name:	file.exe
Analysis ID:	800784
MD5:	17a74a0281ce…
SHA1:	d88585c6c948…
SHA256:	2814b2a02771…
Tags:	exe RecordBreaker
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Djvu, Fabookie, Raccoon Stealer v2, SmokeLoader

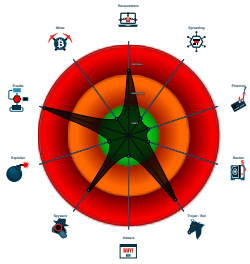
Score: 100

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

Signatures

- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Raccoon Stealer v2
- Multi AV Scanner detection for subm…
- Yara detected Fabookie
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 4356 cmdline: C:\Users\user\Desktop\file.exe MD5: 17A74A0281CEFB5D9C29022FBC79981A)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - 4113.exe (PID: 4968 cmdline: C:\Users\user\AppData\Local\Temp\4113.exe MD5: B141BC58618C537917CC1DA179CBE8AB)
    - 3046.exe (PID: 3680 cmdline: C:\Users\user\AppData\Local\Temp\3046.exe MD5: 46909DA148DE57B2D85591626AEDBD76)
      - 3046.exe (PID: 5672 cmdline: C:\Users\user\AppData\Local\Temp\3046.exe MD5: 46909DA148DE57B2D85591626AEDBD76)
        - icacls.exe (PID: 3460 cmdline: icacls "C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0" /deny *S-1-1-0:(OI)(CI)(DE,DC) MD5: FF0D1D4317A44C951240FAE75075D501)
        - 3046.exe (PID: 5256 cmdline: "C:\Users\user\AppData\Local\Temp\3046.exe" --Admin IsNotAutoStart IsNotTask MD5: 46909DA148DE57B2D85591626AEDBD76)
    - A33B.exe (PID: 3776 cmdline: C:\Users\user\AppData\Local\Temp\A33B.exe MD5: B328ABE938AE81E9382BD6858A6EE77F)
      - llpb1133.exe (PID: 2560 cmdline: "C:\Users\user\AppData\Local\Temp\llpb1133.exe" MD5: 81A0ECC23B44DA5116D397C0A3104A05)
      - pliu.exe (PID: 1952 cmdline: "C:\Users\user\AppData\Local\Temp\pliu.exe" MD5: B9363486500E209C05F97330226BBF8A)
        - conhost.exe (PID: 5060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - pliu.exe (PID: 5180 cmdline: "C:\Users\user\AppData\Local\Temp\pliu.exe" -h MD5: B9363486500E209C05F97330226BBF8A)
          - conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - XandETC.exe (PID: 5632 cmdline: "C:\Users\user\AppData\Local\Temp\XandETC.exe" MD5: 3006B49F3A30A80BB85074C279ACC7DF)
    - 98D7.exe (PID: 5352 cmdline: C:\Users\user\AppData\Local\Temp\98D7.exe MD5: 81A0ECC23B44DA5116D397C0A3104A05)
    - E4.exe (PID: 2096 cmdline: C:\Users\user\AppData\Local\Temp\E4.exe MD5: 29C3DE14DFFA53EDC7E690D0FC0ECCE2)
    - ECFB.exe (PID: 996 cmdline: C:\Users\user\AppData\Local\Temp\ECFB.exe MD5: 3A452937E8A961C5E19974C2CBB4AFAA)
      - WerFault.exe (PID: 4116 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 996 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - D8D3.exe (PID: 5128 cmdline: C:\Users\user\AppData\Local\Temp\D8D3.exe MD5: 0CA939E14D58B13997144F0AF89ADEA9)
    - 3046.exe (PID: 3112 cmdline: "C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart MD5: 46909DA148DE57B2D85591626AEDBD76)
    - 3046.exe (PID: 4084 cmdline: "C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart MD5: 46909DA148DE57B2D85591626AEDBD76)
- sievwvt (PID: 3176 cmdline: C:\Users\user\AppData\Roaming\sievwvt MD5: 17A74A0281CEFB5D9C29022FBC79981A)
- 3046.exe (PID: 4424 cmdline: C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe --Task MD5: 46909DA148DE57B2D85591626AEDBD76)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://uaery.top/dl/build2.exe",
    "http://bihsy.com/files/1/build3.exe"
  ],
  "C2 url": "http://bihsy.com/lancer/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-8pCGyFnOj6\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@freshmail.top\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0641JOsie",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||"
```

```
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApKaxnIXI+dNswr3BwHaz||||n2d48dsnCgVqNaCi3raCQH9vXnap8L2JxiWeoQF+T2OGE+ecKJpaifomH2NUPid9n||||n1YbThm64VJFv||/QkGa3aGDfcOQJP+wnHTaJNGHnh||/1JyhqlfJDJ||/FZvINl4VJFyWS||||nJd||/zSb4vp8WmkqCTPgQ5nH8fy1kL9c1Z8BQVhqzuCeiJVFn4QjIt7ct||/vsQXfhOg||||nkmRpwR3oJ40fghjpkqxS+wreCfNIHPXHq8Ope0eOfQ9vXQQ2sapKLhE97+NJ0os0||||n4JoAS5yjNOCUk8aDxFTDbWCtnutApBuv93hFaMpbOlVDbBmBl+ZCXwyfyx8cMEzm||||npQIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://bulimu55t.net/",
    "http://soryytlic4.net/",
    "http://bukubuka1.net/",
    "http://novanosa5org.org/",
    "http://hujukui3.net/",
    "http://newzelannd66.org/",
    "http://golilopaster.org/"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\A33B.exe	MALWARE_Win_DLInjector04	Detects downloader / injector	ditekSHen	• 0x75be97:$s1: Runner • 0x75bffc:$s3: RunOnStartup • 0x75beab:$a1: Antis • 0x75bed8:$a2: antiVM • 0x75bedf:$a3: antiSandbox • 0x75beeb:$a4: antiDebug • 0x75bef5:$a5: antiEmulator • 0x75bf02:$a6: enablePersistence • 0x75bf14:$a7: enableFakeError • 0x75c025:$a8: DetectVirtualMachine • 0x75c04a:$a9: DetectSandboxie • 0x75c075:$a10: DetectDebugger • 0x75c084:$a11: CheckEmulator

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.443553763.0000000000640000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000013.00000003.441885976.000000000087E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000011.00000002.444263115.0000000000816000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x59db:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000013.00000003.462471829.000000000087E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000000.00000002.313442333.0000000000926000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x6012:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B

Click to see the 49 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.3046.exe.400000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth (Nextron Systems)	• 0xe0dea:$s1: http:// • 0xfee98:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0xff528:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0xff54b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10312b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x101026:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe0dea:$f1: http://
15.2.3046.exe.400000.0.unpack	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	
15.2.3046.exe.400000.0.unpack	MALWARE_Win_STOP	Detects STOP ransomware	ditekSHen	• 0xfe888:$x1: C:\SystemID\PersonalID.txt • 0xfed34:$x2: /deny *S-1-1-0:(OI)(CI)(DE,DC) • 0xfe6f0:$x3: e:\doc\my work (c++)_git\encryption\ • 0x104528:$x3: E:\Doc\My work (C++)_Git\Encryption\ • 0xfecec:$s1: " --AutoStart • 0xfed00:$s1: " --AutoStart • 0x102948:$s2: --ForNetRes • 0x102910:$s3: --Admin • 0x102d90:$s4: %username% • 0x102eb4:$s5: ?pid= • 0x102ec0:$s6: &first=true • 0x102ed8:$s6: &first=false • 0xfedf4:$s7: delself.bat • 0x102df8:$mutex1: {1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D} • 0x102e20:$mutex2: {FBB4BCC6-05C7-4ADD-B67B-A98A697323C1} • 0x102e48:$mutex3: {36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}
15.2.3046.exe.400000.0.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0x104528:$a: E:\Doc\My work (C++)_Git\Encryption\Release\encrypt_win_api.pdb • 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
33.2.3046.exe.23515a0.1.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth (Nextron Systems)	• 0xe0dea:$s1: http:// • 0xfee98:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0xff528:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0xff54b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10312b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x101026:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe0dea:$f1: http://
Click to see the 36 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

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

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands

Yara detected Djvu Ransomware

System Summary

Malicious sample detected (through community Yara rule)

Detected VMProtect packer

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

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

Tries to detect virtualization through RDTSC time measurements

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

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

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information

Yara detected SmokeLoader

Yara detected Raccoon Stealer v2

Yara detected Fabookie

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

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality

Yara detected SmokeLoader

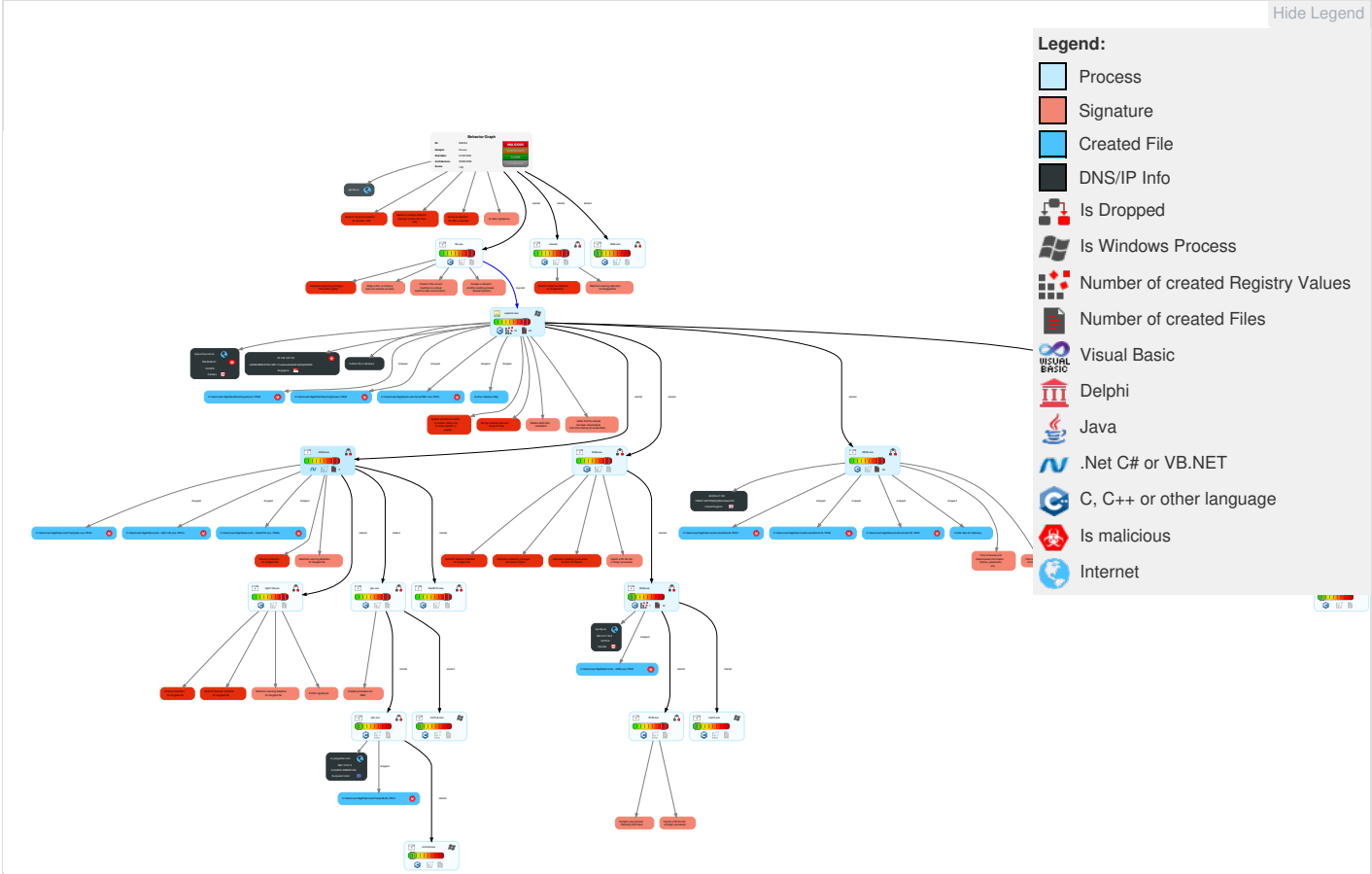
Yara detected Raccoon Stealer v2

Yara detected Fabookie

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	5 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 Services File Permissions Weakness	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	1 Services File Permissions Weakness	2 1 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 Software Packing	NTDS	1 4 4 System Information Discovery	Distributed Component Object Model	2 Clipboard Data	Scheduled Transfer	1 2 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	4 2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Virtualization/Sandbox Evasion	DCSync	1 3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	5 1 2 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Services File Permissions Weakness	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

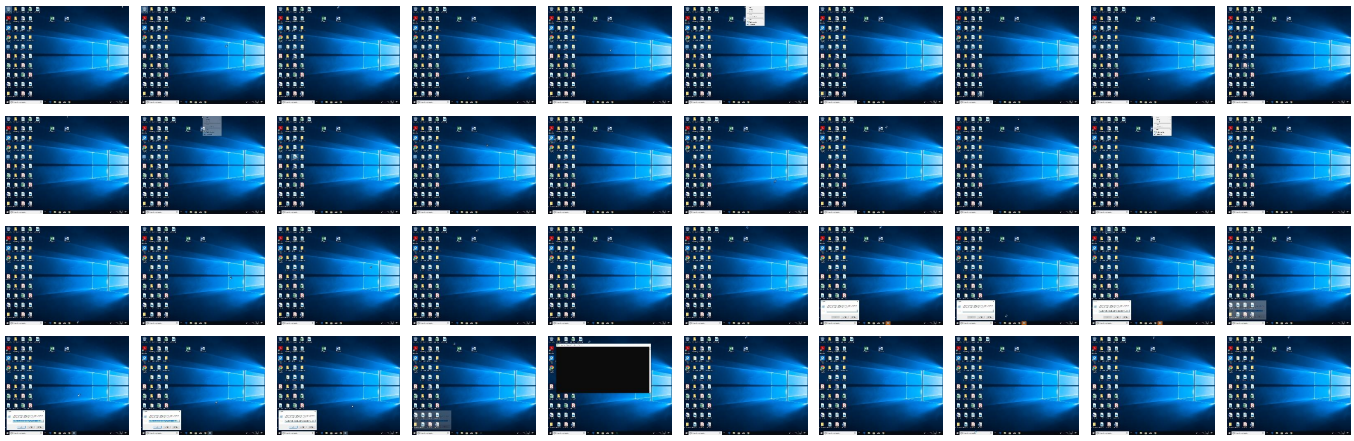
Behavior Graph



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
file.exe	49%	ReversingLabs	Win32.Trojan.RedLine	
file.exe	34%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\98D7.exe	100%	Avira	HEUR/AGEN.1210601	
C:\Users\user\AppData\Local\Temp\llpb1133.exe	100%	Avira	HEUR/AGEN.1210601	
C:\Users\user\AppData\Local\Temp\A33B.exe	100%	Avira	HEUR/AGEN.1234960	
C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\12C0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D8D3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FB61.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\98D7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ECFB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sievwvt	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\llpb1133.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3046.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jhevwvt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4113.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A33B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\nss3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe	62%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Local\Temp\3046.exe	62%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Local\Temp\4113.exe	82%	ReversingLabs	Win32.Trojan.SmokeLoader	
C:\Users\user\AppData\Local\Temp\98D7.exe	77%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\ECFB.exe	56%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Temp\XandETC.exe	92%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\db.dll	42%	ReversingLabs	Win32.Trojan.Ulise	
C:\Users\user\AppData\Local\Temp\llpb1133.exe	77%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\pliu.exe	85%	ReversingLabs	Win32.Backdoor.Manuscrypt	
C:\Users\user\AppData\Roaming\sievwvt	49%	ReversingLabs	Win32.Trojan.RedLine	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.ECFB.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.E4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.4113.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1213203		Download File
15.2.3046.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
14.0.A33B.exe.7b0000.0.unpack	100%	Avira	HEUR/AGEN.1234960		Download File
0.3.file.exe.6d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.3.E4.exe.7e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.3.ECFB.exe.6e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.pliu.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1241636		Download File
0.2.file.exe.680e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.pliu.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1241636		Download File
18.2.ECFB.exe.6d0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.E4.exe.640e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
perficut.at	1%	Virustotal		Browse
potunulit.org	17%	Virustotal		Browse
siaoheg.aappatey.com	0%	Virustotal		Browse
flytourchip.com.br	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://potunulit.org/	0%	URL Reputation	safe	
http://soryytlic4.net/	0%	URL Reputation	safe	
http://siaoheg.aappatey.com/	0%	URL Reputation	safe	
http://novanosa5org.org/	0%	URL Reputation	safe	
http://golilopaster.org/	0%	URL Reputation	safe	
http://iueg.aappatey.com:80/check/safe	0%	URL Reputation	safe	
http://https://xv.yxzgamen.com/2701.html	100%	URL Reputation	malware	
http://bulimu55t.net/	0%	URL Reputation	safe	
http://https://xv.yxzgamen.com/logo.png	100%	URL Reputation	malware	
http://iueg.aappatey.com/check/safe	0%	URL Reputation	safe	
http://hujukui3.net/	0%	URL Reputation	safe	
http://77.73.134.27/llpb1133.exe	100%	URL Reputation	malware	
http://bukubuka1.net/	0%	URL Reputation	safe	
http://newzelannd66.org/	0%	URL Reputation	safe	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	
http://iueg.aappatey.com/check/safeXdkojlmpp	0%	Avira URL Cloud	safe	
http://62.204.41.134/_	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=288019&key=8611a052d7ff506dc761df9a028c28ef	0%	Avira URL Cloud	safe	
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e6044	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/r	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/K	0%	Avira URL Cloud	safe	
http://perficut.at/	0%	Avira URL Cloud	safe	
http://perficut.at/tmp/	0%	Avira URL Cloud	safe	
http://https://flytourchip.com.br/systems/ChromeSetup.exe	0%	Avira URL Cloud	safe	
http://iueg.aappatey.com/check/safeB	0%	Avira URL Cloud	safe	
http://bihsy.com/lancer/get.php	100%	Avira URL Cloud	malware	
http://iueg.aappatey.com/m	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675preseMu	0%	Avira URL Cloud	safe	
http://62.204.41.134/	0%	Avira URL Cloud	safe	
http://perw.facebook.cueg.aappatey.com/check/safe	0%	Avira URL Cloud	safe	
http://iueg.aappatey.com/check/safei	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675	0%	Avira URL Cloud	safe	
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e604	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com:80/check/?sid=288019&key=8611a052d7ff506dc761df9a028c28ef	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675?	0%	Avira URL Cloud	safe	
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e604o	0%	Avira URL Cloud	safe	
http://62.204.41.134/ll	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=288019&key=8611a052d7ff506dc761df9a028c28efcfBb4E4	0%	Avira URL Cloud	safe	
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e604n	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=286587&key=075ea35c9751668450c9ec4c0067c0f6	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=288019&key=8611a052d7ff506dc761df9a028c28efcohor	0%	Avira URL Cloud	safe	
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675c	0%	Avira URL Cloud	safe	
http://iueg.aapp	0%	Avira URL Cloud	safe	
http://iueg.aappatey.com/check/safeT7-16b8-4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	157.240.253.35	true	false		high
perficut.at	195.158.3.162	true	true	• 1%, Virustotal, Browse	unknown
potunulit.org	188.114.96.3	true	true	• 17%, Virustotal, Browse	unknown
siaoheg.aappatey.com	45.66.159.142	true	false	• 0%, Virustotal, Browse	unknown
api.2ip.ua	162.0.217.254	true	false		high
flytourchip.com.br	158.69.96.67	true	true	• 0%, Virustotal, Browse	unknown
xv.yxzgamen.com	188.114.97.3	true	false		unknown
iueg.aappatey.com	45.66.159.142	true	false		unknown
www.facebook.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://flytourchip.com.br/systems/ChromeSetup.exe	true	• Avira URL Cloud: safe	unknown
http://perficut.at/tmp/	true	• Avira URL Cloud: safe	unknown
http://potunulit.org/	true	• URL Reputation: safe	unknown
http://https://www.facebook.com/login.php?next=https%3A%2F%2Fwww.facebook.com%2Fads%2Fmanager%2Faccount_settings%2Faccount_billing	false		high
http://soryytlic4.net/	true	• URL Reputation: safe	unknown
http://novanosa5org.org/	true	• URL Reputation: safe	unknown
http://golilopaster.org/	true	• URL Reputation: safe	unknown
http://bihsy.com/lancer/get.php	true	• Avira URL Cloud: malware	unknown
http://62.204.41.134/	false	• Avira URL Cloud: safe	unknown
http://https://xv.yxzgamen.com/2701.html	true	• URL Reputation: malware	unknown
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e604	false	• Avira URL Cloud: safe	unknown
http://bulimu55t.net/	true	• URL Reputation: safe	unknown
http://https://xv.yxzgamen.com/logo.png	true	• URL Reputation: malware	unknown
http://https://api.2ip.ua/geo.json	false		high
http://siaoheg.aappatey.com/check/?sid=286587&key=075ea35c9751668450c9ec4c0067c0f6	false	• Avira URL Cloud: safe	unknown
http://iueg.aappatey.com/check/safe	false	• URL Reputation: safe	unknown
http://hujukui3.net/	true	• URL Reputation: safe	unknown
http://https://www.facebook.com/ads/manager/account_settings/account_billing	false		high
http://77.73.134.27/llpb1133.exe	true	• URL Reputation: malware	unknown
http://bukubuka1.net/	true	• URL Reputation: safe	unknown
http://newzelannd66.org/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

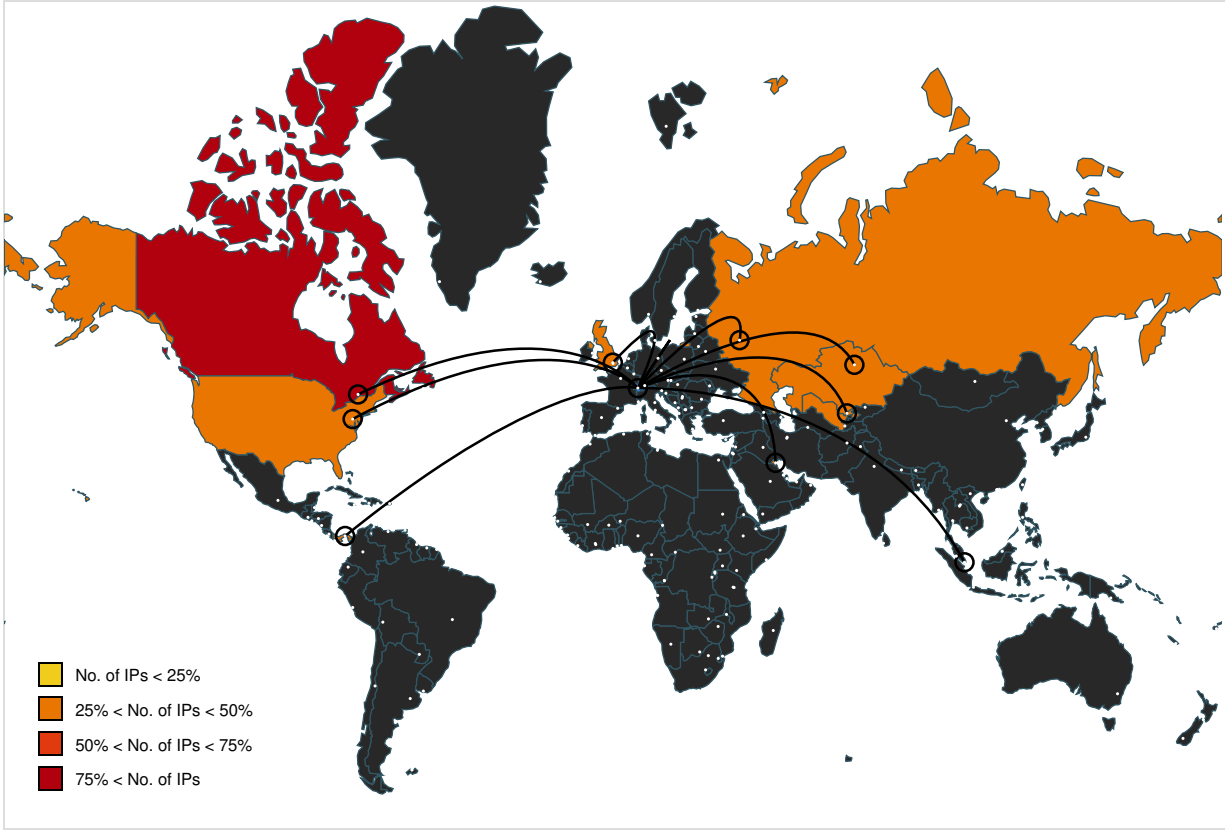
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	D8D3.exe, 00000013.00000003.514197063.000000008E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3i7M54/yX/l/en_US/WYC6LbamQUd.js?_nc_x=Ij3Wp8lg5Kz	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e6044	D8D3.exe, 00000013.00000003.512998592.000000084F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://siaoheg.aappatey.com/K	llpb1133.exe, 00000014.00000002.602167234.00000000004BA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	D8D3.exe, 00000013.00000003.514197063.000000008E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://62.204.41.134/_	D8D3.exe, 00000013.00000003.441885976.000000085F000.00000004.00000020.00020000.00000000.sdmp, D8D3.exe, 00000013.00000003.441770993.000000000084F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://messenger.com/	98D7.exe, 00000010.00000003.474645572.000000002892000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000003.485181523.00000000028B2000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com?fr=crmas_sfpf	D8D3.exe, 00000013.00000003.514197063.000000008E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://siaoheg.aappatey.com/check/?sid=288019&key=8611a052d7ff506dc761df9a028c28ef	98D7.exe, 00000010.00000002.602257740.000000004AB000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000002.603774182.0000000000503000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000002.603774182.0000000000513000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000002.603774182.0000000000549000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.openssl.org/support/faq.html	3046.exe, 00000021.00000002.516427401.000000002350000.00000040.00001000.00020000.00000000.sdmp	false		high
http://iueg.aappatey.com/check/safeXdkojlmpp	98D7.exe, 00000010.00000002.602257740.000000004AB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	3046.exe, 0000000D.00000002.396916881.000000002350000.00000040.00001000.00020000.00000000.sdmp, 3046.exe, 0000000F.00000002.467843881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, 3046.exe, 00000021.00000002.516427401.000000002350000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://siaoheg.aappatey.com/r	98D7.exe, 00000010.00000002.603774182.000000000596000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yR/r/n9ktzHPknGx.js?_nc_x=lj3Wp8lg5Kz	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://perficut.at/	98D7.exe, 00000010.00000002.605295836.0000000289E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://siaoheg.aappatey.com/	98D7.exe, 00000010.00000002.603774182.000000000596000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000002.605295836.000000000289E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://siaoheg.aappatey.com:80/check/?sid=288019&key=8611a052d7ff506dc761df9a028c28ef	98D7.exe, 00000010.00000002.603774182.000000000549000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://iueg.aappatey.com/check/safeB	98D7.exe, 00000010.00000002.605295836.0000000288C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yW/l/0	98D7.exe, 00000010.00000002.605295836.0000000288C000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000003.485181523.00000000028B2000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.602167234.00000000004D1000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.602167234.0000000000522000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604851431.0000000002865000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604870150.00000000288F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/ya/l/0	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://iueg.aappatey.com:80/check/safe	98D7.exe, 00000010.00000002.602257740.000000004AB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://iueg.aappatey.com/m	98D7.exe, 00000010.00000003.492565099.000000004C8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yi/l/0	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yM/r/4x04rJtLVMo.js?_nc_x=Ij3Wp8lg5Kz	98D7.exe, 00000010.00000003.476889083.000000000288E000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000003.485181523.00000000028B2000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.602167234.0000000005220000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604870150.000000000288F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675preseMu	llpb1133.exe, 00000014.00000002.604730284.0000000002820000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yG/l/0	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.602167234.0000000000522000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604870150.000000000288F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yb/r/mkZZ0EnRB0x.js?_nc_x=Ij3Wp8lg5Kz	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://iueg.aappatey.com/check/safei	98D7.exe, 00000010.00000002.605295836.000000000288C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.303832836.000000000F270000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yY/r/ue_OWlkLDZP.js?_nc_x=Ij3Wp8lg5Kz	98D7.exe, 00000010.00000003.484805156.000000000502000.00000004.00000020.00020000.00000000.sdmp, 98D7.exe, 00000010.00000003.485706369.00000000004CF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yE/l/0	98D7.exe, 00000010.00000003.485181523.000000028B2000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.602167234.0000000000522000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604851431.0000000002865000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604870150.000000000288F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	D8D3.exe, 00000013.00000003.514197063.000000008E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://perw.facebook.cueg.aappatey.com/check/safe	98D7.exe, 00000010.00000002.605295836.000000000289E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675	llpb1133.exe, 00000014.00000002.604730284.0000000002841000.00000004.00000020.00020000.00000000.sdmp, llpb1133.exe, 00000014.00000002.604730284.0000000002820000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://siaoheg.aappatey.com/check/?sid=287855&key=53966fc5c1f009ecd22e4b74973b5675?	llpb1133.exe, 00000014.00000002.604730284.0000000002841000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.134/ll	D8D3.exe, 00000013.00000003.514324898.000000087C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	D8D3.exe, 00000013.00000003.514197063.000000008E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	D8D3.exe, 00000013.00000003.514197063.000000008E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e604o	D8D3.exe, 00000013.00000003.512998592.000000084F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.134/2bdc6e9a1ce82117657287e1bc36e604n	D8D3.exe, 00000013.00000003.514324898.000000000843000.00000004.00000020.00020000.00000000.sdmp, D8D3.exe, 00000013.00000003.517099850.0000000000843000.00000004.00000020.00020000.00000000.sdmp, D8D3.exe, 00000013.00000003.512998592.000000000843000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://iueg.aappatey.com/check/safeT7-16b8-4	llpb1133.exe, 00000014.00000002.60473028 4.0000000002820000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://static.xx.fbcdn.net/rsrc.php/v3/yO/r/_tJ17sGyxO X.js?_nc_x=lj3Wp8lg5Kz	98D7.exe, 00000010.00000003.484805156.00 0000000502000.00000004.00000020.0002000 0.00000000.sdmp, 98D7.exe, 00000010.0000 0003.485706369.00000000004CF000.00000004 .00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome? output=fxjson&appid=crmas_sfp&command=	D8D3.exe, 00000013.00000003.514197063.00 000000008E1000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http://siaoheg.aappatey.com/check/? sid=288019&key=8611a052d7ff506dc761df9a028c28ef cfBb4E4	98D7.exe, 00000010.00000002.603774182.00 0000000503000.00000004.00000020.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://siaoheg.aappatey.com/check/? sid=288019&key=8611a052d7ff506dc761df9a028c28ef cohor	98D7.exe, 00000010.00000002.602257740.00 000000004AB000.00000004.00000020.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://static.xx.fbcdn.net/rsrc.php/v3/ym/r/2Z9gzYPL3 TW.js?_nc_x=lj3Wp8lg5Kz	98D7.exe, 00000010.00000003.485181523.00 000000028B2000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	D8D3.exe, 00000013.00000003.514197063.00 000000008E1000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfp	D8D3.exe, 00000013.00000003.514197063.00 000000008E1000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y-/r/qu9vi- bmWl3.js?_nc_x=lj3Wp8lg5Kz	98D7.exe, 00000010.00000003.485181523.00 000000028B2000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http://siaoheg.aappatey.com/check/? sid=287855&key=53966fc5c1f009ecd22e4b74973b567 5c	llpb1133.exe, 00000014.00000002.60473028 4.0000000002841000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/y0/l/0	98D7.exe, 00000010.00000003.485181523.00 000000028B2000.00000004.00000020.0002000 0.00000000.sdmp, llpb1133.exe, 00000014. 00000002.602167234.00000000004D1000.0000 0004.00000020.00020000.00000000.sdmp, ll pb1133.exe, 00000014.00000002.602167234. 0000000000522000.00000004.00000020.00020 000.00000000.sdmp, llpb1133.exe, 0000001 4.00000002.604870150.000000000288F000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y9/l/0	llpb1133.exe, 00000014.00000002.60487015 0.000000000288F000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://iueg.aapp	98D7.exe, 00000010.00000002.607336347.00 000001400EE000.00000002.00000001.0100000 0.0000000D.sdmp, llpb1133.exe, 00000014. 00000002.607091637.00000001400EE000.0000 0002.00000001.01000000.00000012.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/ym/l/0	98D7.exe, 00000010.00000003.485181523.00 000000028B2000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttp s://www.ecosia.org/search?q=	D8D3.exe, 00000013.00000003.514197063.00 000000008E1000.00000004.00000020.0002000 0.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.34.248.24	unknown	Kuwait		42961	GPRS-ASZAINKW	true
190.219.54.242	unknown	Panama		18809	CableOndaPA	true
23.106.124.133	unknown	Singapore		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificpteltdSG	true
45.66.159.142	siaoheg.aappatey.com	Russian Federation		18978	ENZUINC-US	false
62.204.41.134	unknown	United Kingdom		30798	TNNET-ASTNNetOyMainnetworkFI	false
195.158.3.162	perficut.at	Uzbekistan		8193	BRM-ASUZ	true
188.114.97.3	xv.yxzgamen.com	European Union		13335	CLOUDFLARENETUS	false
158.69.96.67	flytourchip.com.br	Canada		16276	OVHFR	true
188.114.96.3	potunulit.org	European Union		13335	CLOUDFLARENETUS	true
77.73.134.27	unknown	Kazakhstan		206751	FIBEROPTIXDE	true
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
157.240.253.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800784
Start date and time:	2023-02-07 19:42:59 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@40/35@15/12
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 74.5% (good quality ratio 66.5%) • Quality average: 67.2% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, consent.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.20
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, g.agametog.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target 4113.exe, PID 4968 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:44:11	API Interceptor	759x Sleep call for process: explorer.exe modified
19:44:47	Task Scheduler	Run new task: Firefox Default Browser Agent 965BA40FEDD9AA3B path: C:\Users\user\AppData\Roaming\sievwvt
19:45:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart
19:45:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart
19:45:28	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe s>--Task
19:45:41	API Interceptor	1x Sleep call for process: WerFault.exe modified
19:45:44	API Interceptor	9x Sleep call for process: 98D7.exe modified
19:45:47	API Interceptor	4x Sleep call for process: pliu.exe modified
19:45:55	Task Scheduler	Run new task: Firefox Default Browser Agent 71F89663E6ACBAD9 path: C:\Users\user\AppData\Roaming\jhevwvt
19:46:06	API Interceptor	4x Sleep call for process: llpb1133.exe modified
19:46:44	Task Scheduler	Run new task: NoteUpdateTaskMachineQC path: C:\Program Files\Notepad\Chrome\updater.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ECFB.exe_c28f7e147f7233fac35d68c9fdcbff1142cbb9f3_c36f58af_10581eb1\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8209235901306622
Encrypted:	false
SSDEEP:	96:f/FTVYCR+kHPwglog7Ro6tpXIQcQ3c6dglcEpcw3b+HbHg/8BRTf3Oy1E/8lh4lj:nBVYCRj7HZ2T0jum/u7sdS274ltL7
MD5:	2ED88DB7DBCF47D1AA71578074509CBC
SHA1:	30D162AC4C2E9AE2B4730A708874254C6271B007
SHA-256:	7ED6039C52041360F4D1C253032180C38FA328404C538C2C1CF787BBAE4C4B9E
SHA-512:	78AC1D5FDD78133BAFF9496A808ABDC7AEBE0D409F8412462A1EB0CA2DBA2B9628D1979933277D70CD4CEC31CCFDBB99A89D810BC56D1AC0AAE6C09070F3CF4
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.=.1.3.3.2.0.3.0.1.5.2.0.0.1.3.5.8.0.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.0.3.0.1.5.2.1.8.7.2.9.0.7.1.....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.=.c.7.9.5.1.2.f.c.-.9.5.6.2.-.4.2.5.c.-.b.8.5.8.-.f.4.6.7.d.4.2.4.6.8.8.0.....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.=.1.3.0.3.4.2.4.5.-.e.6.7.2.-.4.6.c.0.-.b.f.1.c.-.d.4.6.6.6.8.9.d.0.2.9.7.....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.=.E.C.F.B...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.3.e.4.-.0.0.0.1.-.0.0.1.f.-.9.3.7.9.-.1.8.b.b.6.f.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.d.2.0.c.5.0.f.0.3.9.1.d.5.5.0.9.0.c.7.9.1.3.e.2.9.0.f.1.6.4.9.0.0.0.0.0.a.0.4.!.0.0.0.0.6.c.8.5.2.2.a.c.5.4.5.4.4.2.f.2.9.b.6.a.5.a.7.6.8.f.a.9.f.0.f.c.4.a.3.8.a.9.2.8.!.E.C.F.B...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.1.2././.2.3.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5036.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 8 03:45:20 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	42908
Entropy (8bit):	2.0291098699015357
Encrypted:	false
SSDEEP:	192:9kmpyWzYOQzfvGiSUJC+KAA2yglw+HKRME:TLQPFKAA2ynqqE
MD5:	9454AA6B755A43C9F67DFBFAA593A755
SHA1:	1468E2C56D4BABE46A264FE008F93E520A0B1928
SHA-256:	EF8FF51F45A650DEBCC57AE98329F175AEC73134F11A0E1474ABF07548F1D183
SHA-512:	ECC70BE077A376D1236199CFD6D494A1524B8A628346E1DB6E8014AAF0998A0B0CF3CEB5C02A365ADC47BC255DEF5A05FD4F06F8777648B07011F61A3694D3C3
Malicious:	false
Reputation:	unknown

Preview:	MDMP..... .....c.....(.....T.....8.....T.....U.....B.....h.....GenuineIntelW.....T.....c..... .....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\WER5392.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8380
Entropy (8bit):	3.699783088515253
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilN6g6YqUSU9sgmf1SmCCpD689bT1sfBxm:RrlsNi/6g6YpSU9sgmf1SgTOfG
MD5:	96506463F75BA6FD08E77B5ED03E6B87
SHA1:	11D1C5E86BDF69AFB1A84F55F96A1B470519B986
SHA-256:	AD62DA7A69B466F94CEF6F3B56EBB83CC604640BEF37A2F08713EA4EE0ABE2B9
SHA-512:	CEA6031B4C78ABF269C667EB4F1CAF5C48AF2529E6887E088459496FF7F732D64283ACB5B9ACA0636EEE841B446DD94107F23BD023C52C9E9D2616DE2EB35D1
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.>.9.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER545E.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.469696494300214
Encrypted:	false
SSDEEP:	48:cvIwSD8zslJgtWI97jWgc8sqYjj8fm8M4JASF7+q8vP2yD/d:uITf/ESgrsqYMJzKOyD/d
MD5:	1E44FBC26D85C541164EF6FCD3D39196
SHA1:	655E036714A3F5D8D52A5B0A90D30D32FC1C39C5
SHA-256:	EAF64E95B418E07BA14D4C58C14F1CCEC364F781BA557C8788E0C550D3D624E7
SHA-512:	D4B4E2B8DC0DC468ABFA772132885980FCAB561834ED332D632F4884A3A1F0A32D4D8014D76AC351D76A105A61080235A931D8C3241ADDCFFE184991AE39107
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1903015" />.. <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\LocalLow\10PkIt2V82WR

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Reputation:	unknown

Preview:	SQLite format 3.....@ .....[5.....

C:\Users\user\AppData\LocalLow\2KyP65ecp6T3

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*

C:\Users\user\AppData\LocalLow\432zCWSnwm1N

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*

C:\Users\user\AppData\LocalLow\cdE656z8QTF7

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....[5.....g...$.....

C:\Users\user\AppData\LocalLow\freebl3.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684984
Entropy (8bit):	6.857030838615762
Encrypted:	false
SSDEEP:	12288:0oUg2twzqWC4kBNv1pMByWk6TYnhCevOEH07OqHM65BaFBuY3NUNeCLIV/Rqnhab:0oUg2tJWC44WUuY3mMCLA/R+hw
MD5:	15B61E4A910C172B25FB7D8CCB92F754
SHA1:	5D9E319C7D47EB6D31AAED27707FE27A1665031C
SHA-256:	B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
SHA-512:	7C1C982A2B597B665F45024A42E343A0A07A6167F77EE428A203F23BE94B5F225E22A270D1A41B655F3173369F27991770722D765774627229B6B1BBE2A6DC3F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...&.9b....."!.....6.....@A.....4,..S.....x.....T.....8$...&.....0.....D.....text..... ..`.rdata.....0.....@..@.data...<F...@.....&.....@....00cfg.....(.....@..@.rsrc...x.....*.....@..@.reloc..8$.....&.....@..B.....

C:\Users\user\AppData\LocalLow\mozglue.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	627128
Entropy (8bit):	6.792651884784197
Encrypted:	false
SSDEEP:	12288:dfsiG5KNZea77VUHQqROmbIDm0ICRfCtbtEE/2OH9E2ARlZYSd:df53NZea3V+QqROmum0nRKx79E2ARlrd
MD5:	F07D9977430E762B563EAADC2B94BBFA
SHA1:	DA0A05B2B8D269FB73558DFCF0ED5C167F6D3877
SHA-256:	4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862
SHA-512:	6AFD512E4099643BBA3FC7700DD72744156B78B7BDA10263BA1F8571D1E282133A433215A9222A7799F9824F244A2BC80C2816A62DE1497017A4B26D562B7EAF
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b....."!.....V...../.....@A.....cQ.....p.....r.....4C.....W.....h0.....text..... ..`.rdata.....0.....@..@.data.....0.....@....00cfg.....P..... .....@..@.tls.....`....."....@....rsrc.....p.....$.....@..@.reloc..4C.....D.....@..B.....

C:\Users\user\AppData\LocalLow\msvcp140.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	449280
Entropy (8bit):	6.670243582402913
Encrypted:	false
SSDEEP:	12288:UEPa9C9VbL+3Omy5CvyOvzeOKaqhUgiW6QR7t5s03Ooc8dHkC2esGgW8g:UEPa90Vbky5CvyUeOKg03Ooc8dHkC2ed
MD5:	1FB93933FD087215A3C7B0800E6BB703
SHA1:	A78232C352ED06CEDD7CA5CD5CB60E61EF8D86FB
SHA-256:	2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
SHA-512:	79CD448E44B5607863B3CD0F9C8E1310F7E340559495589C428A24A4AC49BEB06502D787824097BB959A1C9CB80672630DAC19A405468A0B64DB5EBD6493590E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._)n..._.....^.".._.^..._..\..._..[..._..Z..._..._.....]..._.Rich.._.....PE..L....(.[....."!....(.....`.....@.....@A.....g.....r.....?.....=..`x..8.....w..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>...^.....@..B.....

C:\Users\user\AppData\LocalLow\nss3.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2042296
Entropy (8bit):	6.775178510549486
Encrypted:	false
SSDEEP:	49152:6dvFywfzFAF7fg39IwA49Kap9bGt+qoStYnOsbqbeQom7gN7BpDD5SkIN1g5D92+:pptximYfpx8OwNiVG09
MD5:	F67D08E8C02574CBC2F1122C53BFB976
SHA1:	6522992957E7E4D074947CAD63189F308A80FCF2
SHA-256:	C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
SHA-512:	2E9D0A211D2B085514F181852FAE6E7CA6AED4D29F396348BEDB59C556E39621810A9A74671566A49E126EC73A60D0F781FA9085EB407DF1EEFD942C18853BE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b....."!.....&.....`.....@A.....!..\...T...@....@..x.....P..h...h.....\....!..@.....text...i..... ..`.rdata.....@..@.data....N.....*.....@....00cfg.....0.....@..@.rsrc...x....@.....@..@.reloc..h....P.....@..B.....

C:\Users\user\AppData\LocalLow\softokn3.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254392
Entropy (8bit):	6.686038834818694
Encrypted:	false
SSDEEP:	6144:uI7A8DMhFE2PlKOcpHSvV6x/CHQyhvs277H0mhWGzTdtb2bbIFxW7zrM2ruyYz+h:uI7A8DMhFE2PlbcpSv0x/CJVUmhDzTvS
MD5:	63A1FE06BE877497C4C2017CA0303537
SHA1:	F4F9CBD7066AFB86877BB79C3D23EDDACA15F5A0
SHA-256:	44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0
SHA-512:	0475EDC7DFBE8660E27D93B7B8B5162043F1F8052AB28C87E23A6DAF9A5CB93D0D7888B6E57504B1F2359B34C487D9F02D85A34A7F17C04188318BB8E89126B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...'.9b....."!.....@A.....tv..S....w.....5..hq.....D{.....text...V..... ..`.rdata.....@..@.data.....~.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B.....

C:\Users\user\AppData\LocalLow\sqlite3.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1099223
Entropy (8bit):	6.502588297211263
Encrypted:	false
SSDEEP:	24576:9jxwSkSteuT4P/y7HjsXAGJyGvN5z4Rui2IXLbO:9Vww8HyrjsvyWN54RZH+
MD5:	DBF4F8DCEFB8056DC6BAE4B67FF810CE
SHA1:	BBAC1DD8A07C6069415C04B62747D794736D0689
SHA-256:	47B64311719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68
SHA-512:	B572CA2F2E4A5CC93E4FCC7A18C0AE6DF888AA4C55BC7DA591E316927A4B5CFCBDDA6E60018950BE891FF3B26F470CC5CCE34D217C2D35074322AB84C32A5D1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...",.b.v.....!..... .....a..... .....n*..... ...;.....text.....`.P`.data...|'... ...(.....@.`..rdata...D...P. ..F...:.....@.`@.bss....(.....`..edata..n*.....,.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... .@.0..rsrc.....@.0..reloc...;... ...<.....@.0B/4.....8....`.....@.@B/19.....R....p.....@..B/31.....]'...@...(.....@..B/45.....-...p. .....@..B/57.....\.....&.....@.0B/70.....#.....2..

C:\Users\user\AppData\LocalLow\vcruntime140.dll

Process:	C:\Users\user\AppData\Local\Temp\D8D3.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80128
Entropy (8bit):	6.906674531653877
Encrypted:	false
SSDEEP:	1536:l9j/j2886xv555et/MCsjw0BuRK3jteopUecbAdz86B+JfBL+eNv:l9j/j28V55At/zqw+lqLUecbAdz8lJrv
MD5:	1B171F9A428C44ACF85F89989007C328
SHA1:	6F25A874D6CBF8158CB7C491DCEDAA81CEAEBBAE
SHA-256:	9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
SHA-512:	99A06770EEA07F36ABC4AE0CECB2AE13C3ACB362B38B731C3BAED045BF76EA6B61EFE4089CD2EFAC27701E9443388322365BDB039CD388987B24D4A43C973BD1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L....(.[......"!.....0.....t(....@A.....?... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe

Process:	C:\Users\user\AppData\Local\Temp\3046.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	722944
Entropy (8bit):	7.843693287624674
Encrypted:	false
SSDEEP:	12288:zUJFDhiQSO/bmqK1NIK6kxk7q4p/dn57k/x4omG1ZQHdt1AaQf8O:zQF0Qn6qQoTLdH76x1R1Z4AaQL
MD5:	46909DA148DE57B2D85591626AEDBD76
SHA1:	8000C3D7B0B33EAA538F8B0E09EFF0559AF06287
SHA-256:	0CA1867B6E512A1E78D8A00CECF4FDC09B665B31F9AF122C78EE4A1E5DE5A692
SHA-512:	C3A4C1392E9300C5A9255A8BEC4757D8244023F5353D693A9E7A1496DA92F1B90482F9201035AB07B669C228F8BEDBE467F5C54BFB8F4D50C90350B0F2076603
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 62%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Qn..Qn..Qn..O<..Mn..O<i..n..v...Vn..Qn...n..O<n.}n..O<~.Pn ..O<{.Pn..RichQn.....PE..L.....a.....6.....fy.....@.....B.....P.....D...P.....?..@. .....text..... ..`.data...0.....*.....@....rsrc..... .....@..@.reloc...,.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\A33B.exe.log

Process:	C:\Users\user\AppData\Local\Temp\A33B.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D

Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat

Process:	C:\Windows\explorer.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.227423502376633
Encrypted:	false
SSDEEP:	24:Yq6CUXyhm5lUmtQlbNdB6hm5VUmtQlz0Jahm5SUmtQlHZ6T06Mhm5vUmtQlbxdB8:YqDUXyclwbNdUcpwz0JacWwHZ6T06Mcb
MD5:	D9512E54D33D06E68E0C0D36726F7776
SHA1:	2E2ED852C188E0F96FCF861D7B73B8C479379845
SHA-256:	C70B840F192B885EF63C8426B0667EF175424A96DEC79A988C9525AD8E6997D2
SHA-512:	AAFCD49F2C87D4D43076CB4C1357FFAC9AB224ADBD4CEB06961755A0D6305D550090DDA34CAAA3C9B2700EF182CC9D6000BAB87A1A31D15A6A9F7565F60BA515
Malicious:	false
Reputation:	unknown
Preview:	{"RecentItems":[{"AppID":"Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim","PenUsageSec":15,"LastSwitchedLowPart":2360844864,"LastSwitchedHighPart":30747916,"PrePopulated":true},{"AppID":"Microsoft.WindowsMaps_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":2350844864,"LastSwitchedHighPart":30747916,"PrePopulated":true},{"AppID":"Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint","PenUsageSec":15,"LastSwitchedLowPart":2340844864,"LastSwitchedHighPart":30747916,"PrePopulated":true},{"AppID":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","PenUsageSec":15,"LastSwitchedLowPart":2330844864,"LastSwitchedHighPart":30747916,"PrePopulated":true},{"AppID":"Microsoft.Windows.Photos_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":2320844864,"LastSwitchedHighPart":30747916,"PrePopulated":true},{"AppID":"Microsoft.Getstarted_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":2310844864,"LastSwitchedHighPart":30747916,"PrePopulated":true}]}

C:\Users\user\AppData\Local\Temp\12C0.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254464
Entropy (8bit):	7.32436195105757
Encrypted:	false
SSDEEP:	3072:LRvnO9N2bPgOyL/dnBYWZf354wHGXobm/JRO0LDl8ABIx8VM6Q3DTNJ3nJWPfo3:1vnptyLFBYkmXF/DHFJw8VM93DDEPfo
MD5:	38E67B1288479162D6BC93EE31A90564
SHA1:	3457AE59AC2FDCF4B2013B4245EBEBFD22841196
SHA-256:	A2AE21D0E3746DD06AC2B1C69517DF60E3998D4D3DB47D655B1C01504BBA21AA
SHA-512:	76B931CE148CC722412C454ADAD5A22FE295E6A879E6491658E274D06FA46557810EB34285CD48537D749E0F819E8D9134F903C132A55592006DE2F44505E72B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE..L.....b.....r.....@.....\...P....p.....@.....p9..@.....text.. ..`.data.....@....rsrc.....p... .....@..@.reloc...'.....(.....@..B.....

C:\Users\user\AppData\Local\Temp\3046.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	722944
Entropy (8bit):	7.843693287624674
Encrypted:	false
SSDEEP:	12288:zUJFDhiQSO/bmqK1NIK6kxk7q4p/dn57k/x4omG1ZQHdt1AaQf8O:zQF0Qn6qQoTLdH76x1R1Z4AaQL
MD5:	46909DA148DE57B2D85591626AEDBD76
SHA1:	8000C3D7B0B33EAA538F8B0E09EFF0559AF06287
SHA-256:	0CA1867B6E512A1E78D8A00CECF4FDC09B665B31F9AF122C78EE4A1E5DE5A692
SHA-512:	C3A4C1392E9300C5A9255A8BEC4757D8244023F5353D693A9E7A1496DA92F1B90482F9201035AB07B669C228F8BEDBE467F5C54BFB8F4D50C90350B0F2076603
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 62%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Qn..Qn..Qn..O<..Mn..O<i..n..v...Vn..Qn...n..O<n.}n..O<~.Pn ..O<{.Pn..RichQn.....PE..L.....a.....6.....fy.....@.....B.....P.....D...P.....?..@. .....text..... ..`.data...0.....*.....@....rsrc..... .....@..@.reloc...,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\4113.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387584
Entropy (8bit):	6.881738348627874
Encrypted:	false
SSDEEP:	6144:x8DLMZy4voyHwQ+CADR/Qe/eEWajEcf4:CQDvfHwQgVQwVEcf
MD5:	B141BC58618C537917CC1DA179CBE8AB
SHA1:	C76D3F5EEAE9493E41A272A974B5DFEC5F4E4724
SHA-256:	FD999E4A07D8B3D95F9D9231FD496B0125B56094F1B03DDCA7A7B074C1D8C03E
SHA-512:	5C72F63124A394602A36A4F985E33A41E8159F54653F431C270B8F0FA8E13131517C31B497A936D5F5D3D27397F40FC7909EFC4BFD04C01BCCA7F306860C3114
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z...z...z...(j..z...({..z...(m..z.....z...z...z...(d..z...(z..z...(...z..Ric h.z.....PE..L...;..a.....@.....@.....)<.....a.....h,..@.....I..... .....text..... ..`.data...@.....@....guno.....N.....@..@.jofolo.F.....R.....@..@.nabog.....I.....@..@.rsrc.... a.....b...p.....@..@.reloc.."....@..B..... .....

C:\Users\user\AppData\Local\Temp\98D7.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3657728
Entropy (8bit):	7.795668090342615
Encrypted:	false
SSDEEP:	98304:8gleOA+U9OYPQAY0YdNa1rcO7B9elk44MRTVkVu:tleOA+oDP20YdNa1IM90YMRTm
MD5:	81A0ECC23B44DA5116D397C0A3104A05
SHA1:	01EFD55A04010EC4E7197BCAC7EC351BB8E5BF07
SHA-256:	3F59D2CF23B45B7F56563E85BF818F827F2607D12661FB438BCF031550EC0EC0
SHA-512:	CF0C87B4B5101898A48AB312CD1436E2738762EE74D1D77A29635053A373D5DFF237DA84A17DFE7897C7E99B919325FF8C47238A2FD06DFDB04F3D18F4A9718
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...?;.c.....#.....:.....@.....b..... .....-.d.....a.....^a.....8.+.0...@]a.8.....text...P..... ..`.rdata..b.....@.. @.data.....@....pdata..... .....@..@_RDATA.....@..@.vmp0... T.....`..`.vmp1...t.7.. *...7.....`..h.rsrc.....a..... .7.....@..@..... .....

C:\Users\user\AppData\Local\Temp\A33B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7722496
Entropy (8bit):	7.943852397063956
Encrypted:	false
SSDEEP:	196608:xmnP/F68J3FxrU93Eq3zPgSnbWOGGY7p:Y37RjqjPDbWhGY
MD5:	B328ABE938AE81E9382BD6858A6EE77F
SHA1:	EDBEBCBBEEDB642D906A5E96A1E76A1FB580A11C

SHA-256:	CB354C4E272DE841E4A2CC6D96C88C291A720487637EFF8075F6725896137DED
SHA-512:	5D9A58ACA575F68D872A7C9643207636CBE0E8B86644971C1E36DC1707A9694F5D5F2B32BD10565CB0EC27FB616A0D6B51EC5E602D86B3DCC538CCA80BE6E8 45
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\A33B.exe, Author: ditekSHen
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...l..c.....u.....u.. ....v...@.. .....@.v..... ..@.....H.u.S.....v..... v..... ....H.....text.....u.. ....u..... ..`.rsrc.....v.....u.....@..@.rel oc..... v.....u.....@..B.....u.....H.....u.\.....'....u.....0..._.....~.....(....,..(....~.....(....,..(....~.....(....,..(....~.....(....,.~.... ... .Z(....~....,r...pr...p.(...&..8....~.....o.....~.....o.....~.....o.....(.....~.....(.....~....r...p(....,.(....r...po.....(.....+)~....r1..p(....,..(....r...po....(.....(....(.....(.....(..... X..~....o....?....~....&*..0../.....s.....s.....s.....o......,

C:\Users\user\AppData\Local\Temp\D8D3.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	200192
Entropy (8bit):	7.034764103148747
Encrypted:	false
SSDEEP:	3072:8gJO/TK0wdrrseL/iyoWo5s1412e1YqsVf0cnas1pbzeVCTAaGtR:8gJsmFdEeLfoW1412toQas1XAvtR
MD5:	0CA939E14D58B13997144F0AF89ADEA9
SHA1:	65DD44DDE830E9CBAB5149369A333D4F6464E86D
SHA-256:	A2C60618D112DA73E9019312A77CD8CD78A4E924E128F21DC8410E012A510CD3
SHA-512:	FD9C6B5A9CD78AAC50443B44DFC46F5F60F17D1F3D858B7B85097D66EA703BB8491B63EBBA3A2F2C3A7869FDFBB1BF9F8A3A763B015E0886DA0526BE59309D FB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e...e...e.B....e.....e....e.....e...d.x.e.....e.....e.....e.Rich..e..... .....PE..L.....b.....>.....w.....@.....P.....4...@.....>..@..... .....text...~..... ..`.data.....8.....@....rsrc..... .....@..@.reloc...'.....(.....@..B..... ....

C:\Users\user\AppData\Local\Temp\E4.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	198656
Entropy (8bit):	7.0336896297722555
Encrypted:	false
SSDEEP:	3072:9SbOLZRNAmrLJhkdW75GZK926+oi75o0eEHSLVWE8:9Sbc5rLUd5Z76+J5xeEkVWE8
MD5:	29C3DE14DFFA53EDC7E690D0FC0ECCE2
SHA1:	B35F5F268762A950EB18741B4944DB7DB232DB00
SHA-256:	81AF8254226542C9E5538369E4643DB192DB7BC31817BBCF0931AA897B11CA84
SHA-512:	03E68667B3C8361860464F81E38A074E148A3A017405BA6D641901D0F1F887006DFEE326C8A7D868781C69DF162885FACB94223B2CCF656E88C1AAB62B4C456E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE.. L.....Vb.....>.....Or.....@.....l.....L...P.....@.....p9..@.....text. ....`.data.....8.....@....rsrc..... .....@..@.reloc..n'.....(.....@..B..... ....

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

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	200192
Entropy (8bit):	7.021128640275825

Encrypted:	false
SSDEEP:	3072:KGmOScBINJYW7LNxrWU5qJw5TN7Ow+CsfOaMqhpmx7OwSSZ+ER:KGmkIB7LTrwyd717OOrR
MD5:	3A452937E8A961C5E19974C2CBB4AFAA
SHA1:	6C8522AC545442F29B6A5A768FA9F0FC4A38A928
SHA-256:	DE5F535B0A84C65BB341EE58B72BDA0B75C18CD795EFF21A5318D0BFDAEE21BD
SHA-512:	C12172037F48F14394CD2D408DC2B31AD683C253B57EB807949F05E53AF95954BA8D10EBCBAD4B0562AB69D932F2D8463E4891350756170940054182A72D8252
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e...e...e.B....e.....e....e.....e.....e...d.x.e.....e.....e.....e.Rich..e..... .....PE..L.....~b.....>.....w.....@.....o.....P.....@...@.....>..@..... .....text...~..... ..`.data.....8.....@....rsrc..... .....@..@.reloc...'.....(.....@..B..... ....

C:\Users\user\AppData\Local\Temp\FB61.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	3847168
Entropy (8bit):	7.985609186180041
Encrypted:	false
SSDEEP:	98304:MSQ3/Y0ws5Zw/QJCZObVeCuMFWxrMKUs+mNXc:MSQPY/s5stsPDIoKUs+
MD5:	7E01B1A967FADD92B78A52411556C945
SHA1:	B8C9839599B8F721E05B68B2E9AFE81FB8FC5225
SHA-256:	696682568C05C3EA48ABA981D359133B72457417C8C10C27A80BDF83CCEC7B61
SHA-512:	BA4AC3BC16A6B71A4B7F564625C536AAC4C9F1C950B3D9604DFA6F61E37690B5A261857D007F85CCB059255CD837C29FFEB4410C5F87EB2F15839BEACA1AB4 7D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE.. L....;.b.....K.....Or.....@.....O.....w.:.....L...P.... M.....0O.....@.....9.....p9..@..... .....text..... ..`.data....}K.....8.....@....rsrc..... M.. ...H:.....@..@.reloc...J...0O..L...h:.....@..B..... ....

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

Process:	C:\Users\user\AppData\Local\Temp\A33B.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	3890176
Entropy (8bit):	7.902408557753204
Encrypted:	false
SSDEEP:	49152:8Pu803iSM2N7aUjjqpEbUS2qv5MQBsSY/b7KoiTFUgxylC42lVJpiU71PP:s12BEE4vqxMQzub7OTFUgxylqTiU7J
MD5:	3006B49F3A30A80BB85074C279ACC7DF
SHA1:	728A7A867D13AD0034C29283939D94F0DF6C19DF
SHA-256:	F283B4C0AD4A902E1CB64201742CA4C5118F275E7B911A7DAFDA1EF01B825280
SHA-512:	E8FC5791892D7F08AF5A33462A11D39D29B5E86A62CBF135B12E71F2FCAAA48D40D5E3238F64E17A2F126BCFB9D70553A02D30DC60A89F1089B2C1E7465105D D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 92%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...Bu.c.....&.....X;.....@.....;....!.;. ..`.. .....8.....9.....8.....;.....8.(.....D.8.....text.....`..`.data.....7.....7.....@. ...rdata.....8.....8.....@..@.pdata.....8.....8.....@..@.xdata.....8.....8.....@..@.bss....8....8.....idata.....8.....8.....@....CRT.... h.....8.....8.....@....tls.....9.....8.....@....rsrc.....9.....8.....@....reloc.....;.....Z;.....@..B..... .....

C:\Users\user\AppData\Local\Temp\db.dat

Process:	C:\Users\user\AppData\Local\Temp\pliu.exe
File Type:	data

Category:	dropped
Size (bytes):	571230
Entropy (8bit):	7.964582338724255
Encrypted:	false
SSDEEP:	12288:FV1e0UgkVT6ZT+3JCnoxgLgoCXwbePLJrH8fwpL:FV1edgkV8T0CnoxZ4ePLJTMwpL
MD5:	30D5F615722D12FDDA4F378048221909
SHA1:	E94E3E3A6FAE8B29F0F80128761AD1B69304A7EB
SHA-256:	B7CB464CD0C61026EC38D89C0A041393BC9369E217303677551EEC65A09D2628
SHA-512:	A561A224D7228EC531A966C7DBD6BC88138E2F4A1C8112E5950644F69BF3A43B1E87E03BC1B4FD5E9CA071B5A9353B18697573404602CCD51F2946FAF95144C
Malicious:	false
Reputation:	unknown
Preview:	P,..Hh.j...?...O}3..8v,)cml.T/.....V.r.....n.?y..oz#V.....N.{.....!....Y."..)v.T.....Ub.V..*.)..8..,.%.{4.yWrA.a36&..,...V...l9.y....39.y...wW.j.ox.....l..;..%..p.b..>..j.....j..awT..r...j....o./ .7...,=uk..i../h..j*j.P.j..?.-X.k..R}.j.5.b-F.k..c.....j...j..Q?...).qe.....,o'k.....j.J..))O.....k..\.....u,..k...,..k....k...tOT.X.jXe-.k..7.k...83U.....%..o.....Y%.....7.F.(j...KP..l..j..y...o..no... ...z.....u/..DJP.e+.Dj..Z....k.....j$T.X.j[..`....o....k{..2|6...H.....c%.....z.....~^..j.-s.....o.-.....6.L.`.j.-s.....i|..y.Q'....k...}FT.X.jY..Y....o.....y..=|6..%..z/.....s....>.j.-s.k../.:.....> |/...h...2/..R..-.....k....9.y.....j.6Z.j.o....l&..%.UD..`....&..t>".6g..j,..../W=..5...n.....X..h>.k..'...|/h..jfDX.S...`&*...Y....)U]bc[.....'(..l..+....b.i....[...lf!S...r.....i.....Q^..*.....aeddT.`.'....*. [.h....e...?>....n....5.....-..j..T..ow.....k....-...k16.+i(~..L....j,...c.L./w=j...~./

C:\Users\user\AppData\Local\Temp\db.dll

Process:	C:\Users\user\AppData\Local\Temp\pliu.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	5.2806602069772195
Encrypted:	false
SSDEEP:	384:XehpWSsdMRgTh4QPt0RaYaGCp9FclU2sSadM7yjR+Lcuczw0RoR/5rdy7olDJfUw:ipW6+grtlU2v7yGLwwouflpZ2tVtkTF
MD5:	1B20E998D058E813DFC515867D31124F
SHA1:	C9DC9C42A748AF18AE1A8C882B90A2B9E3313E6F
SHA-256:	24A53033A2E89ACF65F6A5E60D35CB223585817032635E81BF31264EB7DABD00
SHA-512:	79849FBDB9A9E7F7684B570D14662448B093B8AA2B23DFD95856DB3A78FAF75A95D95C51B8AA8506C4FBECFFEBCC57CD153DDA38C830C05B8CD38629FAE67 C6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 42%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.....7.....Rich..... .....PE..L.....c.....!.....p...P.....>W.....@..$...<.....4.....0...@..... .....text....g.....p..... ..`.rdata..... .....@..@.data.....@....rsrc.....@..@.reloc.....@..B..... ....

C:\Users\user\AppData\Local\Temp\llpb1133.exe

Process:	C:\Users\user\AppData\Local\Temp\A33B.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3657728
Entropy (8bit):	7.795668090342615
Encrypted:	false
SSDEEP:	98304:8gleOA+U9OYPQAY0YdNa1rcO7B9elk44MRTVkVu:tleOA+oDP20YdNa1IM90YMRTm
MD5:	81A0ECC23B44DA5116D397C0A3104A05
SHA1:	01EFD55A04010EC4E7197BCAC7EC351BB8E5BF07
SHA-256:	3F59D2CF23B45B7F56563E85BF818F827F2607D12661FB438BCF031550EC0EC0
SHA-512:	CF0C87B4B5101898A48AB312CD1436E2738762EE74D1D77A29635053A373D5DFF237DA84A17DFE7897C7E99B919325FF8C47238A2FD06DFDB04F3D18F4A9718
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...?;.c.....#.....:.....@.....b..... .....-.d.....a.....^a.....8.+.0...@]a.8.....text...P..... ..`.rdata..b.....@.. @.data.....@....pdata..... .....@..@_RDATA.....@..@.vmp0... T.....`..`.vmp1...t.7.. *...7.....`..h.rsrc.....a..... .7.....@..@..... .....

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

Process:	C:\Users\user\AppData\Local\Temp\A33B.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	163840
Entropy (8bit):	5.025420345934772
Encrypted:	false
SSDEEP:	768:Dz6Gwy7E2OreQTFwf32MVnZbmQNLk7mtlqWGG9Lto8hecAD9Grp/2mPYHfMDy4If:ZyrRqf32MXb38mSzuhPAK/23kTktX6
MD5:	B9363486500E209C05F97330226BBF8A
SHA1:	BFE2D0072D09B30EC66DEE072DDE4E7AF26E4633
SHA-256:	01138F2318E59E1FE59F1EB7DE3859AF815EBF9A59AAE1084C1A97A99319EE35
SHA-512:	6D06E5BAEAB962D85B306C72F39A82E40E22EB889867C11C406A069011155CB8901BF021F48EFC98FD95340BE7E9609FC11F4E24FC322DBF721E610120771534
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 85%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../2N.N\..N\..N\...!..N\...1..N\.uA...N\...2..N\.uA...N\..N]..N\.....N\. ..$..N\.Rich.N\.....PE..L.....c.....)..... .....@..... .....<....@...E.....`.....@.... ..... .....text..... ..`.rdata...+.....0.....@..@.data...8"..... .....@....rsrc....P...@...P...0.....@..@.....

C:\Users\user\AppData\Roaming\jhevwvt

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	198656
Entropy (8bit):	7.0336896297722555
Encrypted:	false
SSDEEP:	3072:9SbOLZRNAmrLJhkdW75GZK926+oi75o0eEHSLVWE8:9Sbc5rLUd5Z76+J5xeEkVWE8
MD5:	29C3DE14DFFA53EDC7E690D0FC0ECCE2
SHA1:	B35F5F268762A950EB18741B4944DB7DB232DB00
SHA-256:	81AF8254226542C9E5538369E4643DB192DB7BC31817BBCF0931AA897B11CA84
SHA-512:	03E68667B3C8361860464F81E38A074E148A3A017405BA6D641901D0F1F887006DFEE326C8A7D868781C69DF162885FACB94223B2CCF656E88C1AAB62B4C456E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE.. L.....Vb.....>.....Or.....@.....l.....L...P.....@.....p9..@.....text. ....`.data.....8.....@....rsrc..... .....@..@.reloc..n'.....(.....@..B.....

C:\Users\user\AppData\Roaming\sievwvt

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	198144
Entropy (8bit):	7.041743566438781
Encrypted:	false
SSDEEP:	3072:hlrXO4DHzvDSyUPLoigWo351k/Z2N/BbET2tOWIbq0ES4vy3DwHkEforb:/rXbT0PL1g5W2pZETbWIULvy3UHkEQ
MD5:	17A74A0281CEFB5D9C29022FBC79981A
SHA1:	D88585C6C9488B6D28B71DD0659EDB8649E32DCA
SHA-256:	2814B2A02771E2D16CE2EFB1586D8623B54B50D6E1C8DFA9AB2BBF54AB8B249D
SHA-512:	E53AE73584F2DE67589AB0354F4D7CF16053109E4AC458E962C17EE5DFBE65BFDCD05553574E839EBCF2925A130D75BC14994B908A2928F017776D43A7BFDD5 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE.. L.....b.....<....._r.....@.....\...P.....@.....p9..@.....text. ....`.data.....6.....@....rsrc..... .....@..@.reloc..n'.....(.....@..B.....

C:\Users\user\AppData\Roaming\sievwvt: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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.041743566438781
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:	file.exe
File size:	198144
MD5:	17a74a0281cefb5d9c29022fbc79981a
SHA1:	d88585c6c9488b6d28b71dd0659edb8649e32dca
SHA256:	2814b2a02771e2d16ce2efb1586d8623b54b50d6e1c8dfa9ab2bbf54ab8b249d
SHA512:	e53ae73584f2de67589ab0354f4d7cf16053109e4ac458e962c17ee5dfbe65bfdcd05553574e839ebcf2925a130d75bc14994b908a2928f017776d43a7bfdd55
SSDEEP:	3072:hlrXO4DHzvDSyUPLoigWo351k/Z2N/BbET2tOWIbq0ES4vy3DwHkEforb:/rXbT0PL1g5W2pZETbWIULvy3UHkEQ
TLSH:	7514CF3336D0F072C96B55305834DBA57ABFB8319675899B7BA807AE5F303E06336252
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w.....a.....q.....t.....Rich.....PE..L.....b.....

File Icon

Icon Hash:	70d0eeeaeacae2dd

Static PE Info

General

Entrypoint:	0x40725f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F4FA9D [Thu Aug 11 12:48:29 2022 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:	87e1f4e32d01d5a52e605f27fd138118

Entrypoint Preview
Instruction
call 00007F1A14C0985Ch
jmp 00007F1A14C031CEh
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F1A14C03376h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F1A14C033A0h
test ecx, 00000003h
jne 00007F1A14C03341h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F1A14C0333Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F1A14C03384h
test ah, ah
je 00007F1A14C03376h
test eax, 00FF0000h
je 00007F1A14C03365h
test eax, FF000000h
je 00007F1A14C03354h
jmp 00007F1A14C0331Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]

Instruction
sub eax, ecx
ret
cmp ecx, dword ptr [0042C2B0h]
jne 00007F1A14C03354h
rep ret
jmp 00007F1A14C0984Ch
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0042C2B0h]

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1875c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15a000	0x1ee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15c000	0xf08	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1240	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3970	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1f4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1830a	0x18400	False	0.5318943298969072	COM executable for DOS	6.3718422303346625	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x13f3b0	0x13600	False	0.9458291330645161	data	7.8477215097242885	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x15a000	0x1ee8	0x2000	False	0.610595703125	data	5.7865329961947936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15c000	0x276e	0x2800	False	0.32138671875	data	3.342680269338327	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	Tibet
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	Nepal
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	India
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	Tibet
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	Nepal
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	India
RT_STRING	0x15bd90	0x4e	data	Tibetan	Tibet
RT_STRING	0x15bd90	0x4e	data	Tibetan	Nepal
RT_STRING	0x15bd90	0x4e	data	Tibetan	India
RT_STRING	0x15bde0	0x50	data	Tibetan	Tibet
RT_STRING	0x15bde0	0x50	data	Tibetan	Nepal
RT_STRING	0x15bde0	0x50	data	Tibetan	India
RT_STRING	0x15be30	0xb6	data	Tibetan	Tibet
RT_STRING	0x15be30	0xb6	data	Tibetan	Nepal
RT_STRING	0x15be30	0xb6	data	Tibetan	India
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	Tibet
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	Nepal
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	India
RT_VERSION	0x15bb38	0x258	data		

Imports

DLL	Import
KERNEL32.dll	RequestWakeupLatency, CreateFileA, FindActCtxSectionStringA, WriteConsoleInputA, ClearCommBreak, WriteFile, FindFirstVolumeMountPointW, CreateDirectoryExA, LocalSize, WaitForMultipleObjects, ReadConsoleInputA, GetProcessId, FreeUserPhysicalPages, WriteConsoleOutputAttribute, DebugActiveProcessStop, GetLocaleInfoW, GetProcAddress, LocalAlloc, GetCommandLineW, GetBinaryTypeW, InterlockedExchange, OpenMutexW, GetConsoleTitleA, SearchPathA, FreeConsole, EndUpdateResourceA, GetLastError, GetProfileSectionA, SetConsoleCursorInfo, GetConsoleAliasW, CreateSemaphoreA, GlobalFlags, GetConsoleAliasesLengthA, FindResourceW, SetVolumeMountPointW, GetModuleHandleW, HeapAlloc, GetComputerNameA, GetCurrentProcessId, CreateNamedPipeA, EnumResourceLanguagesA, SetHandleInformation, _hwrite, CreateActCtxA, DeleteVolumeMountPointA, MoveFileWithProgressA, AddRefActCtx, WritePrivateProfileStringA, GetUserDefaultLangID, QueryMemoryResourceNotification, WaitForSingleObject, GetLongPathNameW, InterlockedDecrement, VerifyVersionInfoA, EnumCalendarInfoW, FindNextFileW, EnumTimeFormatsA, SetLastError, SetCriticalSectionSpinCount, WritePrivateProfileSectionA, LoadLibraryA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, RtlUnwind, HeapFree, DeleteFileA, GetStartupInfoW, GetModuleHandleA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, HeapReAlloc, Sleep, ExitProcess, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetStartupInfoA, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapSize, InitializeCriticalSectionAndSpinCount, WideCharToMultiByte, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, GetConsoleCP, GetConsoleMode, FlushFileBuffers, SetFilePointer, CloseHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle
USER32.dll	GetComboBoxInfo
GDI32.dll	GetTextFaceW

Possible Origin

Language of compilation system	Country where language is spoken	Map
Tibetan	Tibet	
Tibetan	Nepal	

Language of compilation system	Country where language is spoken	Map
Tibetan	India	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:44:46.600966930 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.619282007 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.619430065 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.619829893 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.619877100 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.638236046 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.638267040 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.768254995 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.768284082 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.768481016 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.776756048 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.776806116 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.794220924 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.794245958 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862286091 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862343073 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862392902 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862442970 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862492085 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862540007 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862567902 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.862637997 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862685919 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.862756968 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.862935066 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.862965107 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.863015890 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.863063097 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.863106012 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.863106012 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.863171101 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.906440973 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906534910 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906580925 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906630039 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906687021 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.906748056 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.906778097 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906893015 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906944036 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.906955957 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.906991959 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.907037973 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.907042027 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.907881021 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.907934904 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.907979965 CET	80	49697	188.114.96.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:44:46.908025980 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.908029079 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.908057928 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.908618927 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.908668995 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.908714056 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.908740044 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.908760071 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.908766985 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.909514904 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.909563065 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.909589052 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.909609079 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.909656048 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.909728050 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.910384893 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.910444021 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.910479069 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.910597086 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.955492020 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955538988 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955564976 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955588102 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955683947 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.955744028 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955765963 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.955770016 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955796957 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955821037 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.955846071 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.955873966 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.956593037 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.956629992 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.956656933 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.956681013 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.956685066 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.956732035 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.957412004 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.957448006 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.957499981 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.957518101 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.957545042 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.957988977 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.958277941 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.958318949 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.958343983 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.958369017 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.958388090 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.958425045 CET	49697	80	192.168.2.3	188.114.96.3
Feb 7, 2023 19:44:46.959188938 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.959223032 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.959249020 CET	80	49697	188.114.96.3	192.168.2.3
Feb 7, 2023 19:44:46.959274054 CET	80	49697	188.114.96.3	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 19:44:46.530975103 CET	192.168.2.3	8.8.8.8	0xd71e	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:01.171063900 CET	192.168.2.3	8.8.8.8	0x5d0	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:03.833204985 CET	192.168.2.3	8.8.8.8	0xf00f	Standard query (0)	flytourchip.com.br	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:04.918548107 CET	192.168.2.3	8.8.8.8	0xee27	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:05.436633110 CET	192.168.2.3	8.8.8.8	0x93ab	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:34.826117039 CET	192.168.2.3	8.8.8.8	0x29e1	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:41.806687117 CET	192.168.2.3	8.8.8.8	0xfc92	Standard query (0)	xv.yxzgamen.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:47.377264977 CET	192.168.2.3	8.8.8.8	0x36ee	Standard query (0)	iueg.aappatey.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:53.661890984 CET	192.168.2.3	8.8.8.8	0x3dbb	Standard query (0)	xv.yxzgamen.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:54.348076105 CET	192.168.2.3	8.8.8.8	0xe0b6	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:54.582577944 CET	192.168.2.3	8.8.8.8	0x6340	Standard query (0)	siaoheg.aappatey.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.575400114 CET	192.168.2.3	8.8.8.8	0xa3e2	Standard query (0)	perficut.at	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:56.694607973 CET	192.168.2.3	8.8.8.8	0x2fbe	Standard query (0)	perficut.at	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.098745108 CET	192.168.2.3	8.8.8.8	0xfe0f	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.370901108 CET	192.168.2.3	8.8.8.8	0xe71a	Standard query (0)	perficut.at	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:44:46.554482937 CET	8.8.8.8	192.168.2.3	0xd71e	No error (0)	potunulit.org		188.114.96.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:44:46.554482937 CET	8.8.8.8	192.168.2.3	0xd71e	No error (0)	potunulit.org		188.114.97.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:01.191075087 CET	8.8.8.8	192.168.2.3	0x5d0	No error (0)	potunulit.org		188.114.96.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:01.191075087 CET	8.8.8.8	192.168.2.3	0x5d0	No error (0)	potunulit.org		188.114.97.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:04.151479006 CET	8.8.8.8	192.168.2.3	0xf00f	No error (0)	flytourchip.com.br		158.69.96.67	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:04.941478014 CET	8.8.8.8	192.168.2.3	0xee27	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:05.458060026 CET	8.8.8.8	192.168.2.3	0x93ab	No error (0)	potunulit.org		188.114.96.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:05.458060026 CET	8.8.8.8	192.168.2.3	0x93ab	No error (0)	potunulit.org		188.114.97.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:34.843812943 CET	8.8.8.8	192.168.2.3	0x29e1	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:45:34.843812943 CET	8.8.8.8	192.168.2.3	0x29e1	No error (0)	star-mini.c10r.facebook.com		157.240.253.35	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:41.829817057 CET	8.8.8.8	192.168.2.3	0xfc92	No error (0)	xv.yxzgamen.com		188.114.97.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:41.829817057 CET	8.8.8.8	192.168.2.3	0xfc92	No error (0)	xv.yxzgamen.com		188.114.96.3	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:45:47.396763086 CET	8.8.8.8	192.168.2.3	0x36ee	No error (0)	iueg.aappatey.com		45.66.159.142	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:53.683685064 CET	8.8.8.8	192.168.2.3	0x3dbb	No error (0)	xv.yxzgamen.com		188.114.97.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:53.683685064 CET	8.8.8.8	192.168.2.3	0x3dbb	No error (0)	xv.yxzgamen.com		188.114.96.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:54.369381905 CET	8.8.8.8	192.168.2.3	0xe0b6	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:54.603955984 CET	8.8.8.8	192.168.2.3	0x6340	No error (0)	siaoheg.aappatey.com		45.66.159.142	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		195.158.3.162	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		189.156.154.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		189.143.172.107	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		190.219.54.242	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		190.117.75.91	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		222.236.49.123	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:55.803621054 CET	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	perficut.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		190.219.54.242	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		190.117.75.91	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		222.236.49.123	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		195.158.3.162	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		189.156.154.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:57.166321993 CET	8.8.8.8	192.168.2.3	0x2fbe	No error (0)	perficut.at		189.143.172.107	A (IP address)	IN (0x0001)	false

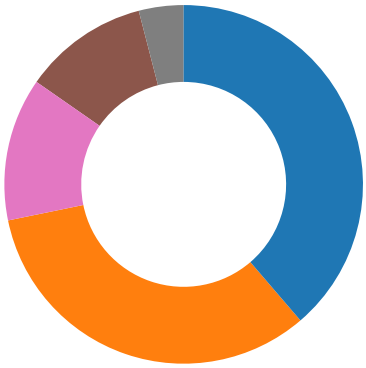
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:45:58.118758917 CET	8.8.8.8	192.168.2.3	0xfe0f	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		189.156.154.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		189.143.172.107	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		190.219.54.242	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		190.117.75.91	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		222.236.49.123	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:45:58.845731974 CET	8.8.8.8	192.168.2.3	0xe71a	No error (0)	perficut.at		195.158.3.162	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- flytourchip.com.br
- api.2ip.ua
- www.facebook.com
- xv.yxzgamen.com
- qmxjpgcre.net
  - potunulit.org
- mxhagj.org
- idkcje.org
- dxwvikrtgo.org
- usbhmmnst.net
- nqnoakwgow.net
- scuexnvs.com
- tmafbpv.org
- 77.73.134.27
- fjgurrg.com
- yxysrc.org
- vrtsdpwuux.com
- saeqmrs.com
- auuuhpc.com
- tpniggi.com
- fxqslbplw.net
- fixgfsjkdd.org
- mhfgwrr.org
- 62.204.41.134
- iueg.aappatey.com
- siaoheg.aappatey.com
- esvui.net
  - perficut.at
- xacanotyi.org
- coaqka.com

Statistics

Behavior



- file.exe
- explorer.exe
- 4113.exe
- sievwvt
- 3046.exe
- A33B.exe
- 3046.exe
- 98D7.exe
- E4.exe
- ECFB.exe
- D8D3.exe
- llpb1133.exe
- icacls.exe
- WerFault.exe
- pliu.exe
- conhost.exe
- XandETC.exe
- 3046.exe
- 3046.exe
- 3046.exe
- pliu.exe
- conhost.exe
- 3046.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: **4356**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:43:58
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	198144 bytes
MD5 hash:	17A74A0281CEFB5D9C29022FBC79981A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.313442333.0000000000926000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.313241208.0000000000680000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.313394418.0000000000851000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.313394418.0000000000851000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.313299344.0000000000720000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.313299344.0000000000720000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **4356**

General

Target ID:	4
Start time:	19:44:10
Start date:	07/02/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sievwvt	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5792156	CopyFileW
C:\Users\user\AppData\Roaming\sievwvt\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5792156	CopyFileW
C:\Users\user\AppData\Local\Temp\4113.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\4113.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\3046.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\3046.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\A33B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\A33B.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\98D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\98D7.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\E4.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\ECFB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\ECFB.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\D8D3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5792BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\D8D3.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5792C7A	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jhevwvt	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	58A1FE2	CopyFileW
C:\Users\user\AppData\Local\Temp\FB61.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	58A2A42	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FB61.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	58A2B06	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	5792167	DeleteFileW
C:\Users\user\AppData\Roaming\sievwvt:Zone.Identifier	success or wait	1	57921B2	DeleteFileW
C:\Users\user\AppData\Local\Temp\4113.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\3046.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\A33B.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\98D7.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\E4.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\ECFB.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\D8D3.tmp	success or wait	1	5792BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\E4.exe	success or wait	1	58A1FF3	DeleteFileW
C:\Users\user\AppData\Local\Temp\FB61.tmp	success or wait	1	58A2A4B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sievwvt	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 42 fd 73 fd fd fd fd 70 fd fd fd fd fd 66 fd fd fd fd 08 fd fd fd fd fd fd fd 77 fd fd fd 61 fd fd fd fd 71 fd fd fd fd fd 74 fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$BspfwaqtRichPE Lb	success or wait	2	5792156	CopyFileW
C:\Users\user\AppData\Roaming\sievwvt:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	5792156	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4113.exe	0	387584	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 1b fd fd fd 7a fd fd fd 7a fd fd fd 7a fd fd fd 28 6a fd fd 7a fd fd fd 28 7b fd fd 7a fd fd fd 28 6d fd fd 7a fd fd bc fd fd fd 7a fd fd fd 7a fd fd fd 7a fd fd fd 28 64 fd fd 7a fd fd fd 28 7a fd fd 7a fd fd fd 28 7f fd fd 7a fd fd 52 69 63 68 fd 7a fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 3b fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$zzz(jz({z(mzzz z(dz(zz(zRichzPEL;a	success or wait	1	5792CA0	WriteFile
C:\Users\user\AppData\Local\Temp\3046.exe	0	722944	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 15 0f fd fd 51 6e fd fd 51 6e fd fd 51 6e fd fd 4f 3c 7f fd 4d 6e fd fd 4f 3c 69 fd 2e 6e fd fd 76 fd fd fd 56 6e fd fd 51 6e fd fd fd 6e fd fd 4f 3c 6e fd 7d 6e fd fd 4f 3c 7e fd 50 6e fd fd 4f 3c 7b fd 50 6e fd fd 52 69 63 68 51 6e fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$QnQnQnO<MnO<i. nvVnQnnO<n}nO<~PnO<{PnRichQnPELa	success or wait	1	5792CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A33B.exe	0	7722496	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6c fd fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 75 00 00 08 00 00 00 00 00 00 fd fd 75 00 00 20 00 00 00 00 76 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 76 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELlcuu v@ @v@	success or wait	1	5792CA0	WriteFile
C:\Users\user\AppData\Local\Temp\98D7.exe	0	3657728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 3f 3b fd 63 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 0e 1d 00 fd 0e 00 00 fd 04 00 00 00 00 00 19 fd 3a 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 62 00 00 04 00 00 00 00 00 00 02 00 20 fd 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd?;c#:@b	success or wait	1	5792CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E4.exe	0	198656	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 42 fd 73 fd fd fd fd 70 fd fd fd fd fd 66 fd fd fd fd fd 08 fd fd fd fd fd fd fd 77 fd fd fd 61 fd fd fd fd 71 fd fd fd fd 74 fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 11 fd 56 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$BspfwaqtRichPELVb	success or wait	1	5792CA0	WriteFile
C:\Users\user\AppData\Local\Temp\ECFB.exe	0	200192	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 0b fd fd fd 65 fd fd fd 65 fd fd fd 65 fd 42 fd fd fd fd 65 fd fd fd fd fd 65 fd fd c2 fd 65 fd fd 08 1e fd fd fd 65 fd fd fd 64 fd 78 fd 65 fd fd fd fd fd 65 fd fd fd fd fd 65 fd fd fd fd fd fd 65 fd 52 69 63 68 fd fd 65 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 17 7e 62 00 00 00	MZ@!L!This program cannot be run in DOS mode.$eeeBeeeedxeeeeRichePEL~b	success or wait	1	5792CA0	WriteFile
C:\Users\user\AppData\Local\Temp\D8D3.exe	0	200192	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 0b fd fd fd 65 fd fd fd 65 fd fd fd 65 fd 42 fd fd fd fd 65 fd fd fd fd fd 65 fd fd c2 fd 65 fd fd 08 1e fd fd fd 65 fd fd fd 64 fd 78 fd 65 fd fd fd fd fd 65 fd fd fd fd fd 65 fd fd fd fd fd fd 65 fd 52 69 63 68 fd fd 65 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 07 62 00 00 00	MZ@!L!This program cannot be run in DOS mode.$eeeBeeeedxeeeeRichePELb	success or wait	1	5792CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jhevwvt	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 42 fd 73 fd fd fd fd 70 fd fd fd fd fd 66 fd fd fd fd fd 08 fd fd fd fd fd fd fd 77 fd fd fd 61 fd fd fd fd 71 fd fd fd fd 74 fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 11 fd 56 62 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$BspfwaqtRichPELVb	success or wait	2	58A1FE2	CopyFileW
C:\Users\user\AppData\Local\Temp\FB61.exe	0	3847168	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 42 fd 73 fd fd fd fd 70 fd fd fd fd fd 66 fd fd fd fd fd 08 fd fd fd fd fd fd fd 77 fd fd fd 61 fd fd fd fd 71 fd fd fd fd 74 fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 3b fd 62 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$BspfwaqtRichPEL;b	success or wait	1	58A2B2C	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: 4113.exe PID: **4968**, Parent PID: **3452**

General

Target ID:	11
Start time:	19:44:46
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\4113.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\4113.exe
Imagebase:	0x400000
File size:	387584 bytes
MD5 hash:	B141BC58618C537917CC1DA179CBE8AB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.604551133.0000000000550000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.605642320.00000000007C6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 82%, ReversingLabs
Reputation:	moderate

Analysis Process: sievwvt PID: **3176**, Parent PID: **1080**

General

Target ID:	12
Start time:	19:44:47
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\sievwvt
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\sievwvt
Imagebase:	0x400000
File size:	198144 bytes
MD5 hash:	17A74A0281CEFB5D9C29022FBC79981A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 49%, ReversingLabs
Reputation:	low

Analysis Process: 3046.exe PID: **3680**, Parent PID: **3452**

General

Target ID:	13
Start time:	19:44:47
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\3046.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3046.exe
Imagebase:	0x400000
File size:	722944 bytes
MD5 hash:	46909DA148DE57B2D85591626AEDBD76
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000D.00000002.396738460.000000000222E000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000D.00000002.396916881.0000000002350000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000D.00000002.396916881.0000000002350000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 62%, ReversingLabs
Reputation:	low

Analysis Process: A33B.exe PID: 3776, Parent PID: 3452

General

Target ID:	14
Start time:	19:44:59
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\A33B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A33B.exe
Imagebase:	0x7b0000
File size:	7722496 bytes
MD5 hash:	B328ABE938AE81E9382BD6858A6EE77F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\A33B.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\llpb1133.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\pliu.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\XandETC.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\A33B.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\llpb1133.exe	0	3657728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 3f 3b fd 63 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 0e 1d 00 fd 0e 00 00 fd 04 00 00 00 00 00 19 fd 3a 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 62 00 00 04 00 00 00 00 00 00 02 00 20 fd 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd?;c#:@b	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pliu.exe	0	163840	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 2f 32 4e fd 4e 5c 1d fd 4e 5c 1d fd 4e 5c 1d fd fd 21 1d fd 4e 5c 1d fd fd 31 1d fd 4e 5c 1d 75 41 03 1d fd 4e 5c 1d fd fd 32 1d fd 4e 5c 1d 75 41 01 1d fd 4e 5c 1d fd 4e 5d 1d fd 4e 5c 1d fd fd 2e 1d fd 4e 5c 1d fd fd 24 1d fd 4e 5c 1d 52 69 63 68 fd 4e 5c 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 25 fd 63 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$/2NN\N\N\!N\1N\uAN\2N\uAN\N]N\.N\$N\RichN\PELc	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\XandETC.exe	0	3890176	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 42 75 fd 63 00 00 00 00 00 00 00 00 fd 00 2e 02 0b 02 02 26 00 fd 00 00 00 58 3b 00 00 0e 00 00 fd 14 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 3b 00 00 04 00 00 21 fd 3b 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdBuc.&X;@;!;`	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\A33B.exe.log	0	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile

Analysis Process: 3046.exe PID: **5672**, Parent PID: **3680**

General

Target ID:	15
Start time:	19:45:02
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\3046.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3046.exe
Imagebase:	0x400000
File size:	722944 bytes
MD5 hash:	46909DA148DE57B2D85591626AEDBD76
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000F.00000002.467843881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000F.00000002.467843881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000F.00000002.467843881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000F.00000002.467843881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	411F94	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	412052	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 15 0f fd fd 51 6e fd fd 51 6e fd fd 51 6e fd fd 4f 3c 7f fd 4d 6e fd fd 4f 3c 69 fd 2e 6e fd fd 76 fd fd fd 56 6e fd fd 51 6e fd fd fd 6e fd fd 4f 3c 6e fd 7d 6e fd fd 4f 3c 7e fd 50 6e fd fd 4f 3c 7b fd 50 6e fd fd 52 69 63 68 51 6e fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$QnQnQnO<MnO<i. nvVnQnnO<n}nO<~PnO<{PnRichQnPELa	success or wait	3	412052	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SysHelper	expand unicode	"C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart	success or wait	1	4120F9	RegSetValueExW

Analysis Process: 98D7.exe PID: **5352**, Parent PID: **3452**

General

Target ID:	16
Start time:	19:45:02
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\98D7.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\98D7.exe
Imagebase:	0x140000000
File size:	3657728 bytes
MD5 hash:	81A0ECC23B44DA5116D397C0A3104A05
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 77%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	6	1400DA971	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	84	1400DA971	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	6	1400DA971	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	0	100	success or wait	6	140029FBB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	0	4096	success or wait	6	140029FBB	ReadFile

Analysis Process: E4.exe PID: **2096**, Parent PID: **3452**

General

Target ID:	17
Start time:	19:45:04
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\E4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E4.exe
Imagebase:	0x400000
File size:	198656 bytes
MD5 hash:	29C3DE14DFFA53EDC7E690D0FC0ECCE2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000011.00000002.443553763.0000000000640000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000011.00000002.444263115.0000000000816000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.443874552.00000000007E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000011.00000002.443874552.00000000007E0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.444700260.00000000021E1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000011.00000002.444700260.00000000021E1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: ECFB.exe PID: **996**, Parent PID: **3452**

General

Target ID:	18
Start time:	19:45:05
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\ECFB.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\ECFB.exe
Imagebase:	0x400000
File size:	200192 bytes
MD5 hash:	3A452937E8A961C5E19974C2CBB4AFAA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000012.00000002.483535048.0000000000726000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000012.00000002.483475283.00000000006D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 56%, ReversingLabs

Analysis Process: D8D3.exe PID: **5128**, Parent PID: **3452**

General

Target ID:	19
Start time:	19:45:05
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\D8D3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D8D3.exe
Imagebase:	0x400000
File size:	200192 bytes
MD5 hash:	0CA939E14D58B13997144F0AF89ADEA9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.441885976.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.462471829.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.465231730.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.511550380.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.514324898.000000000087C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.517099850.0000000000874000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.464907460.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.464370990.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.462319085.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.441770993.000000000083A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.464693455.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.441770993.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.444370287.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000013.00000003.446299900.000000000087E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	408F1A	HttpSendRequestW
C:\Users\user\AppData\LocalLow\nss3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	409637	CreateFileW
C:\Users\user\AppData\LocalLow\msvcp140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	409637	CreateFileW
C:\Users\user\AppData\LocalLow\vcruntime140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	409637	CreateFileW
C:\Users\user\AppData\LocalLow\mozglue.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	409637	CreateFileW
C:\Users\user\AppData\LocalLow\freebl3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	409637	CreateFileW
C:\Users\user\AppData\LocalLow\softokn3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	409637	CreateFileW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\LocalLow\sqlite3.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>sequential only | synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>409637</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\10PkIt2V82WR</td><td>read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write</td><td>device</td><td>sequential only | non directory file</td><td>success or wait</td><td>1</td><td>402E0A</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\cdE656z8QTF7</td><td>read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write</td><td>device</td><td>sequential only | synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>4032CF</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\2KyP65ecp6T3</td><td>read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write</td><td>device</td><td>sequential only | synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>403C0E</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\LocalLow\432zCWSnwm1N</td><td>read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write</td><td>device</td><td>sequential only | synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>40380C</td><td>CopyFileW</td></tr>
</table>

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\10PkIt2V82WR	success or wait	1	40308D	DeleteFileW
C:\Users\user\AppData\LocalLow\cdE656z8QTF7	success or wait	1	403606	DeleteFileW
C:\Users\user\AppData\LocalLow\2KyP65ecp6T3	success or wait	1	403D40	DeleteFileW
C:\Users\user\AppData\LocalLow\432zCWSnwm1N	success or wait	1	403ADD	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\nss3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 26 05 00 00 00 00 00 fd 01 15 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd fd 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 21 1d 00 5c fd 00 00 54 fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@	success or wait	998	40965B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\msvcp140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	220	40965B	WriteFile
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd 0a fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 28 fd 5b 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["	success or wait	40	40965B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\mozglue.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 fd 2f 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 fd fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd fd 08 00 63 51 00 00 10 0e 09 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,	success or wait	307	40965B	WriteFile
C:\Users\user\AppData\LocalLow\freebl3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 fd 1f 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 fd 2c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4 ,S,	success or wait	335	40965B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \softokn3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 fd fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 fd fd 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw	success or wait	125	40965B	WriteFile
C:\Users\user\AppData\LocalLow \sqlite3.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 fd 2c 62 00 76 0e 00 fd 13 00 00 fd 00 06 21 0b 01 02 19 00 0c 0b 00 00 fd 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 fd 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 1d 11 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 0c 00 6e 2a 00	MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n*	success or wait	537	40965B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \10PkIt2V82WR	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 5b 35 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5	success or wait	1	402E0A	CopyFileW
C:\Users\user\AppData\LocalLow \cdE656z8QTF7	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 11 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5g$	success or wait	1	4032CF	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \2KyP65ecp6T3	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	403C0E	CopyFileW
C:\Users\user\AppData\LocalLow \432zCWSnwm1N	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	40380C	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61355	success or wait	1	402118	ReadFile
C:\Users\user\AppData\LocalLow\10PkIt2V82WR	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\10PkIt2V82WR	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\10PkIt2V82WR	28672	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\cdE656z8QTF7	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\cdE656z8QTF7	0	4096	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\2KyP65ecp6T3	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\2KyP65ecp6T3	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\432zCWSnwm1N	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\432zCWSnwm1N	0	2048	success or wait	1	61E33E79	ReadFile

Analysis Process: llpb1133.exe PID: **2560**, Parent PID: **3776**

General	
Target ID:	20
Start time:	19:45:08
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\llpb1133.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\llpb1133.exe"
Imagebase:	0x140000000
File size:	3657728 bytes
MD5 hash:	81A0ECC23B44DA5116D397C0A3104A05
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 77%, ReversingLabs

Analysis Process: icacls.exe PID: **3460**, Parent PID: **5672**

General	
Target ID:	21
Start time:	19:45:09
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	icacls "C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Imagebase:	0xf40000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **4116**, Parent PID: **996**

General	
Target ID:	26
Start time:	19:45:19
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 996 -s 520
Imagebase:	0x360000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: pliu.exe PID: **1952**, Parent PID: **3776**

General	
Target ID:	27
Start time:	19:45:22
Start date:	07/02/2023

Path:	C:\Users\user\AppData\Local\Temp\pliu.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\pliu.exe"
Imagebase:	0x400000
File size:	163840 bytes
MD5 hash:	B9363486500E209C05F97330226BBF8A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 85%, ReversingLabs

Analysis Process: conhost.exe PID: **5060**, Parent PID: **1952**

General

Target ID:	28
Start time:	19:45:22
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: XandETC.exe PID: **5632**, Parent PID: **3776**

General

Target ID:	29
Start time:	19:45:23
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\XandETC.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\XandETC.exe"
Imagebase:	0x7ff6ec770000
File size:	3890176 bytes
MD5 hash:	3006B49F3A30A80BB85074C279ACC7DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 92%, ReversingLabs

Analysis Process: 3046.exe PID: **3112**, Parent PID: **3452**

General

Target ID:	33
Start time:	19:45:26
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart
Imagebase:	0x400000
File size:	722944 bytes
MD5 hash:	46909DA148DE57B2D85591626AEDBD76

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000021.00000002.516055302.00000000022BA000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000021.00000002.516427401.0000000002350000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000021.00000002.516427401.0000000002350000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 62%, ReversingLabs

Analysis Process: 3046.exe PID: **4424**, Parent PID: **1080**

General

Target ID:	35
Start time:	19:45:31
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe --Task
Imagebase:	0x400000
File size:	722944 bytes
MD5 hash:	46909DA148DE57B2D85591626AEDBD76
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 3046.exe PID: **5256**, Parent PID: **5672**

General

Target ID:	39
Start time:	19:45:35
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\3046.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\3046.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	722944 bytes
MD5 hash:	46909DA148DE57B2D85591626AEDBD76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000027.00000002.517661661.00000000022E4000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000027.00000002.518320509.0000000002380000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000027.00000002.518320509.0000000002380000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: pliu.exe PID: **5180**, Parent PID: **1952**

General

Target ID:	40
Start time:	19:45:35
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\pliu.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\pliu.exe" -h
Imagebase:	0x400000

File size:	163840 bytes
MD5 hash:	B9363486500E209C05F97330226BBF8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6136**, Parent PID: **5180**

General	
Target ID:	41
Start time:	19:45:36
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 3046.exe PID: **4084**, Parent PID: **3452**

General	
Target ID:	42
Start time:	19:45:36
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\09cc62dd-ff65-4927-b82d-d455eaaeb9f0\3046.exe" --AutoStart
Imagebase:	0x400000
File size:	722944 bytes
MD5 hash:	46909DA148DE57B2D85591626AEDBD76
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000002A.00000002.518333813.0000000002290000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000002A.00000002.518796436.0000000002330000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000002A.00000002.518796436.0000000002330000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Disassembly

No disassembly