ID: 830301
Sample Name:
SC.028UCCP.exe
Cookbook: default.jbs
Time: 08:44:20
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

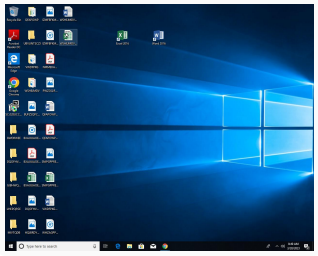
Windows Analysis Report

SC.028UCCP.exe

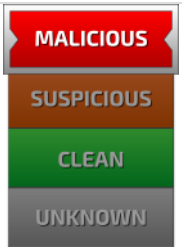
Overview

General Information

Sample Name:	SC.028UCCP.exe
Analysis ID:	830301
MD5:	3f8f4a7f43b562..
SHA1:	1c1931fe8db9b..
SHA256:	0ae741990942...
Tags:	exe signed
Infos:	



Detection



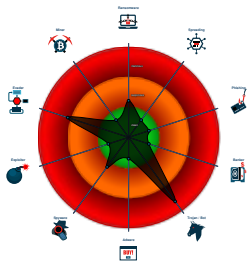
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Contains functionality to dynamicall…
- Abnormal high CPU Usage
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- SC.028UCCP.exe (PID: 5928 cmdline: C:\Users\user\Desktop\SC.028UCCP.exe MD5: 3F8F4A7F43B5627ED45128BB99F0B471)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.782049027.00000000005D0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000000.00000002.782394015.0000000002B00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000000.00000002.782394015.000000000400D000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

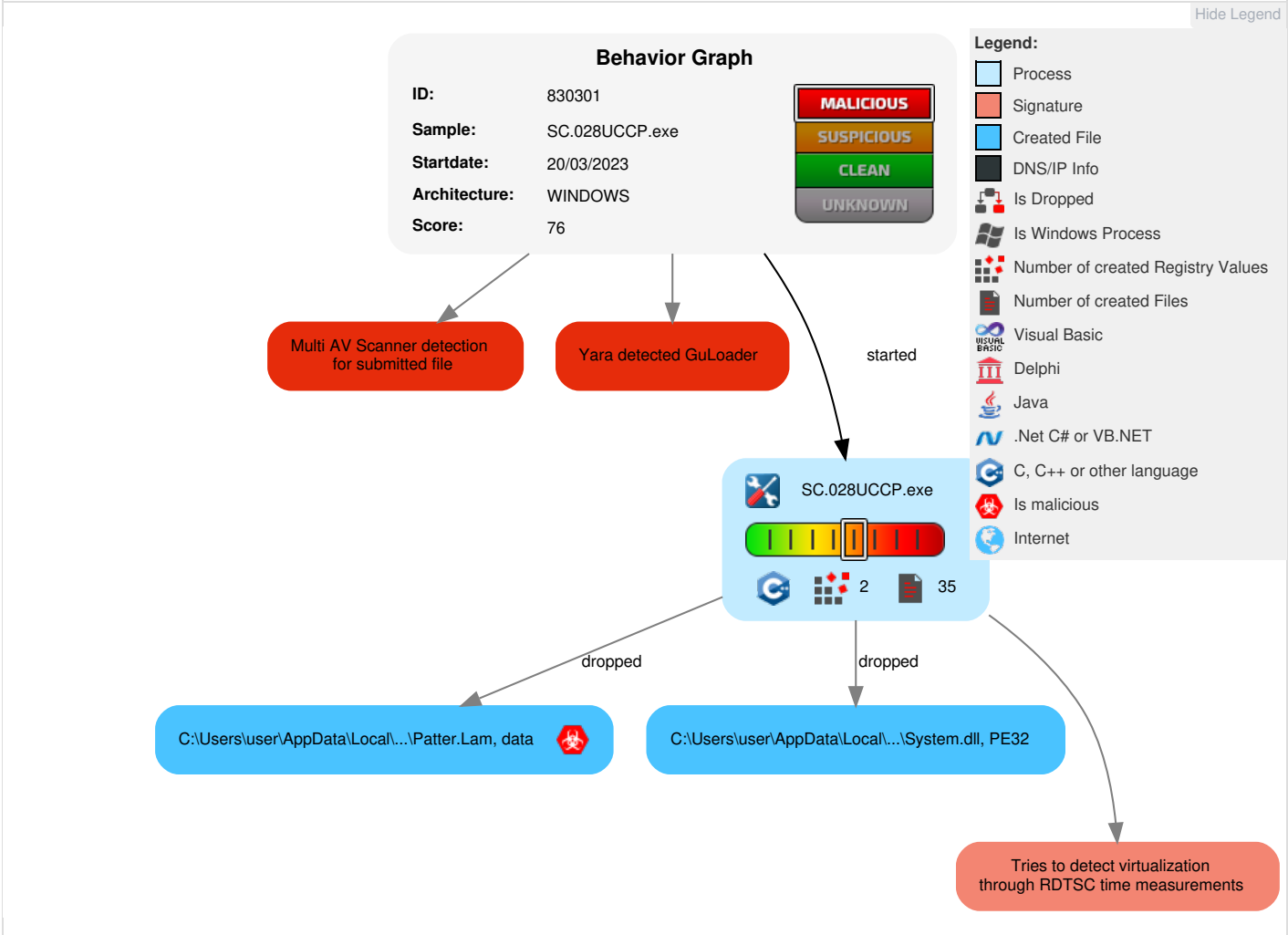
Tries to detect virtualization through RDTSC time measurements

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 Native API	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

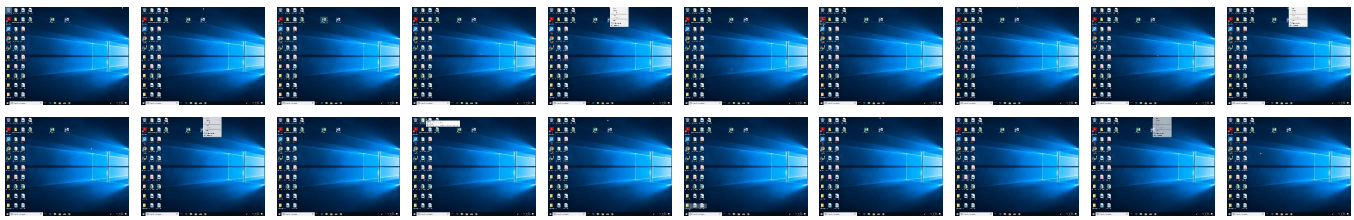
Behavior Graph



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
SC.028UCCP.exe	33%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	SC.028UCCP.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	SC.028UCCP.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830301
Start date and time:	2023-03-20 08:44:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 28s
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SC.028UCCP.exe
Detection:	MAL
Classification:	mal76.troj.evad.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.4% (good quality ratio 59%) • Quality average: 87% • Quality standard deviation: 23.1%
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 • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: SC.028UCCP.exe

Simulations

Behavior and APIs

No simulations

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:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam

Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	data
Category:	dropped
Size (bytes):	268768
Entropy (8bit):	7.143396451103385
Encrypted:	false
SSDEEP:	6144:qJAA/mPgVn081S1KOqplrh02aq18CUcmQd:TA/moVw1HP02J8CUcVd
MD5:	C6AF2E59D4C09946D5F809241D770F50
SHA1:	266B1073C52D94E9451AA08B2605F2237E5F8A0C
SHA-256:	89E42F99BB457998B2FA3A4D0973ABFE9A39163227F56C8D000CCE44F1EF0070
SHA-512:	B005D4324152790A8BDAAAEE6272A899639FF8D5E1E1FFE1E1219C569F9D271C4A21440F709CA3693A5F80A664501D3AB79EBA81B5B9D07C8870FE5AC15D5124
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam, Author: Joe Security
Reputation:	low

Preview:	.....

C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\ArtDeco_green_7.bmp

Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, components 3
Category:	dropped
Size (bytes):	5717
Entropy (8bit):	7.862470085974542
Encrypted:	false
SSDEEP:	96:BSTzREom7JPxQ7OTst5UcVq9JD6EgZEoW249KONYq9iwry9t1Bs6UQJaE424CZ:oXRgtPEOa6+q65Zr87YXwry9tzuCZ
MD5:	B182207A878FA708746DA5A94F08A581
SHA1:	4EF329C2643A9B5E19F491D644A96EF3E7388BE6
SHA-256:	40125E69AA66C655FA44F83BBDEB7E9F24FE81D69CC717651A42C908483FF687
SHA-512:	2368E6533A4D660C08C6F196F38CE2F706C8486AA9E5B1C2413988251184D6A928A348E74DDF0FB098F928D7FCFA4DD71829766E1964E3E5085D642497D034B4
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\Patronymens.Hov230

Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	GTA audio index data (SDT)
Category:	dropped
Size (bytes):	42868
Entropy (8bit):	4.531239376712852
Encrypted:	false
SSDEEP:	768:BmzeD2YSUGt8UN3/hCwqfWCixEmPmXZNIYmhaspQZV:BF9SfyUNvrxEmMAHpQT
MD5:	545F37C048EB23C04FF82F592FB89DEB
SHA1:	9ED7C0D724A7A1C7E38F2A5134D1325B49FCCF25
SHA-256:	DA3CADFEE6D3939C607B6F60B12861931ABD8E7441A2C148C396A38957C7D4DF
SHA-512:	0EB46B15043855818821DD3C60A491E83DF943A30E3BC57E9D37F81AAFF697DFFEF94CE8874A1F61E1E93B7BA2FD740E4FAF7E267BFB1B5B708F1979ED29265 5
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll

Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.72460245623286
Encrypted:	false
SSDEEP:	96:3IsUxO9udx4qYp7AJb76BykUbQMtHUOA5Iv+RnsrqeXV+d1g2IW9t2c+cEwF9oug:YVL7ikJb76BQUoUm+RnyXVYO2RvHoug
MD5:	CF85183B87314359488B850F9E97A698
SHA1:	6B6C790037EEC7EBEA4D05590359CB4473F19AEA
SHA-256:	3B6A5CB2A3C091814FCE297C04FB677F72732FB21615102C62A195FDC2E7DFAC
SHA-512:	FE484B3FC89AEED3A6B71B90B90EA11A787697E56BE3077154B6DDC2646850F6C38589ED422FF792E391638A80A778D33F22E891E76B5D65896C6FB4696A2C3E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....I....I.Richm.....PE..L...k..Q.. .....!.....&.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... .`.rdata..C....0....."....@..@.data...h....@.....&.....@....reloc..H....P.....(.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.920107350850815
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	SC.028UCCP.exe
File size:	267392
MD5:	3f8f4a7f43b5627ed45128bb99f0b471
SHA1:	1c1931fe8db9b5df89d39e3121fa72c2a355ded1
SHA256:	0ae741990942bc5b9a51a72dc1cc9f2197b8fe140b76eee9170c3260c00e8656
SHA512:	800a88ff5985f832c73fbada7fa71175531dbe9bd47a93bc8941817e791d8868cfedd4dad2f82604ce06e1e2136821b963d35e23d580edf2d260475eb213ff6f
SSDEEP:	6144:4auq7FPth0P6iM7EFsjSHR58yQITE1vE1P57hO5FKHJa:HFPr0SirFjC1yP5NO5FKg
TLSH:	AE4412172BE645FFF9D78C72103AEAB3F5BBE6580817144E0B266F7A7D00603092969D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1p.:u..iu..iu..i...iw..iu..i...i...id..i!2.i...i...it..iRichu..i.....PE..L.....Q.....^.....1.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40310b
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x51E3058F [Sun Jul 14 20:09:51 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b40f29cd171eb54c01b1dd2683c9c26b

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=synsmaades@Lakeside.Fo, OU="Virksomhedsledelsens Tensionerne ", O=Draconis, L=Saint-Projet, S=Nouvelle-Aquitaine, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 8/19/2022 10:31:00 PM 8/18/2025 10:31:00 PM
Subject Chain	• E=synsmaades@Lakeside.Fo, OU="Virksomhedsledelsens Tensionerne ", O=Draconis, L=Saint-Projet, S=Nouvelle-Aquitaine, C=FR

Version:	3
Thumbprint MD5:	82A2F162C13C97C7C5BD9D1EF5E3E352
Thumbprint SHA-1:	0A4EF0B597133BD21B48A5030DE4541818CB48DA
Thumbprint SHA-256:	9B7EDD84EF52310C29E72A78ED7E0EB44C977D6DE7359675C1845C3D1CD29EBC
Serial:	3E36636B7C2A21B05072BFF828C9540A74C9C941

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409190h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407034h]
push 00008001h
call dword ptr [004070B0h]
push ebx
call dword ptr [0040728Ch]
push 00000008h
mov dword ptr [0042EC58h], eax
call 00007FB3B0AB27D8h
mov dword ptr [0042EBA4h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00428FE0h
call dword ptr [00407164h]
push 00409180h
push 0042E3A0h
call 00007FB3B0AB2482h
call dword ptr [0040711Ch]
mov ebp, 00434000h
push eax
push ebp
call 00007FB3B0AB2470h
push ebx
call dword ptr [00407114h]
cmp byte ptr [00434000h], 00000022h
mov dword ptr [0042EBA0h], eax
mov eax, ebp
jne 00007FB3B0AAFA6Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00434001h
push dword ptr [esp+14h]
push eax
call 00007FB3B0AB1F1Dh
push eax
call dword ptr [00407220h]
mov dword ptr [esp+1Ch], eax
jmp 00007FB3B0AAFB25h
cmp cl, 00000020h
jne 00007FB3B0AAFA68h
inc eax

Instruction
cmp byte ptr [eax], 00000020h
je 00007FB3B0AAFA5Ch

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74b0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x44000	0x10b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3fc20	0x1860	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x298	.rdata
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	0x5de8	0x5e00	False	0.6791057180851063	data	6.503326078284377	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x12da	0x1400	False	0.4388671875	data	5.095966873256735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c98	0x400	False	0.63671875	data	5.037907617207934	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2f000	0x15000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x44000	0x10b0	0x1200	False	0.3513454861111111	data	4.2798158371727295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x44238	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x445a0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x44888	0x144	data	English	United States
RT_DIALOG	0x449d0	0x13c	data	English	United States
RT_DIALOG	0x44b10	0x100	data	English	United States
RT_DIALOG	0x44c10	0x11c	data	English	United States
RT_DIALOG	0x44d30	0x60	data	English	United States
RT_GROUP_ICON	0x44d90	0x14	data	English	United States
RT_MANIFEST	0x44da8	0x305	XML 1.0 document, ASCII text, with very long lines (773), with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	Sleep, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, CompareFileTime, SearchPathA, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, GetWindowsDirectoryA, SetFileAttributesA, lstrcmpiA, SetErrorMode, LoadLibraryA, lstrlenA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrcpyA, lstrcatA, GetSystemDirectoryA, GetVersion, GetProcAddress, WaitForSingleObject, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, GetModuleHandleA, LoadLibraryExA, GetCommandLineA, GetTempPathA, FreeLibrary, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, MulDiv, WriteFile, MultiByteToWideChar
USER32.dll	CreateWindowExA, EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, GetDC, SystemParametersInfoA, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, CreateDialogParamA, SetTimer, GetDlgItem, wsprintfA, SetForegroundWindow, ShowWindow, IsWindow, LoadImageA, SetWindowLongA, SetClipboardData, EmptyClipboard, OpenClipboard, EndPaint, PostQuitMessage, FindWindowExA, SendMessageTimeoutA, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegCloseKey, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegEnumValueA, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	CoCreateInstance, CoTaskMemFree, OleInitialize, OleUninitialize
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: SC.028UCCP.exe PID: **5928**, Parent PID: **3452**

General

Target ID:	0
Start time:	08:45:18
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\SC.028UCCP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC.028UCCP.exe
Imagebase:	0x400000
File size:	267392 bytes
MD5 hash:	3F8F4A7F43B5627ED45128BB99F0B471

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000000.00000002.782049027.00000000005D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000000.00000002.782394015.0000000002B00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.782394015.000000000400D000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4030FE	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nstD527.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4058A9	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4015E1	CreateDirectoryA
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	2	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4015E1	CreateDirectoryA
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	2	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Unepitomizeds	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405872	CreateFileA
C:\Users\user\AppData\Local\Temp\Unepitomizeds	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\ArtDeco_green_7.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405872	CreateFileA
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\Patronymens.Hov230	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405872	CreateFileA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4058A9	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405872	CreateFileA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	2	405872	CreateFileA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	7126	405872	CreateFileA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

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	4015E1	CreateDirectoryA
C:\Users\user\Music	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\Music\Talests	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\Music\Talests\Unimaginatively	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\Music\Talests\Unimaginatively\Wrathless	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	6	405872	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstD527.tmp	success or wait	1	403322	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsuD883.tmp	success or wait	1	4054A4	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam	0	32768	fd fd		success or wait	13	402FE7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\ArtDeco_green_7.bmp	0	5717	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	402FE7	WriteFile
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\Patronymens.Hov230	0	32015	00 00 00 00 0a 00 00 00 7a 7a 00 00 1b 1b 1b 00 00 2b 2b 00 00 fd 00 00 00 00 00 fd 00 5e 5e 5e 00 00 fd 00 00 00 00 00 00 00 00 00 fd 00 00 6c 00 00 fd 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 22 22 00 52 00 fd fd fd fd fd 00 fd 00 00 00 fd 00 00 36 00 00 fd fd 00 00 63 63 63 63 63 63 00 42 00 00 00 00 00 28 00 00 7d 7d 00 00 00 00 3e 3e 3e 3e 3e 00 42 00 3f 00 43 00 00 4a 00 4f 00 00 79 79 00 fd 00 00 00 43 00 fd fd 00 00 21 21 00 00 4d 4d 4d 4d 00 00 00 00 fd fd 00 00 70 70 00 00 00 fd 00 00 00 00 00 00 00 fd fd 00 00 00 00 fd fd 00 00 00 00 50 00 00 00 27 00 00 00 fd fd fd fd fd 00 00 00 00 00 00 00 00 67 00 43 43 00 11 00 77 77 00 00 00 fd fd fd fd 00 4b 00 00 00 00 00 00 00 39 00 3b 3b 00 fd fd 00 58 00 00 fd 00 00 19 19 19 00 57 00 fd	zz++^^^l""R6ccccccB(}}>>>>>B?CJOyyC!!MMMMppP'gCCwwK9;;XW	success or wait	2	402FE7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsuD883.tmp\System.dll	0	11264	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 29 fd fd fd 6d fd 6d fd 6d fd fd bd 6b fd 6d fd 7e b3 6e fd fd 6a fd 39 4c fd 69 fd 0e 16 fd 6c b3 52 b8 fd 6c fd 52 69 63 68 6d 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 6b 05 fd 51 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$)mmmkm~j9illRichmPELkQ!	success or wait	1	402FE7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SC.028UCCP.exe	unknown	512	success or wait	78	4030AB	ReadFile
C:\Users\user\Desktop\SC.028UCCP.exe	unknown	4	success or wait	1	4030AB	ReadFile
C:\Users\user\Desktop\SC.028UCCP.exe	unknown	4	success or wait	3	4030AB	ReadFile
C:\Users\user\Desktop\SC.028UCCP.exe	unknown	4	success or wait	1	4030AB	ReadFile
C:\Users\user\Desktop\SC.028UCCP.exe	unknown	4	success or wait	1	4030AB	ReadFile
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\Patronymens.Hov230	unknown	1	success or wait	634	402569	ReadFile
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam	unknown	53243904	success or wait	1	1000285D	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Planlgningers	success or wait	1	40235E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Planlgningers\Reanesthetized	success or wait	1	40235E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Planlgningers\Reanesthetized\Skvendes	success or wait	1	40235E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Planlgningers\Reanesthetized\Skvendes\Anisopleural	success or wait	1	40235E	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Alkanet	success or wait	1	40235E	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Alkanet\Mystifically	success or wait	1	40235E	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Planlgningers\Reanesthetized\Skvendes\Anisopleural	Interning	unicode	Makedoniske	success or wait	1	4023B7	RegSetValueExA
HKEY_CURRENT_USER\Software\Alkanet\Mystifically	Otterer	binary	6F A3 DB	success or wait	1	4023B7	RegSetValueExA

Disassembly

No disassembly