ID: 680367
Sample Name: Ordene 501527,pdf.exe
Cookbook: default.jbs
Time: 13:21:19
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

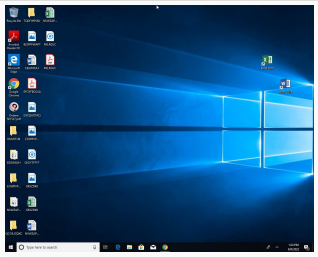
Windows Analysis Report

Ordene 501527,pdf.exe

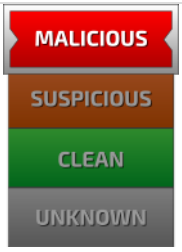
Overview

General Information

Sample Name:	Ordene 501527,pdf.exe
Analysis ID:	680367
MD5:	5162b6782f86f1f..
SHA1:	0d1ead84c74ee4..
SHA256:	6730e52c8075c7..
Tags:	exe
Infos:	



Detection



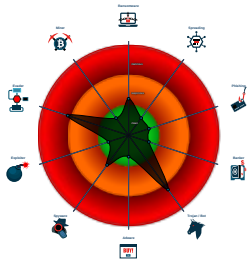
GuLoader

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Stores files to the Windows start me…
- PE / OLE file has an invalid certifica…

Classification



Process Tree

- **System is w10x64**
- Ordene 501527,pdf.exe (PID: 5396 cmdline: "C:\Users\user\Desktop\Ordene 501527,pdf.exe" MD5: 5162B6782F86F1F24E8610544D159AE9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.669759237.0000000002E00000.00000040.00001000.00020000.00000000.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

Data Obfuscation

Yara detected GuLoader

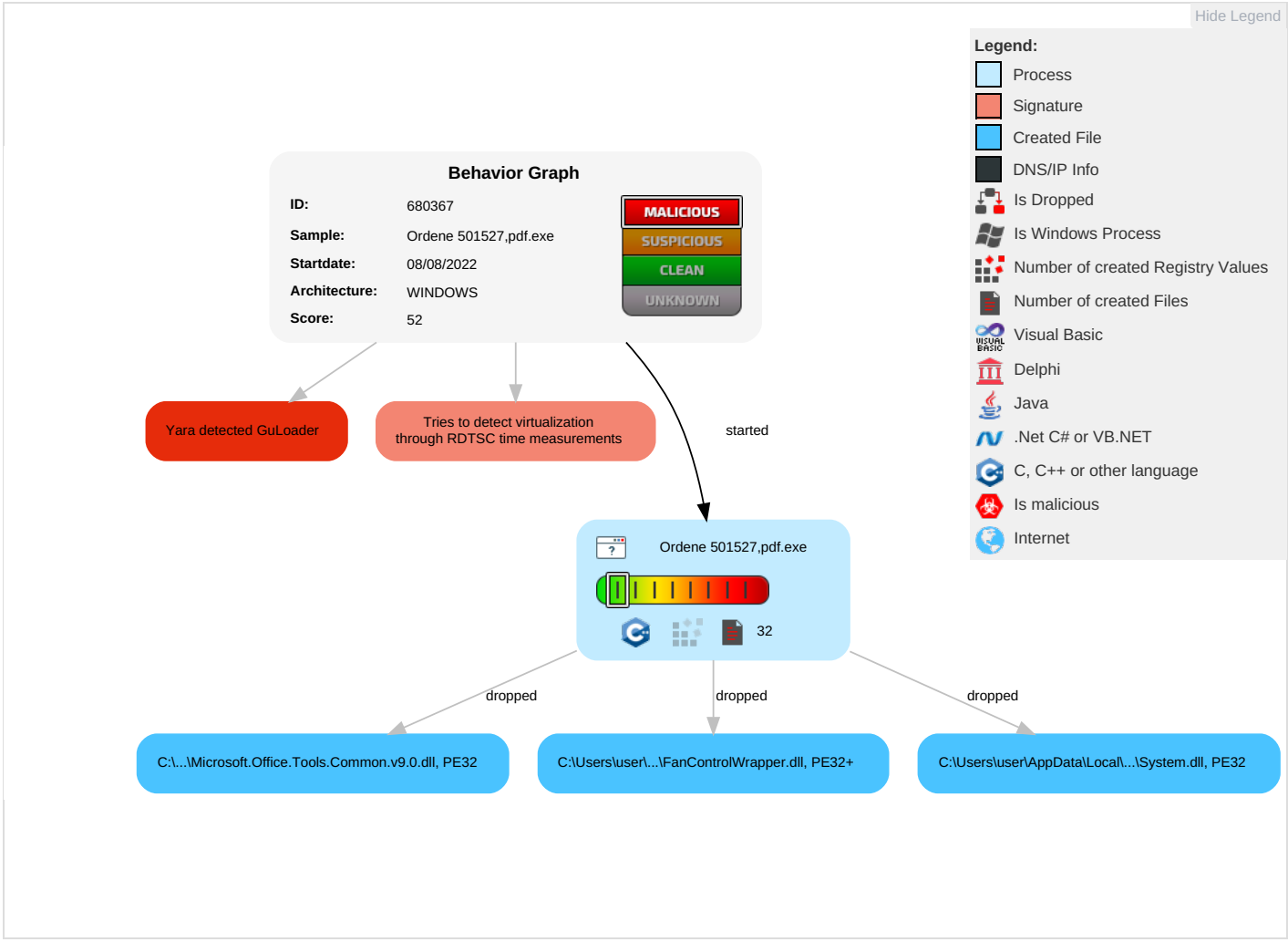
Malware Analysis System Evasion

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	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	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)	1 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

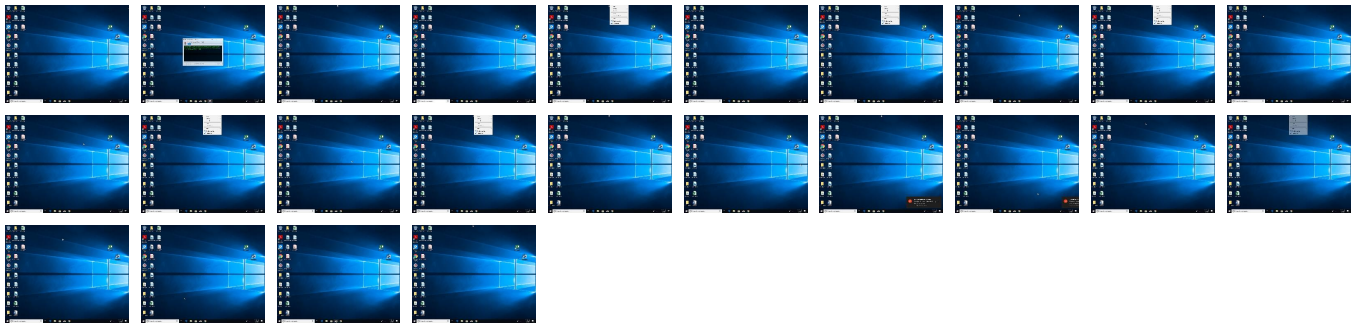
Behavior Graph



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
Ordene 501527,pdf.exe	7%	ReversingLabs	Win32.Malware.Teddy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nshB62A.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nshB62A.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.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_ErrorError	Ordene 501527,pdf.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680367
Start date and time: 08/08/202213:21:19	2022-08-08 13:21:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ordene 501527,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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
Detection:	MAL
Classification:	mal52.troj.evad.winEXE@1/5@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.5%) • Quality average: 87.8% • Quality standard deviation: 22.4%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, licensing.mp.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\nshB62A.tmp\System.dll

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8Qll972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	53480
Entropy (8bit):	6.013119476725682
Encrypted:	false
SSDEEP:	768:Sd5iVw6ve4HsIrMTW5q6Aq2g1AEpwhaPvWFzg4KClyQ2c94PkhEeaA2X9qKh:s4wmnMT6Jp2g1a4s+7
MD5:	8D512C6FFE33E6B77981497ED40D9092
SHA1:	A31DE10B01C626D528FEF987CE5D7DB68D228849
SHA-256:	25673566002F8EEF81872E2913DA0E44D0B7480EF824EDD1C12D725A122CAE1C
SHA-512:	479DDADE0F58CFDEB43EEACD38D0CE8A361275A2BD4257CDF4FA3DD5A5FEEF231E6E41D0F2BF3F17AF8DF38B0DB72114677C42B69865F90F81329041CDFBE 4A5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3..-w..~w..~w..~~..~q..~%..t..~...s..~i..~u..~%..d..~%.....~%..u..~...u. .~w..~Y..~...r..~...v..~..x~v..~w..~v..~...v..~Richw..~.....PE..d...h6;a.....' .....2.....>.....$(...`..... ..... .....@....S..p.....T.....P.....XS..H.....text.....0..... ..`.nep....p....@.....4..... ..`.rdata..$m...P...n...6.....@..@.data .....@....pdata.....@..@.rsrc.....@..@.reloc..@.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	356352
Entropy (8bit):	5.597789776248351
Encrypted:	false
SSDEEP:	6144:gAENg6Ta1Hjxcv/IUIuoeT/xK6ur6EaPC:gdgbFK/IU7T/xK6ur6EaP
MD5:	E047210B4CE2BBF0F6A9819031C5874A
SHA1:	FBE964CABCD15468EFF6848ACE2F49E194C2B1B4
SHA-256:	F0C45C94B8B1B38718FD373E9E98BF76A5552D8405DE3A98A6CADBE9610F7E74
SHA-512:	57754F490FAD208076EA717470E431493396556E5DC4BE53ED2ACFBBC00857B9F6A5AEDA66FFE82F4E4CF405ABEF16E72F77535932E9D166CC4F3DE262AC09 8
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..H.....!.....P.....-... ...@....UA. ....@.....-..W....@..`7..... ..... ..H.....text..... ..... ..`.rsrc...`7...@...@... .....@..@.rel oc.....`.....@..B..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\edit-cut-symbolic.svg

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1327
Entropy (8bit):	4.272364610533777
Encrypted:	false
SSDEEP:	24:2dPnnxu3tlKpRe+9abXi2QP+60wWgP7IC233P+60cXW7GTNWgPN:cfnHFabXij+zgP7ICK+r7GTUgPN
MD5:	36C1AE9391F50D4AD3A1E61CA30CBFCB
SHA1:	DF3D58AB8DBFD1CE9F0456C4F8C84440A1005507
SHA-256:	9FDDABAAF63AE19BA00A965BBDAACAC3703AB2F055661040A4ACFF2882D0087B
SHA-512:	180D77E3FA447CED1276C2E2070E110667530C864C71961E97E80B51C214C7BEBF604104F6A0DF87A4779E6E3AD08C5A574278F70C6D36C083FE727B1DD6647

Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 14 1 l -5.203125 4.972656 l 1.5625 1.527344 l 5.640625 -5.5 v -1 z m -6.804688 6.5 l -2.976562 2.84375 l 1.6875 1.5 l 2.890625 -2.816406 z m 0 0"/>. <path d="m 4.21875 5.65625 l 9.78125 9.34375 h 2 v -1 l -10.09375 -9.84375 z m 0 0"/>. <path d="m 5.972656 1.019531 c -1.359375 -1.359375 -3.59375 -1.359375 -4.953125 0 c -1.359375 1.359375 -1.359375 3.59375 0 4.953125 s 3.59375 1.363282 4.953125 0 c 1.359375 -1.359375 1.359375 -3.59375 0 -4.953125 z m -1.414062 1.414063 c 0.597656 0.59375 0.597656 1.53125 0 2.125 c -0.59375 0.597656 -1.527344 0.597656 -2.125 0 c -0.59375 -0.59375 -0.59375 -1.527344 0 -2.125 c 0.597656 -0.59375 1.53125 -0.59375 2.125 0 z m 0 0"/>. <path d="m 5.972656 10.019531 c -1.359375 -1.359375 -3.59375 -1.359375 -4.953125 0 c -1.359375 1.359375 -1.359375 3.597657 0 4.957031 c 1.359

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven\vrkstedsbygninger\Ricciaceae185.lnc

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	76679
Entropy (8bit):	6.814432315698124
Encrypted:	false
SSDEEP:	1536:XJV/wgXTw40tzGcM8E7nhHaxpqeGhJrfBxdKTi:XJWgXTyvE7nqMhJvL
MD5:	FFDF86E18706923E73DE9A5D67A8C9EB
SHA1:	F01102765BEEB1330F29E2427C9559EDBEEA8D4E
SHA-256:	63D2CBFFAB97859707640C94C9810AF953093F01FF0E7FDB2DBFF3827935EDC0
SHA-512:	1D3E7DD9A687580682CB827CAB4C3D50F9EEC145411EEE24261DB0F89B8A087B5B6DE57B33E2D6B6E807D9AA79005050E5E09A4D58FC60F4E48F31BD32C7BF 72
Malicious:	false
Reputation:	low
Preview:	8..f9.8.f9..r..._.b.f9.....X.......?.u/8..nf._....u ..,..8..,9.....u...f.^.f.^.9...;..........X......f._...............$.........f9.......5h...f.^..b..9.5..q...X.f9.f._.8...#m.f.^........n........r..E5..........f._.f._.f .^.8.-.....^.f._......f9.P............wZ............8..@......1.......=....f9.f._.=.....4.! .W..f9....9...D9...b.........9.u..u......W..o..X..$...f9..........W!#.zg.9.8.Z.a.%.}+:.!_........^.@.hW0.> LQ{.N.."%eA.U5..v./.....G.n.j`K..7.((....rL\.g..5.......w.a.QY.*...puv.0......~.)....l..(.((.((.((.((.((.((.((.((.((.((.((.((.((.((..Q.9.8.Z.a.%.}+:.!_........^.@.hW0.>LQ{.N.."%eA.U5..v./.....G .n.j`K..7.((....rL\.g..5.......w.a.QY.*...puv.0......~.)....l...((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.....((.((.((.((.((.((.((.((.((.((.((.((.((.((.((..x.Q....((.((.((.((.((.((.((.((.((.((.((.((.((.(.....s{(.((.((.((. ((.((.((.((.((.((.((.((.((.((.((...... ..P...3....5z......m.......((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.(...(.((.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.549201429075207
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:	Ordene 501527,pdf.exe
File size:	596608
MD5:	5162b6782f86f1f24e8610544d159ae9
SHA1:	0d1ead84c74ee462976928783c1f733aa859bc94
SHA256:	6730e52c8075c7e044c2bbaf9f7ad8c0f7f8d03fb23adbd2331adc8b591caec7
SHA512:	ccbea38e4c47edf9172e47f8ea884bae222365500d17bc5d95bef911d64feb6857ac7c2d99bd9b6a0a6112a042ea0e74cd958b656883912827451f21c5113f83
SSDEEP:	6144:B6bAcJOv+qlAcxp8XNbu0lTCzYQhb3VG+rmAYJDB5aRELlQBjokpKE+c0AzugkGd:a+NniSb3VtrHSaklQBjo0KE+72jCMii
TLSH:	96C4AE4179B86ED3F57E03716CA7869212A8EC141672E71B3192FE17B4B23532B0F29D
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@..........................PE..L.....uY.................d....:....

File Icon

Icon Hash:	71c884a498dc7890

Static PE Info

General

Entrypoint:	0x403350

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:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759518 [Mon Jul 24 06:35:04 2017 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:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN="Murdock Hjernespinds Orddannelserne ", OU="Beauti Pilede ", E=Sheeting@Beredelse213.Syn, O=Stregens, L=La Haie-Traversaine, S=Pays de la Loire, 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	• 8/7/2022 8:49:24 PM 8/6/2025 8:49:24 PM
Subject Chain	• CN="Murdock Hjernespinds Orddannelserne ", OU="Beauti Pilede ", E=Sheeting@Beredelse213.Syn, O=Stregens, L=La Haie-Traversaine, S=Pays de la Loire, C=FR
Version:	3
Thumbprint MD5:	D9460ED9973B95EA8561C6C26E032EC9
Thumbprint SHA-1:	64BCC2EC4F74B5FAADE9D48BAC0D710AFF171E4F
Thumbprint SHA-256:	599928258A412563BC2620CAD41D51A4EDCF5C8E724A9DF73E6996094DA70D1E
Serial:	F03396B055CCF99F

Entrypoint Preview
Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax
je 00007F971C9E3083h
push ebx
call 00007F971C9E6319h
cmp eax, ebx
je 00007F971C9E3079h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F971C9E6293h

Instruction
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F971C9E305Ch
push 0000000Ah
call 00007F971C9E62ECh
push 00000008h
call 00007F971C9E62E5h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007F971C9E62D9h
cmp eax, ebx
je 00007F971C9E3081h
push 0000001Eh
call eax
test eax, eax
je 00007F971C9E3079h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

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	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c4000	0x59b58	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x8fd60	0x1d20	.data
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	0x8000	0x2b0	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a9000	0x1b000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3c4000	0x59b58	0x59c00	False	0.4010598015320334	data	5.323726974368565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3c4328	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x406350	0xe8be	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x414c10	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x418e38	0x25a8	data	English	United States
RT_ICON	0x41b3e0	0x10a8	data	English	United States
RT_ICON	0x41c488	0x988	data	English	United States
RT_ICON	0x41ce10	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x41d278	0x100	data	English	United States
RT_DIALOG	0x41d378	0x11c	data	English	United States
RT_DIALOG	0x41d498	0xc4	data	English	United States
RT_DIALOG	0x41d560	0x60	data	English	United States
RT_GROUP_ICON	0x41d5c0	0x68	data	English	United States
RT_VERSION	0x41d628	0x1ec	data	English	United States
RT_MANIFEST	0x41d818	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: Ordene 501527,pdf.exe PID: 5396, Parent PID: 5596

General	
Target ID:	0
Start time:	13:22:19
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ordene 501527,pdf.exe"
Imagebase:	0x400000
File size:	596608 bytes
MD5 hash:	5162B6782F86F1F24E8610544D159AE9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.669759237.0000000002E00000.00000040.00001000.00020000.00000000.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	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsfE849.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DBF	GetTempFileNameW
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	3	40581B	CreateDirectoryW

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	3	40581B	CreateDirectoryW
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	3	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven\vrkstedsbygninger	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven\vrkstedsbygninger\Ricciaceae185.Inc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\edit-cut-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\nshB62A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DBF	GetTempFileNameW
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	40581B	CreateDirectoryW
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	40581B	CreateDirectoryW
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	40581B	CreateDirectoryW
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	40581B	CreateDirectoryW
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	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshB62A.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	4057DB	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshB62A.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\nshB62A.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405D7D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsfE849.tmp	success or wait	1	403601	DeleteFileW
C:\Users\user\AppData\Local\Temp\nshB62A.tmp	success or wait	1	40599C	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven\vrkstedsbygninger\Ricciaceae185.Inc	0	32768	38 c4 fd 66 39 fd 38 fd 66 39 fd fd 72 01 00 00 5f 0f 62 fd 66 39 fd fd fd fd 0f 58 81 fd fd 00 00 00 fd 3f fd 75 2f 38 c3 fd 6e 66 0f 5f 80 7f 03 00 75 20 fd fd 2c fd fd 38 fd fd 2c 39 fd fd 7f 04 00 75 0f fd fd 66 0f 5e fd 66 0f 5e fd 39 fd fd fd 3b fd fd 00 03 00 00 fd fd fd 0f 58 81 fd fd 00 00 00 66 0f 5f 81 fd fd 00 00 00 fd fd 0d 02 00 00 fd 0c 08 24 fd fd fd fd fd 00 00 00 66 39 fd fd fd fd 00 00 00 35 68 fd 03 fd 66 0f 5e 83 fd 62 fd fd 39 fd 35 fd fd 71 fd fd 0f 58 fd 66 39 fd 66 0f 5f fd 38 fd 05 fd 23 6d 08 66 0f 5e 81 fd fd 00 00 00 fd fd 6e fd fd fd 00 00 00 fd fd 72 fd fd 45 35 fd 1b 10 fd fd fd fd 00 00 00 66 0f 5f fd 66 0f 5f fd 66 0f 5e fd 38 fd 2d fd 00 91 fd 0f 5e fd 66 0f 5f 81 fd fd 00 00 00 66 39 fd	8f98f9r_bf9X?u/8nf_u ,8,9uf^f^ 9;Xf_$f95hf^b95qXf9f_8# mf^nrE5f_f_f^8-^f_f9	success or wait	3	405E1D	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll	0	32768	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 18 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 33 fd fd 2d 77 fd fd 7e 77 fd fd 7e 77 fd fd 7e 7e fd 14 7e 71 fd fd 7e 25 fd 7f 74 fd fd 7e fd fd 7f 73 fd fd 7e 69 fd 14 7e 75 fd fd 7e 25 fd 7f 64 fd fd 7e 25 fd 7f 7f fd fd 7e 25 fd 7f 75 fd fd 7e 04 fd 7f 75 fd fd 7e 77 fd fd 7e 59 fd fd 7e fd fd 7f 72 fd fd 7e fd fd 7f 76 fd fd 7e fd fd 78 7e 76 fd fd 7e 77 fd 10 7e 76 fd fd 7e fd fd 7f 76 fd fd	MZ@!L!This program cannot be run in DOS mode.$3- w~w~w~~~q~%t ~s~i~u~%d~%~%u~u~w ~Y~r~v~x~v~w~v~v	success or wait	2	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll	0	32768	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 03 00 48 1d fd 48 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 08 00 00 10 05 00 00 50 00 00 00 00 00 00 fd 2d 05 00 00 20 00 00 00 40 05 00 00 00 55 41 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 05 00 00 10 00 00 fd 12 06 00 03 00 40 05 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.$PELHH!P- @UA @	success or wait	11	405E1D	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\edit-cut-symbolic.svg	0	1327	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 31 34 20 31 20 6c 20 2d 35 2e 32 30 33 31 32 35 20 34 2e 39 37 32 36 35 36 20 6c 20 31 2e 35 36 32 35 20 31 2e 35 32 37 33 34 34 20 6c 20 35 2e 36 34 30 36 32 35 20 2d 35 2e 35 20 76 20 2d 31 20 7a 20 6d 20 2d 36 2e 38 30 34 36 38 38 20 36 2e 35 20 6c 20 2d	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <g fill="#2e3436"> <path d="m 14 1 l -5.203125 4.972656 l 1.5625 1.527344 l 5.640625 -5.5 v -1 z m -6.804688 6.5 l -	success or wait	1	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshB62A.tmp\System.dll	0	11776	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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 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 50 45 00 00 4c 01 04 00 0e fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELuY!	success or wait	1	405E1D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Ordene 501527,pdf.exe	unknown	512	success or wait	791	405DEE	ReadFile
C:\Users\user\Desktop\Ordene 501527,pdf.exe	unknown	4	success or wait	2	405DEE	ReadFile
C:\Users\user\Desktop\Ordene 501527,pdf.exe	unknown	4	success or wait	20	405DEE	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven\vrkstedsbygninger\Ricciaceae185.Inc	unknown	1048576	success or wait	1	1000295D	ReadFile

Disassembly

No disassembly