ID: 828071
Sample Name:
DHL04AWB01173903102023PDF.scr.exe
Cookbook: default.jbs
Time: 18:03:16
Date: 16/03/2023
Version: 37.0.0 Beryl

Table of Contents

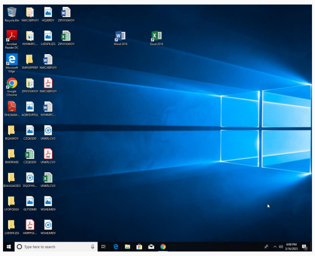
Windows Analysis Report

DHL04AWB01173903102023PDF.scr.exe

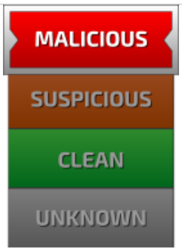
Overview

General Information

Sample Name:	DHL04AWB01173903102023PDF.scr.exe
Analysis ID:	828071
MD5:	1bf124cc783ff4..
SHA1:	b78f2ffb785071..
SHA256:	494d5735144a..
Tags:	DHL exe RemcosRAT scr signed
Infos:	



Detection



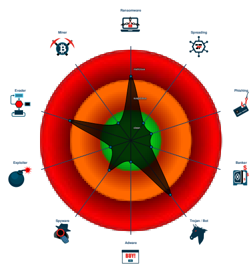
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- Found potential ransomware deman…
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- DHL04AWB01173903102023PDF.scr.exe (PID: 1308 cmdline: C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe MD5: 1BF124CC783FF47A91ADA4E6D4AC9E6B)
- **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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.832197103.0000000006825000.00000040.00001000.00020000.00000000.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

Spam, unwanted Advertisements and Ransom Demands

Found potential ransomware demand text

Data Obfuscation

Yara detected GuLoader

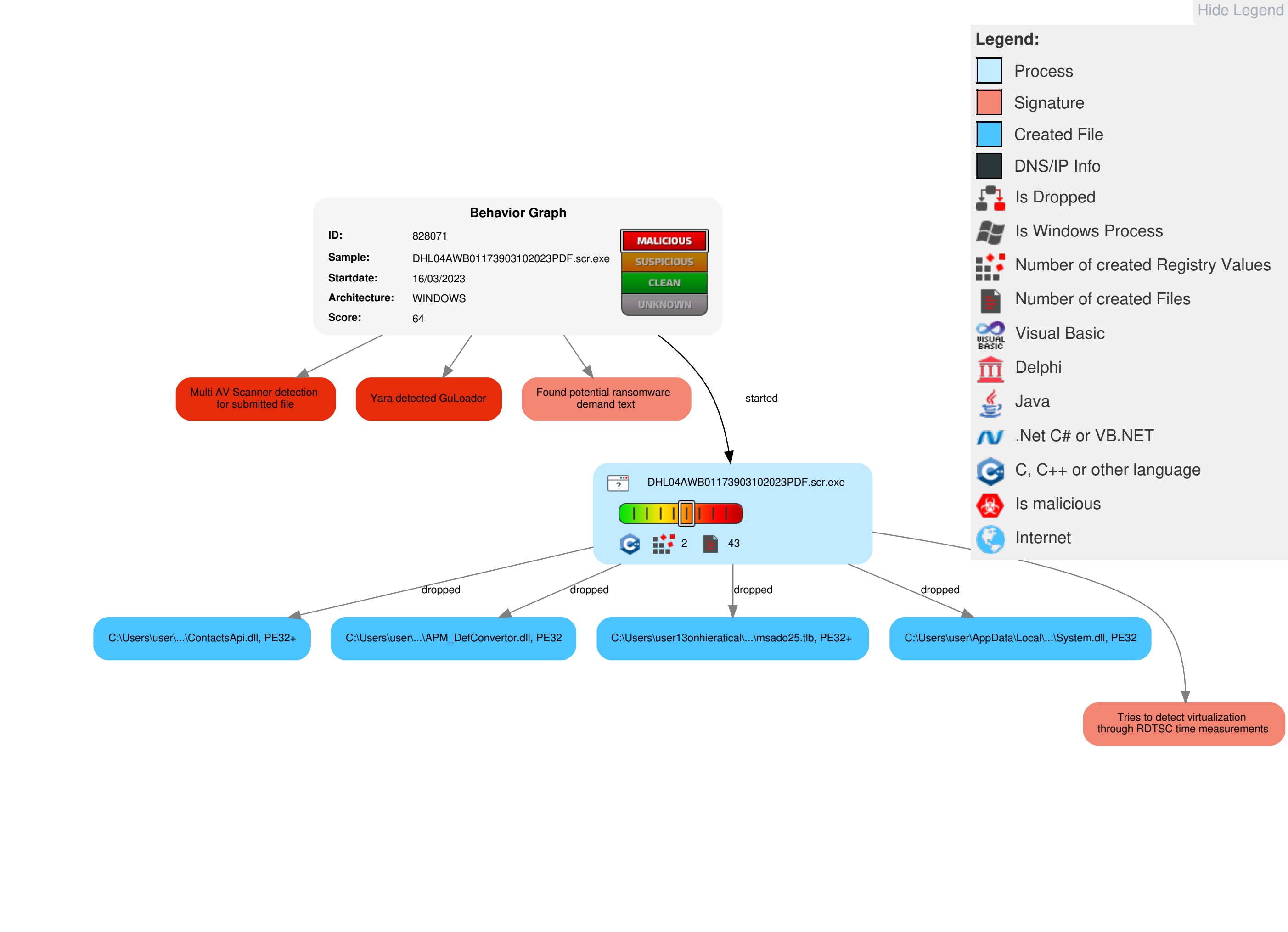
Malware Analysis System Evasion

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 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	Boot or Logon Initialization Scripts	1 Timestomp	LSASS Memory	3 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

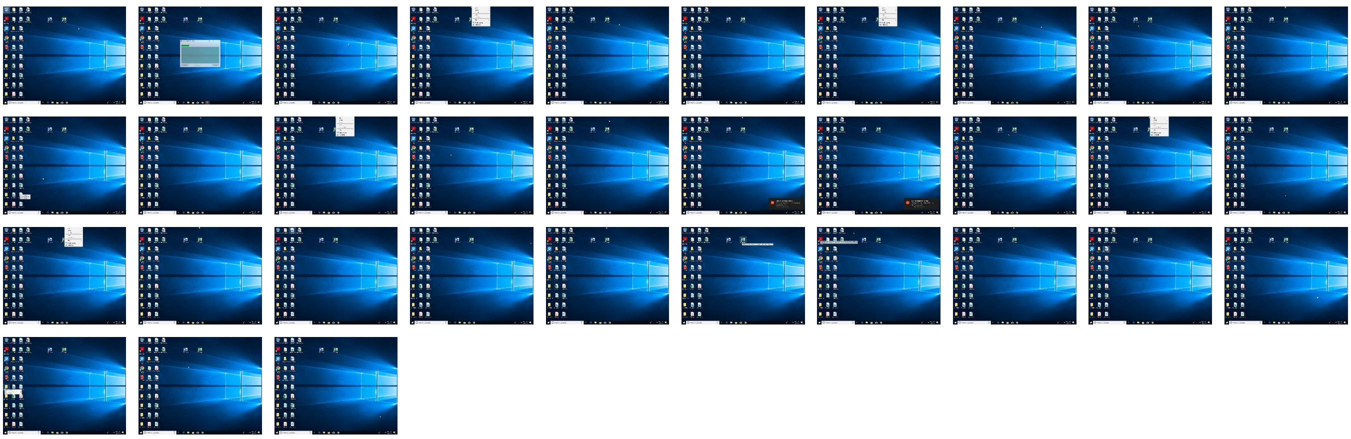
Behavior Graph



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
DHL04AWB01173903102023PDF.scr.exe	8%	ReversingLabs		
DHL04AWB01173903102023PDF.scr.exe	13%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsoF960.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsoF960.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb	0%	ReversingLabs		
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb	0%	Virustotal		Browse
C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll	0%	ReversingLabs		
C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll	0%	Virustotal		Browse
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll	0%	ReversingLabs		
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

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	DHL04AWB01173903102023PDF.scr.exe	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	DHL04AWB01173903102023PDF.scr.exe, 00000000.00000002.831811356.00000000029B2000.00000004.00000020.00020000.00000000.sdmp, nseEDA7.tmp.0.dr, APM_DefConvertor.dll.0.dr	false		high
http://www.symauth.com/cps0(	DHL04AWB01173903102023PDF.scr.exe, 00000000.00000002.831811356.00000000029B2000.00000004.00000020.00020000.00000000.sdmp, nseEDA7.tmp.0.dr, APM_DefConvertor.dll.0.dr	false		high
http://www.symauth.com/rpa00	DHL04AWB01173903102023PDF.scr.exe, 00000000.00000002.831811356.00000000029B2000.00000004.00000020.00020000.00000000.sdmp, nseEDA7.tmp.0.dr, APM_DefConvertor.dll.0.dr	false		high
http://ocsp.thawte.com0	DHL04AWB01173903102023PDF.scr.exe, 00000000.00000002.831811356.00000000029B2000.00000004.00000020.00020000.00000000.sdmp, nseEDA7.tmp.0.dr, APM_DefConvertor.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.nero.com	DHL04AWB01173903102023PDF.scr.exe, 00000000.00000002.831811356.00000000029B2000.00000004.00000020.00020000.00000000.sdmp, nseEDA7.tmp.0.dr, APM_DefConvertor.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828071
Start date and time:	2023-03-16 18:03:16 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
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:	6
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:	DHL04AWB01173903102023PDF.scr.exe
Detection:	MAL
Classification:	mal64.rans.troj.evad.winEXE@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63% (good quality ratio 61.6%) • Quality average: 88.1% • Quality standard deviation: 22.6%
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, conhost.exe, backgroundTaskHost.exe
- 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\nseEDA7.tmp

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	data

Category:	dropped
Size (bytes):	1831716
Entropy (8bit):	7.308492575684153
Encrypted:	false
SSDEEP:	49152:lf4WAQduqXBweZG32poHRS2tQuWikK9jM3:lJAQlnANE2tQTaM3
MD5:	9B4D8ABA094C64270F7878FAE618AC65
SHA1:	FA3D773625A7FE13C127925856A2B015C986E598
SHA-256:	CB136F81690F426D253696166DE342FF05A1C1F3C0C780BBE800A06396424751
SHA-512:	87EBE9A0C8BD59D98236943710F7A739AEE413FD8B198F1F9247943481942385725 2B6D160AB42A0EE8B976AAE3972185E2CC467FB9842AFEB9BF3C3D7577B73
Malicious:	false
Reputation:	low
Preview:	.3......,........................!.......2.......3...w...........-.J... ........................G...X..............j...f.. ....

C:\Users\user\AppData\Local\Temp\nsoF960.tmp\System.dll

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.774411073650885
Encrypted:	false
SSDEEP:	192:eB2HS+ihg200uWz947Wzvxu6v0MI7JOde+Ij5Z77dslFsE+:3S62Gw947ExuGDI7J8EF7KIE
MD5:	BE2621A78A13A56CF09E00DD98488360
SHA1:	75F0539DC6AF200A07CDB056CDDDDEC595C6CFD2
SHA-256:	852047023BA0CAE91C7A43365878613CFB4E64E36FF98C460E113D5088D68EF5
SHA-512:	B80CF1F678E6885276B9A1BFD9227374B2EB9E38BB20446D52EBE2C3DBA89764AA50CB4D49DF51A974478F3364B5DBCBC5B4A16DC8F1123B40C89C01725BE3 D1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
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....e.Q.. ....!................9'.......0..............................`.......................................2.......0..P...........................P.......................................................0..X...........................text..................... .......... ..`.rdata..C....0......."..............@..@.data...x....@.......&..............@....reloc..@....P.......(..............@..B.. ....

C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed\Coccosteid.Udr

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	data
Category:	dropped
Size (bytes):	202342
Entropy (8bit):	7.5372236610693095
Encrypted:	false
SSDEEP:	3072:YTz6SobCaMo6ljmx23UrLpvJvOc9CuKjrDee/jKOVox2EcIHuysfzFC64:w6SPaMo6l4XvOZ5rDtKOVoQrF0
MD5:	E2901A2B3EFA6BB00F2AD1D4AD963F52
SHA1:	1F2C771CEAE379DF9FA7FA1FA5E4ABC36638A42E
SHA-256:	FEFA0B1539475BF0ED224A8D9934FD4558DD0B1297FB661DAB776ABC96C333FF
SHA-512:	DA39BCB8E8C2BD79160B33A7767C58CC7CE204B56005B16AF6825DD6E25612D4C08E2C69A2DF288EC6635A24E740C23C5842E5DA3C08BDCCE9FC677D456C9 5E
Malicious:	false
Reputation:	low
Preview:	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAA

C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\TableTextServiceYi.txt	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	45170
Entropy (8bit):	3.7626877360483184
Encrypted:	false
SSDEEP:	384:wBMdoEQYh/lq7rwSM+jNyql218nyeEJFFCEeFe73c3+AC+mviFuqOtSS0uK3l/:wadoAr7s1+jNyqr6FFweIT0h0/
MD5:	AC05652AF93A583226FD118E23D3652F
SHA1:	DA5BB4AE245369888D1AF981AF6785FAE21C7BC9
SHA-256:	54E26FC4F586B39C4CCB6655735E8AA03AD31498EFD0119AB8406258D5561627
SHA-512:	2C24F1CBD45D5B06DF0A187793E02DA4F085E6E03CF1A697416F3F0B34FE4E96ECFCFD4E25DA3288383B98E1BC112A2418EFF5EA8E69BFBF153F28A20A687BF2
Malicious:	false
Reputation:	low
Preview:	..[.S.y.s.t.e.m.].....L.a.n.g.I.d. .=. .L.A.N.G._.Y.I.,. .S.U.B.L.A.N.G._.D.E.F.A.U.L.T.....G.u.i.d.P.r.o.f.i.l.e.=.{.4.0.9.C.8.3.7.6.-.0.0.7.B.-.4.3.5.7.-.A.E.8.E.-.2.6.3.1.6.E.E.3.F.B.0.D.}.....D.e.s.c.r.i.p.t.i.o.n.=.".Y.i. .I.n.p.u.t. .M.e.t.h.o.d.".....D.i.s.p.l.a.y. .D.e.s.c.r.i.p.t.i.o.n.=.".@.%.p.r.o.g.r.a.m.F.i.l.e.s.%.\.W.i.n.d.o.w.s. .N.T.\.T.a.b.l.e.T.e.x.t.S.e.r.v.i.c.e.\.T.a.b.l.e.T.e.x.t.S.e.r.v.i.c.e...d.l.l.,.-.1.6.".....I.c.o.n.I.n.d.e.x.=.I.C.O.N._.Y.I.........[.C.o.n.f.i.g.u.r.a.t.i.o.n.].....S.h.o.w.I.n.c.r.e.m.e.n.t.a.l.C.a.n.d.i.d.a.t.e.I.m.m.e.d.i.a.t.e.l.y.=.1.....R.e.a.d.i.n.g.W.i.n.d.o.w...W.i.d.t.h.=.3.....F.o.n.t.F.a.c.e.N.a.m.e.=.M.i.c.r.o.s.o.f.t. .Y.i. .B.a.i.t.i.....F.o.n.t.S.i.z.e.=.1.4.........[.P.r.e.s.e.r.v.e.d.K.e.y.].....G.u.i.d.I.m.e.M.o.d.e.=.{.9.8.2.1.3.4.9.4.-.3.6.7.A.-.4.8.5.5.-.9.0.A.1.-.9.7.D.9.1.7.E.3.E.C.3.D.}.....K.e.y.D.e.f.i.n.e.I.m.e.M.o.d.e.=.V.K._.S.H.I.F.T.,. .T.F._.M.O.D._.O.N._.K.E.Y.U.P._.S.H.I.F.T._.O.N.L.Y.....D.e.s.c.r.i.p.t.

C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\Z_Custom2.ini	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	Generic INItialization configuration [allData0]
Category:	dropped
Size (bytes):	6221
Entropy (8bit):	4.623864089058378
Encrypted:	false
SSDEEP:	96:KGz5QTZR5ATsj5sjc9sjnljnDQcaufEjnOAvtDAvVY:BzmTZbAojyjnjljspu8jXvtMvVY
MD5:	CA003CF1D99CDF717768E88DD64BB84C
SHA1:	A0326E46EA68C4649DD6645368B43922B6126FF6
SHA-256:	44100D5F41FE4CDDD1D77EF7124FEC4F8071E5A1678339ACE0DA3DD7E826EF2F
SHA-512:	94D1EB659C22A3614F250C79D1C957876A617158BE538E35E906F12E68C6E12CCBE9C364D1F1C18D280F72FD7958D753348C056CAF320B6843EC3873B59C992
Malicious:	false
Reputation:	low
Preview:	[Config]..modeIndex=1..allIndex=1..wasdIndex=0..qwerIndex=0..fourIndex=0..syncIndex=0....[allData0]..ColorR=255..ColorG=0..ColorB=0..Color2R=0..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=0..TemperatureH=0..TemperatureL=0..StrobingRandom=0....[allData1]..ColorR=8..ColorG=255..ColorB=240..Color2R=255..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=0..TemperatureH=0..TemperatureL=0..StrobingRandom=0....[allData2]..ColorR=255..ColorG=0..ColorB=0..Color2R=0..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=0..TemperatureH=0..TemperatureL=0..StrobingRandom=0....[allData3]..ColorR=0..ColorG=0..ColorB=0..Color2R=0..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=3..TemperatureH=0..Tempe

C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	4.63717105728589
Encrypted:	false
SSDEEP:	768:5U0SzA63tPY1AcbERQzuahkbzM7hX2O4HvypROPzMiibjUsqK0M49uo:5OU63tPY114RX3M7MvPy/OPz/CF09F
MD5:	299DBB927B6390C6B925757DD5B2B7FF
SHA1:	FFCE563E42AF7B1086CB5AE92014801B2C66DC0C
SHA-256:	D9D2BD64DE6176B31A4E704D7E5D08FA9BB75A6A8AC007A61C4DF38F6FA82262
SHA-512:	E88F9DA34960BC13C27F2B236A28410AC8B71619D8175103D0BD5E7F03F395F773BCDF399E805D2150BECF2EE107147287D6FE0C00BD41AC591F868E6229634
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........<..R...R...R......R..P...R.Rich..R.PE..d................." ....0.......Z....`.. ....8...rdata...........................@..@.rsrc........ ....@..@................T...8...8...................$...................8....rdata..8...x....rdata$zzzdbg.... ....rsrc$01..... ....rsrc$02.... .....A..R...)h.s.V.2..d.v.9.. ....

C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\ArtDeco_brown_22.bmp

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.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):	7968
Entropy (8bit):	7.906040167483731
Encrypted:	false
SSDEEP:	192:oXRXorJ1fquj4/Ms9hHCQyTscIhlMN58ZB5oEx5/U8qn8kyx:KRoqu0ksEIhCOjZU8M8kM
MD5:	162F6BB32D6D5AC380A80DA07C13E213
SHA1:	7985EAC367E0B19CC0E30B24399A37663E8436F6
SHA-256:	686310A1A5B8BB4D4EAA316FC0A3970EE878CC39F75E8C68F49ED51A5AD562DF
SHA-512:	F4DC70FB483303906CA8C4D5AE404653C7B761BEB38B3DC88ABDEBED4B28A85F3A02F6E2E1E5D28A1625F09A8EEA7A66F12959AA12E98733023CE5908B9FF199
Malicious:	false
Preview:	......JFIF.....d.d.....:Exif..MM.*......Q...........Q..........aQ..........a.......C..C..n.n..".......... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?.....(..5...l...K.4.....t{.k..........^SD'...g....H.7.......d....=.....RmQ..{.x.. .mj....|Z.m'.|;<l.ykc...j.0X.h...f.O,..M.K.>.xG.......K..sZ...H|U.j.Z...y?,.m.n.[...l...J.(..QUG...(...z_. ...#....Ys=....?......>....?.}.;.V..@7.*.5..-.O...o.\F.....v.........~)...c}.O.....}b.%.........>a..Z.di.l.cH|.a

C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\Iconology.Ess

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	ASCII text, with very long lines (57606), with no line terminators
Category:	dropped
Size (bytes):	57606
Entropy (8bit):	2.670628012232385
Encrypted:	false
SSDEEP:	768:Ip+EachJRWeyBP/QmazA5Bnh+QuGkvrOYKT2Rrt6UptqyBcerao1CEzSkNu8R2QP:uquzgxiGXNyHlqgdeo1CtNQP
MD5:	1EE3EA9EB5F7142B93FE99689B2038A6
SHA1:	AB0D94BDBDC97EEA61B226010584C12D9AED43EA
SHA-256:	67D1985FCBEB4E6FB84785F6304B3CB63A9326B328921E04CCFD50539825FDB7
SHA-512:	BBC7EAEA47011BB96FD26ADB3B71F981AE20FDACCF1A72BAFE96EC8E3071AD29AE052B279465FA700B3AD327DC2EA97408B52FD5A0D73B716F21FCD500D30B67
Malicious:	false
Preview:	0000DB00000000B3B300008E0037373700E100DF0091910000D2D2D20000C1C100DFDF000000006A6A006F000000D80000000000003000004700000000000000037 37373737006E6E003F3F000000B70000C0C00000DDDDDDDD0000DE00B50000007E000303030034005D000900E1E1E1E1003A3A3A3A3A00E0000000A9 00000000D7D70000FCFC00007500F400950000515100EB00DD0000F000920000006A00001800530061610000222200072001B000010006D00B9B9B90000878787 00FEFEFE000072000000000004D00CFCF00007373000000A3A3008B8B00000000000000262600003E000000000000001C0000000000F5000076767600006060000010 10100030000000F10000000028280000000200006565000000000000000C7C70000004A005B00E1E1E1E1001A000000480056560068686800000C1000046006700 B3B300810000003900737300DA0029292900000BFBF009100005E0000001313130026260000000000000460000FFFFFFFFFF00B9B9B9B900000027000000E1E1E1 000000003800F1F1F10000001F002C0000008900000000616161600A0001F00B200002C2C2C2C2C009E00000000AC00004545006300 0A0A00F70000D900000003 030300AF00003300010100989800FDFD00000024242424008300560020D2D0053000000000000000000000000AB00000000EF

C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	251376
Entropy (8bit):	5.684541726348285
Encrypted:	false
SSDEEP:	3072:njOJemjvYiYtrWTovAYYYlDvNYXzMgv9/PuMKISOe1sWQuCyY+2JHfYavRkRYI1N:n+6v671nuMKRv1sHyaJ/YavRkRYIBYA1
MD5:	B44ED270A186763E1DA753AA39553B68
SHA1:	10390F85EA5DB841A8BC70E8ED931A5D34026BE8
SHA-256:	E24E9B9C79199B66B9F847F1E07A2769B82CB7FCCA98E5B53F28B481EEBCABD8
SHA-512:	0BF049851CBD5D29221E7C721F15E58286C030023A9BF66E88A5EE6D4D940F89CBBFB8A4E0376382472940450D631E7E3D0162C871443CA12169DFED4E7C91B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ......................@................................. ....!..L.!This program cannot be run in DOS mode....$.......43..pR..pR..pR..y*^.qR..y*N.xR....sR....}R....xR..pR..-S....wR ......JR..pR..dR......zR......oR......qR......qR..pRJ.qR......qR..RichpR.................PE..L...L..V...........!...@..........................P.......A ....+......8..........................@...@...text.............................. ..`.rdata..=A.......B.................@..@.data...D....`.......F..............@....r src............ ...V..............@..@.reloc...G.......H...v.............@..B... ....

C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	384128
Entropy (8bit):	5.921054568677329
Encrypted:	false
SSDEEP:	6144:zJteC/kw/VKk3g6ZK5RoyPAzv2B9NAlYRuKJOllo:zreCsO3g6QRoyPAw6eRh
MD5:	7E49C04017D860D5EE299FFB104203DF
SHA1:	DDF55616BDABC91EB801CE14A45ACDAD2142B78F
SHA-256:	1AC6E64459440B6EFB03FC256E24BCCBBC512CF6E7DCD85DD3C45E1CA7584176
SHA-512:	EC125C3CD1EDE0F4C24915BC39EA641F58F1D78048E0CCB631F249839440218B02706CC8ACA785DA2B3993EDBABEFB433BF19BA29A9F1EDFB6ACACBDDC0A 4F50
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$...........p...p...p....j..p...?...p.......p.......p.......p...p...p.......p.......p..... ..p..Rich.p..........................PE..d....=.N.........." ....L..@............@.. ....@............0......`E................. .............................@..............\|E..H............text............................... ..`.nep.......... ....`.rdata..v....@.......$..............@..@.data....<..........................@....pdata..@ ..........................@..@.rsrc........ ......................@..@.reloc..`....0......................@..B.. ....

C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\Sports-Wallpapers-1.jpg

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x786, components 3
Category:	dropped
Size (bytes):	782753
Entropy (8bit):	7.972739118836816
Encrypted:	false
SSDEEP:	12288:1xE6g9kiViGNq+W6nQNIDO0tVGb34eaR6fUnMlkTFztQywzV0jyB4Dl9l+qfkwPN:7E6G3VibpHIdebodR6jlKFtQVUv+iP8S
MD5:	E269DECCAC13CF01A0377872E79BC676
SHA1:	54D196FDE9529310F9E5A3EBA6548DAB4F179542
SHA-256:	255874E0A6A5CA862CBAE5C783D582729B343C70C5697062D7F1E587F15F25EC
SHA-512:	08ADAD38BE3472CF8814C40F99D6DCFDA313C2FED765B872AA30C0995B027F2BEDABF75DB625F3C40F003A8EFC3F41169CBA4AF706EC637018DEEF02EC92F 6CC
Malicious:	false
Preview:	......JFIF.....`.`.....XICC_PROFILE......HLino....mntrRGB XYZ ....1..acspMSFT....IEC sRGB.......................-HP ....cprt...P...3desc.......lwtpt.. ......bkpt........rXYZ........gXYZ...,....bXYZ...@....dmnd...T...pdmdd........vued...L....view.......$lumi........meas.......$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyrigh t (c) 1998 Hewlett-Packard Company..desc........sRGB IEC61966-2.1............sRGB IEC61966-2.1...XYZ ....Q........XYZ ....XYZ .. ....o...8.....XYZ ......b.........XYZ ......$.........desc........IEC http://www.iec.ch............IEC http://www.iec.ch...desc........IEC 61966-2.1 Default RGB colour space - sRGB............IEC 61966-2.1 Default RGB colour space - sRGB......................desc.......,Reference Viewing Condition in IEC61966-2.1...........,Reference V iewing Condition in IEC61966-2.1........

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9924781293877105
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:	DHL04AWB01173903102023PDF.scr.exe
File size:	1211760
MD5:	1bf124cc783ff47a91ada4e6d4ac9e6b
SHA1:	b78f2ffb785071ab785830cdd4cbc5f010b7480b
SHA256:	494d5735144af171cc15708b37b491b74be1522494958e605ac348dd4897dcf9
SHA512:	b5e35fda41aedb7c40961098745153efa13470d065ac2cfb343c542011ed58869494770615db8a7e4b64b77ac6dd2de4f1cfd1403efeceee8425993bdf66670b
SSDEEP:	24576:7RNsMRW/uL9M7e36FgHRcMSbA22c91uwozF2KDQcvhNfSf7a09Xe+bUe:c4suGm6SxcD2SczF2aQcffSDb99
TLSH:	214533D212E2B0B3D690D93B5D5D6E7EE173D60014B2274B7340A8AE6F38165AB1F374

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......1.D9u.*ju.*ju.*j..ujw.*ju.+j..*j..wjd.*j!..j..*j...jt.*jRichu.*j........PE..L....e.Q.................`...*.......3.......p....@

File Icon

Icon Hash:	74f0d0c0ccd4f0c4

Static PE Info

General

Entrypoint:	0x40331c
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:	0x519965DC [Sun May 19 23:53:00 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:	17b7d61bda0f7478e36d9ce3d4170680

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=inertnesses@Forbetoning20.En, OU="Falskspillere Unrelinquishable ", O=Inalterableness, L=Montague, S=Texas, C=US
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	• 7/10/2022 7:04:55 AM 7/9/2025 7:04:55 AM
Subject Chain	• E=inertnesses@Forbetoning20.En, OU="Falskspillere Unrelinquishable ", O=Inalterableness, L=Montague, S=Texas, C=US
Version:	3
Thumbprint MD5:	B6296BD55FD696653A6ECFD645239E12
Thumbprint SHA-1:	7B9D3A3205DB42A6F338C423028B131EDDD4F064
Thumbprint SHA-256:	F7E0D7AFE23FD9E15D7B7C6CB47B4662581AE209B91E9046AE6A7AAFDC37720B
Serial:	04D25D90CEF83AEC304DC1F83B1B5CCF54893695

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push ebp
push esi
push edi
push 00000020h
xor ebp, ebp
pop esi
mov dword ptr [esp+18h], ebp
mov dword ptr [esp+10h], 00409230h
mov dword ptr [esp+14h], ebp
call dword ptr [00407034h]
push 00008001h
call dword ptr [004070BCh]
push ebp

Instruction
call dword ptr [004072ACh]
push 00000008h
mov dword ptr [00429298h], eax
call 00007F18C9476A2Dh
mov dword ptr [004291E4h], eax
push ebp
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebp
push 00420690h
call dword ptr [0040717Ch]
push 0040937Ch
push 004281E0h
call 00007F18C9476698h
call dword ptr [00407134h]
mov ebx, 00434000h
push eax
push ebx
call 00007F18C9476686h
push ebp
call dword ptr [0040710Ch]
cmp word ptr [00434000h], 0022h
mov dword ptr [004291E0h], eax
mov eax, ebx
jne 00007F18C9473B8Ah
push 00000022h
mov eax, 00434002h
pop esi
push esi
push eax
call 00007F18C94760F4h
push eax
call dword ptr [00407240h]
mov dword ptr [esp+1Ch], eax
jmp 00007F18C9473C49h
push 00000020h
pop edx
cmp cx, dx
jne 00007F18C9473B89h
inc eax
inc eax
cmp word ptr [eax], dx
je 00007F18C9473B7Bh
add word ptr [eax], 0000h

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	0x7494	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4e000	0x7fc0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x127368	0xa08	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x2b8	.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	0x5e1c	0x6000	False	0.6542561848958334	data	6.407290112650426	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1354	0x1400	False	0.43046875	data	5.037834422880877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x202d8	0x600	False	0.47265625	data	3.7587363087821926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2a000	0x24000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x4e000	0x7fc0	0x8000	False	0.949371337890625	data	7.7369782578420665	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4e1d8	0x7562	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x55740	0x100	data	English	United States
RT_DIALOG	0x55840	0xf8	data	English	United States
RT_DIALOG	0x55938	0x60	data	English	United States
RT_GROUP_ICON	0x55998	0x14	data	English	United States
RT_VERSION	0x559b0	0x25c	data	English	United States
RT_MANIFEST	0x55c10	0x3b0	XML 1.0 document, ASCII text, with very long lines (944), with no line terminators	English	United States

Imports

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

DLL	Import
ADVAPI32.dll	RegCloseKey, RegOpenKeyExW, RegDeleteKeyW, RegDeleteValueW, RegEnumValueW, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	CoCreateInstance, CoTaskMemFree, OleInitialize, OleUninitialize
VERSION.dll	GetFileVersionInfoSizeW, GetFileVersionInfoW, VerQueryValueW

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: DHL04AWB01173903102023PDF.scr.exe PID: **1308**, Parent PID: **3528**

General

Target ID:	0
Start time:	18:04:13
Start date:	16/03/2023
Path:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
Imagebase:	0x400000
File size:	1211760 bytes
MD5 hash:	1BF124CC783FF47A91ADA4E6D4AC9E6B
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: 00000000.00000002.832197103.0000000006825000.00000040.00001000.00020000.00000000.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	40330F	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseEDA6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B94	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B94	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	6	4015E9	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	6	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Apicad	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Apicad\Outjinx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed\Coccosteid.Udr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Extracorpuscular	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Counts	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Counts\Convolution	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Counts\Convolution\Dottily	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\Iconology.Ess	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\ArtDeco_brown_22.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Thonny	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Thonny\Yderligheders	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\Sports-Wallpapers-1.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Clavichordist	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Clavichordist\benenders	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryW
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\TableTextServiceYi.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\Z_Custom2.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\AppData\Local\Temp\nsoF960.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B94	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4015E9	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	4015E9	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	4015E9	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	4015E9	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	4015E9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsoF960.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	4015E9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsoF960.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B52	CreateFileW
C:\Users\user\AppData\Local\Temp\nsoF960.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405B52	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseEDA6.tmp	success or wait	1	403534	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsoF960.tmp	success or wait	1	40575B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	0	32768	fd 33 00 00 01 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 11 00 00 fd 00 00 00 10 21 00 00 00 00 00 00 fd 32 00 00 01 00 00 00 fd 33 00 00 00 00 00 00 00 00 00 00 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 fd fd fd fd fd fd fd fd fd fd 77 fd fd 00 00 00 00 00 fd 00 00 00 2d fd 4a 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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	3,!23w-J	success or wait	2	40322B	WriteFile
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	52504	19352	fd 05 09 fd 02 52 fd fd 13 fd fd 2c fd 58 fd 00 fd fd 32 22 29 fd fd fd 57 39 fd 06 52 fd 32 fd 5f 57 fd fd 36 fd 19 2c fd 61 15 fd fd 26 09 05 fd 94 fd fd fd fd 61 fd fd fd 36 31 8c 3e fd 60 fd 61 fd 33 56 fd 2a fd 64 00 33 fd 6b 2e fd 10 fd fd 06 8c 62 59 fd 25 61 fd fd 79 5b fd 07 fd fd 54 0a 09 55 4f 76 fd 68 fd fd fd 78 52 fd fd fd fd 3f fd 40 fd 3e fd 7f fd 14 fd 76 3b 28 fd 65 fd 56 7f fd d6 fd fd fd fd fd 5d 57 7d fd 3d fd 2e 59 fd 31 62 5a 3e 31 30 25 fd fd 11 3c fd fd 39 fd 46 fd fd 5d 56 7f fd fd fd fd fd 5d 57 fd fd fd f3 0f 59 5f fd 4d fd 56 7f fd 56 fd fd 47 0a c9 bb fd 17 78 fd fd 48 38 fd 74 ab fd 0f fd 09 04 fd fd 40 fd 2f fd fd 7f fd 66 fd fd fd 5d 57 0a fd 60 fd 64 fd fd 58 fd fd 30 55	,X2")W9R2_W6,a&a61>` a3V*d3k.bY %ay[TOvhxR@>v; (eV]W}=.Y1bZ10%< 9F]V]WY_MVVGxHt@/f] W`dX0U	success or wait	89	40322B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed\Coccosteid.Udr	0	16384	41 41	AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAAAA AAAAAAAAAAAAA AAAAAAAAAAAAAAA	success or wait	13	4030C4	WriteFile
C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll	0	16384	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 20 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 34 33 fd fd 70 52 fd fd 70 52 fd fd 70 52 fd fd 79 2a 5e fd 71 52 fd fd 79 2a 4e fd 78 52 fd 54 10 fd 73 52 fd 54 13 fd 7d 52 fd 54 12 fd 78 52 fd fd 70 52 fd fd 2d 53 fd 54 16 fd 77 52 fd fd fd fd 1a fd 4a 52 fd fd 70 52 fd fd 64 52 fd fd 16 fd 12 fd 7a 52 fd fd 16 fd 0e fd 6f 52 fd fd 16 fd 17 fd 71 52 fd fd 16 fd 14 fd 71 52 fd fd 70 52 4a fd 71 52 fd	MZ@ !L!This program cannot be run in DOS mode.$43pRpRpRy*^qRy*NxRsR}RxRpR-SwRJRpRdRzRoRqRqRpRJqR	success or wait	16	4030C4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\Iconology.Ess	0	16384	30 30 30 30 44 42 30 30 30 30 30 30 30 30 42 33 42 33 30 30 30 30 38 45 30 30 33 37 33 37 33 37 30 30 45 31 30 30 44 46 30 30 39 31 39 31 30 30 30 30 44 32 44 32 44 32 30 30 30 30 43 31 43 31 30 30 44 46 44 46 30 30 30 30 30 30 30 30 36 41 36 41 30 30 36 46 30 30 30 30 30 30 44 38 30 30 30 30 30 30 30 30 30 30 30 30 33 30 30 30 30 30 34 37 30 30 30 30 30 30 30 30 30 30 30 30 30 30 33 37 33 37 33 37 33 37 33 37 30 30 36 45 36 45 30 30 33 46 33 46 30 30 30 30 30 30 42 37 30 30 30 30 43 30 43 30 30 30 30 30 44 44 44 44 44 44 44 44 30 30 30 30 44 45 30 30 42 35 30 30 30 30 30 30 37 45 30 30 30 33 30 33 30 33 30 30 33 34 30 30 35 44 30 30 30 39 30 30 45 31 45 31 45 31 45 31 30 30 33 41 33 41 33 41 33 41 33 41 30 30 45 30 30 30 30 30 30 30 41 39 30 30 30 30 30	0000DB00000000B3B300008E003737 3700E100DF0091910000 D2D2D20000 C1C100DFDF000000006 A6A006F0000 00D80000000000003000 0047000000 000000003737373737006 E6E003F3F 000000B70000C0C00000 DDDDDDDD00 00DE00B50000007E0003 0303003400 5D000900E1E1E1E1003 A3A3A3A3A00 E0000000A900000	success or wait	4	4030C4	WriteFile
C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\ArtDeco_brown_22.bmp	0	7968	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 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 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	4030C4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll	0	16384	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 11 7f 6f 70 11 fd fd 70 11 fd fd 70 11 fd fd fd 6a fd fd 70 11 fd 12 3f fd fd fd 70 11 fd fd 08 fd fd fd 70 11 fd fd 08 fd fd fd 70 11 fd fd 08 fd fd fd 70 11 fd fd 70 10 fd fd 70 11 fd fd 08 fd fd fd 70 11 fd fd 08 fd fd fd 70 11 fd fd 08 fd fd fd 70 11 fd 52 69 63 68 fd 70 11 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 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$pppjp?ppppppp pRichpPEd	success or wait	24	4030C4	WriteFile
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\Sports-Wallpapers-1.jpg	0	16384	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 fd fd 0c 58 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 0c 48 4c 69 6e 6f 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 fd 00 02 00 09 00 06 00 31 00 00 61 63 73 70 4d 53 46 54 00 00 00 00 49 45 43 20 73 52 47 42 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd fd 00 01 00 00 00 00 fd 2d 48 50 20 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 63 70 72 74 00 00 01 50 00 00 00 33 64 65 73 63 00 00 01 fd 00 00 00 6c 77 74 70 74 00 00 01 fd 00 00 00 14 62 6b 70 74 00 00 02 04 00 00 00 14 72 58 59 5a 00 00 02 18 00 00 00 14 67 58 59 5a 00 00 02 2c 00 00 00 14 62 58 59 5a 00 00 02 40 00 00 00 14 64	JFIF``XICC_PROFILEHLinomntrRGB XYZ 1acspMSFTIEC sRGB-HP cpr tP3descIwtptbkptrXYZgXYZ,bXYZ@d	success or wait	48	4030C4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\TableTextServiceYi.txt	0	16384	fd fd 5b 00 53 00 79 00 73 00 74 00 65 00 6d 00 5d 00 0d 00 0a 00 4c 00 61 00 6e 00 67 00 49 00 64 00 20 00 3d 00 20 00 4c 00 41 00 4e 00 47 00 5f 00 59 00 49 00 2c 00 20 00 53 00 55 00 42 00 4c 00 41 00 4e 00 47 00 5f 00 44 00 45 00 46 00 41 00 55 00 4c 00 54 00 0d 00 0a 00 47 00 75 00 69 00 64 00 50 00 72 00 6f 00 66 00 69 00 6c 00 65 00 3d 00 7b 00 34 00 30 00 39 00 43 00 38 00 33 00 37 00 36 00 2d 00 30 00 30 00 37 00 42 00 2d 00 34 00 33 00 35 00 37 00 2d 00 41 00 45 00 38 00 45 00 2d 00 32 00 36 00 33 00 31 00 36 00 45 00 45 00 33 00 46 00 42 00 30 00 44 00 7d 00 0d 00 0a 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e 00 3d 00 22 00 59 00 69 00 20 00 49 00 6e 00 70 00 75 00 74 00 20 00 4d 00 65 00 74 00 68 00 6f 00 64 00 22 00 0d	[System]LangId = LANG_YI, SUBLANG_DEFAULTGuidProfile={409C8376-007B-4357-AE8E-26316EE3FB0D}Description="Yi Input Method"	success or wait	3	4030C4	WriteFile
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\Z_Custom2.ini	0	6221	5b 43 6f 6e 66 69 67 5d 0d 0a 6d 6f 64 65 49 6e 64 65 78 3d 31 0d 0a 61 6c 6c 49 6e 64 65 78 3d 31 0d 0a 77 61 73 64 49 6e 64 65 78 3d 30 0d 0a 71 77 65 72 49 6e 64 65 78 3d 30 0d 0a 66 6f 75 72 49 6e 64 65 78 3d 30 0d 0a 73 79 6e 63 49 6e 64 65 78 3d 30 0d 0a 0d 0a 5b 61 6c 6c 44 61 74 61 30 5d 0d 0a 43 6f 6c 6f 72 52 3d 32 35 35 0d 0a 43 6f 6c 6f 72 47 3d 30 0d 0a 43 6f 6c 6f 72 42 3d 30 0d 0a 43 6f 6c 6f 72 32 52 3d 30 0d 0a 43 6f 6c 6f 72 32 47 3d 30 0d 0a 43 6f 6c 6f 72 32 42 3d 30 0d 0a 43 6f 6c 6f 72 33 52 3d 30 0d 0a 43 6f 6c 6f 72 33 47 3d 30 0d 0a 43 6f 6c 6f 72 33 42 3d 30 0d 0a 43 6f 6c 6f 72 34 52 3d 30 0d 0a 43 6f 6c 6f 72 34 47 3d 30 0d 0a 43 6f 6c 6f 72 34 42 3d 30 0d 0a 53 70 65 65 64 54 79 70 65 3d 32 0d 0a 44 69 72 65 63 74 54 79 70 65	[Config]modeIndex=1allIndex=1wasdIndex=0qwerIndex=0fourIndex=0syncIndex=0[allData0]ColorR=255ColorG=0ColorB=0Color2R=0Color2G=0Color2B=0Color3R=0Color3G=0Color3B=0Color4R=0Color4G=0Color4B=0SpeedType=2DirectType	success or wait	1	4030C4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb	0	16384	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 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd 1f fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 00 0e 01 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 0a 00 00 00 00 00 00 00 00 00 30 01 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichRPEd" 0	success or wait	5	4030C4	WriteFile
C:\Users\user\AppData\Local\Temp\nsoF960.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 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 50 45 00 00 4c 01 04 00 fd 65 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.$1uuusuar!qttRichuPELeQ!	success or wait	1	4030C4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe	unknown	512	success or wait	163	4032BC	ReadFile
C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe	unknown	4	success or wait	1	4032BC	ReadFile
C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe	unknown	16384	success or wait	1	4032BC	ReadFile
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	unknown	4	success or wait	1	40304E	ReadFile
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	unknown	13212	success or wait	1	403104	ReadFile
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	unknown	4	success or wait	9	40304E	ReadFile
C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe	unknown	16384	success or wait	69	4032BC	ReadFile
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	unknown	16384	success or wait	115	4030A8	ReadFile
C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\Iconology.Ess	unknown	1	success or wait	998	4025CC	ReadFile
C:\Users\user\AppData\Local\Temp\nseEDA7.tmp	unknown	4	success or wait	1	40304E	ReadFile
C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed\Coccosteid.Udr	unknown	49504256	success or wait	1	100028D5	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Goodtemperedness	success or wait	1	402373	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Goodtemperedness\Rendets	success or wait	1	402373	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Undisguisedness	success or wait	1	402373	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Undisguisedness\Landboeres	success or wait	1	402373	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Undisguisedness\Landboeres\Usseligt	success or wait	1	402373	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Goodtemperedness\Rendets	Skramles	unicode	TOLMEN	success or wait	1	4023CF	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Undisguisedness\Landboeres\Usseligt	Servicearbejde	expand unicode	%Syrefastes%\Syltetjsmadden\Disadvantages.Trk	success or wait	1	4023CF	RegSetValueExW

Disassembly

No disassembly