ID: 828743
Sample Name: invoice.exe
Cookbook: default.jbs
Time: 14:20:40
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

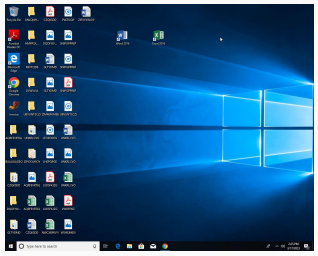
Windows Analysis Report

invoice.exe

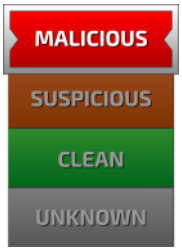
Overview

General Information

Sample Name:	invoice.exe
Analysis ID:	828743
MD5:	f111934675c34..
SHA1:	6c54e0fbae03d..
SHA256:	c627b8bb6c4e...
Tags:	exe signed
Infos:	



Detection

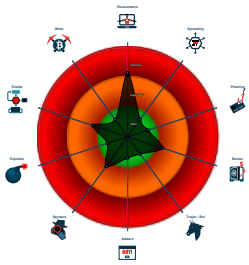


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Initial sample is a PE file and has a...
- Found potential ransomware deman...
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original ...
- Drops certificate files (DER)
- Drops PE files
- Contains functionality to shutdown /...
- Uses code obfuscation techniques (...
- PE file contains sections with non-s...
- Detected potential crypto function

Classification



Process Tree

- System is w10x64
- invoice.exe (PID: 2144 cmdline: C:\Users\user\Desktop\invoice.exe MD5: F111934675C34CCA18D9D76FC34A2E40)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

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

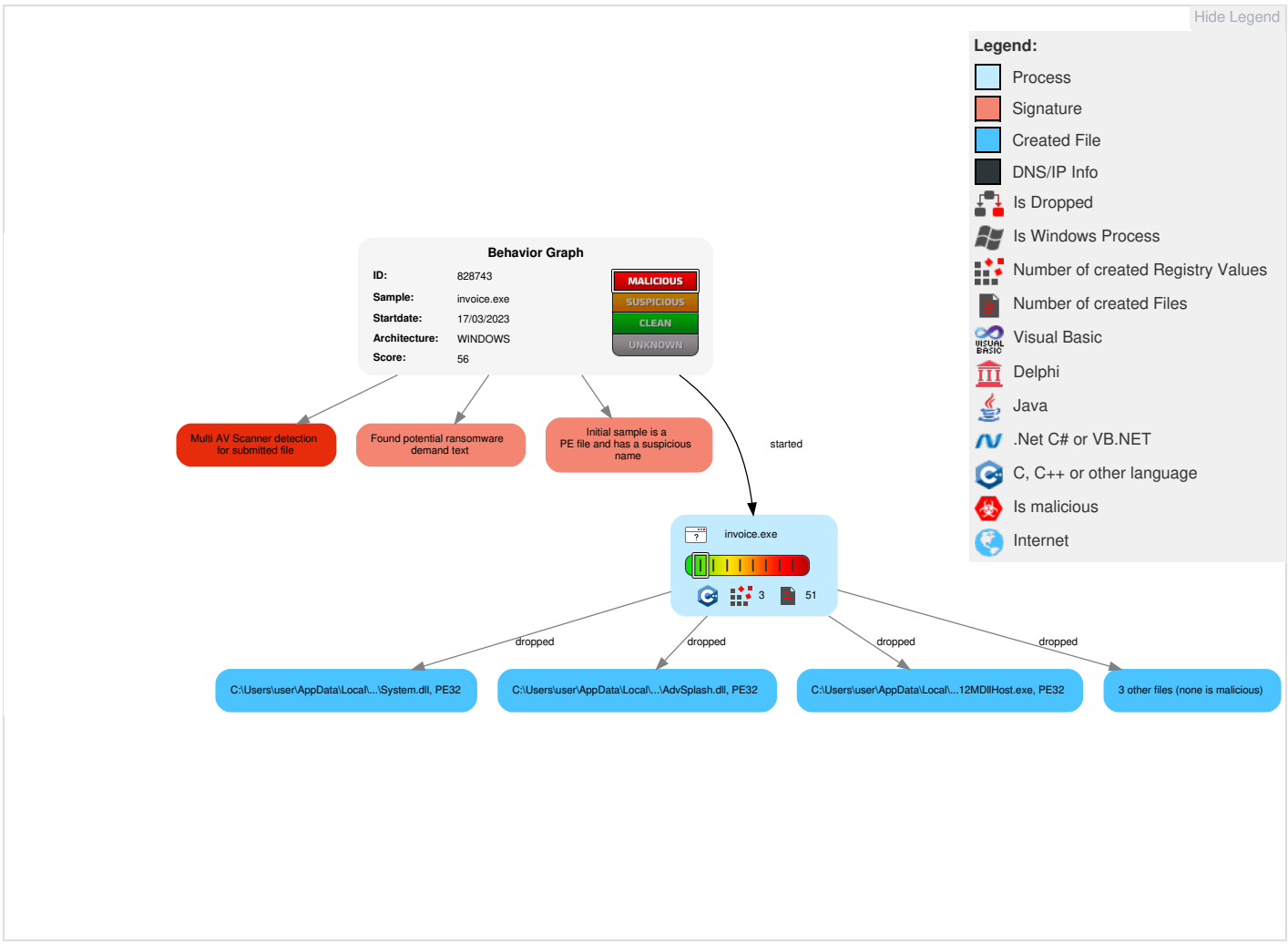
System Summary

Initial sample is a PE file and has a suspicious name

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	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	Boot or Logon Initialization Scripts	1 Access Token Manipulation	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	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

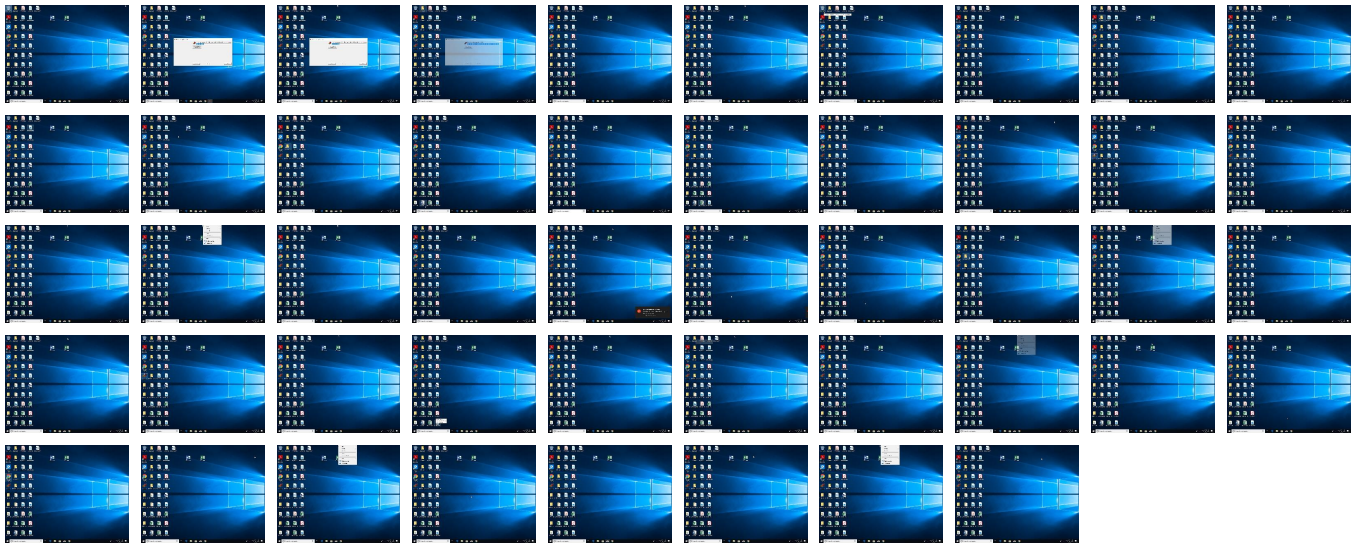
Behavior Graph



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
invoice.exe	36%	ReversingLabs	Win32.Trojan.Tnega	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\lang-1059.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Ath_CoexAgent.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\Mss32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\NMDllHost.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.invoice.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
0.0.invoice.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://www.avast.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://crl.certum.pl/ctsca2021.crl0o	invoice.exe	false		high
http://nsis.sf.net/NSIS_Error	invoice.exe	false		high
http://repository.certum.pl/ctnca.cer09	invoice.exe	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	NMDllHost.exe.0.dr, Mss32.dll.0.dr	false		high
http://repository.certum.pl/ctsca2021.cer0	invoice.exe	false		high
http://crl.certum.pl/ctnca.crl0k	invoice.exe	false		high
http://subca.ocsp-certum.com05	invoice.exe	false	• URL Reputation: safe	unknown
http://www.symauth.com/rpa00	NMDllHost.exe.0.dr	false		high
http://ocsp.thawte.com0	NMDllHost.exe.0.dr, Mss32.dll.0.dr	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com02	invoice.exe	false	• URL Reputation: safe	unknown
http://www.nero.com	NMDllHost.exe.0.dr	false		high
http://subca.ocsp-certum.com01	invoice.exe	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	invoice.exe	false		high
http://repository.certum.pl/ctnca2.cer09	invoice.exe	false		high
http://www.avast.com0/	invoice.exe, 00000000.00000002.837716661 .000000000040A000.00000004.00000001.0100 0000.00000003.sdmp, lang-1059.dll.0.dr	false	• URL Reputation: safe	unknown
http://scripts.sil.org/OFLSource	SourceCodePro-ExtraLight.otf.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	invoice.exe	false		high
http://www.symauth.com/cps0(	NMDllHost.exe.0.dr	false		high
http://www.certum.pl/CPS0	invoice.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828743
Start date and time:	2023-03-17 14:20:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
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:	invoice.exe
Detection:	MAL
Classification:	mal56.rans.winEXE@1/12@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.7% (good quality ratio 84.2%) • Quality average: 87.3% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 99% • 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
- VT rate limit hit for: invoice.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\icon-ui.icns

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\lang-1059.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	160264
Entropy (8bit):	4.358279117234243
Encrypted:	false
SSDEEP:	768:EVS3TP/nITMkSXnOLeecEKVdPGeGlo1ciX9NtfoxOpGHXGHmeVDj3bRQ9pY/ycVa:EVsPQBRodPDW4zMctML/
MD5:	B47C741673A92A16B48140FCBDA04030
SHA1:	AA7A003DA656320A274F276EE4BF8C27203D1B4C
SHA-256:	E6E775E7A5AC1BFA01B5A5CB9A7532171817408E67E346E33CA3CB091BDEA478
SHA-512:	464BFC63FD715E07C02ED78F9603A1C890F3848C0D46BB7B58D352B3FF1E76612E8D772903C9954159586735567DD493A023BCFADA5E15407725F7267567DC60
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.@...R.@.P...R.Rich..R.....PE..L....\)b..... .....!.....P.....p.....V....@..... ...M.....R... .....rdata..p..... .....@..@.rsrc....M... ...N.....@..@.....\)b.....T.....rdata.....T....rdata$zzzdbg.... ... ...rsrc$01.....@..H,...rsrc$02..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Ath_CoexAgent.exe

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	323584
Entropy (8bit):	6.212800759462987
Encrypted:	false
SSDEEP:	3072:KW+Rs18sEZQEwgD+odVKFKLuFv1kJV0YVJL/vFU/lmJ03Hk7OJ3/b7FG66sN4IqF:j7SdPKZ1kJLLH+lmJgHeOVb7o663L
MD5:	86B8B1F5C1189D68B07666784BE882FE
SHA1:	B023E9442CFC9C9652E1C8990F06DEF08BDC5B01
SHA-256:	0DD8C627F3DDBDB61B1910540C465C0D62C9F8D84C7CBB6C80782DB02D535AF0
SHA-512:	E471BEBDD441756CD840420C862CD84EF18A03144DDCAA20D783399D0736BD012D3984E38BDDB9DF16837B205D0A6ECA4C6FEE1D41553B5002A4B1E1B753E39
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mZ.z...z..z....~..z....n..z....m..z.....z...z...z....q..z.....z....{..z..Rich.z.....PE..L....(.P.....p...p.....@.....@...<.....P.....N..@.....text....n.....p..... ..`.rdata..... .....@..@.data...@Y.....@.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Diskofils\Justiciaryship\vmusbmouse.cat

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	10376
Entropy (8bit):	7.080841609849737
Encrypted:	false
SSDEEP:	192:pL/2EJC+EhGRmwBYyKaWFWQFV5NB0884LfqnajnWc:11PCFRVJlLWc
MD5:	DBE99D951395F37E5C3F4164D8A22245
SHA1:	238EF179549F6AEB2E3C6F4188365814A965312B
SHA-256:	671CB26C75AC0256B07835AE00E7018AF6126FAE7400BF21E57707E0CC9164B5
SHA-512:	3A931015C1038965028AD70E439F75BA210B1113BBCD8A7C5063DA376DBB577F250BE6141B93F1CB100084A930DAD4B2205864F19F3A5E3911CD6CC0B6D0D0D
Malicious:	false
Reputation:	low
Preview:	0.(...*.H.....(u0.(q...1.0...`.H.e.....0..h..+.....7.....Y0..U0...+.....7.....V...\B.....*..200624081447Z0...+.....7.....0..N0....RA.A.1.6.5.E.2.A.3.9.8.5.E.4.A.A.5.A.9.2.5.3.8.8.2.1.2.1.4.B.1.0.8.3.5.2.3.D.B.F...1..O0@..+.....7...1200...F.i.l.e.....v.m.u.s.b.m.o.u.s.e...s.y.s...0M..+.....7...1?0=0...+.....7...0.....0!0...+.....^*9..Z.S.!!K..R=.0X..+.....7...1J0H...O.S.A.t.t.r.....22.:.6...0.,.2.:.6...2.,.2.:.6...3.,.2.:.1.0...0...0b..+.....7...1T0R.L.{.C.6.8.9.A.A.B.8.-.8.E.7.8.-.1.1.D.0.-.8.C.4.7.-.0.0.C.0.4.F.C.2.9.5.E.E.}....0....RC.2.2.3.E.C.C.5.6.2.3.D.1.E.C.D.2.3.A.8.0.9.C.A.D.4.B.5.F.C.E.7.C.B.6.C.0.2.F.B...1..G0@..+.....7...1200...F.i.l.e.....v.m.u.s.b.m.o.u.s.e...i.n.f...0E..+.....7...17050...+.....7.....0!0...+.....#..b=..#.....l..0X..+.....7...1J0H...O.S.A.t.t.r.....22.:.6...0.,.2.:.6...2.,.2.:.6...3.,.2.:.1.0...0...0b..+.....7...1T0R.L.{.D.E.3.5.1.A.4.2.-.8.E.5.9.-.1.1.D.0.-.8.C.4.7.-.0.0.C.0.4.F.C.2.9.5.E.E.}.....0...0J..+.....7..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\Mss32.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	353768
Entropy (8bit):	6.836018886719178
Encrypted:	false
SSDEEP:	6144:EpcTapyHuUcl0PUpFawtMR6gP4aHrmtcWR3uA9:MIaQ+l0PoRtW6aHrmtcWRt9
MD5:	B75A8E0DDEEB4330C1DBA37105244B0F
SHA1:	E5302CA8517AC2826B5D56E3395D41C34B5B3DF7
SHA-256:	CC142B9D8B5223E2720C6440CB7A124C0A80D2FB04ECF59AD7331DFD6E3CB51F
SHA-512:	120F91A144B5B6CC9E33B232AE4466AF2E6C5F702F4C04E9A03DD4F239DE752770E4DE2C6BE2CAF3BEE9775C8887EAB9E08A896D7F2EBA1AD8CF928555CC99A3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.lq..."..."..."..."h.."..."..."..."e.."..."e..."k.."..."..."..."..."^.2"..."^.3"..."..."..."Rich..."........PE..L...#..<.....!.....!.....A.....0..p...P.....X.....N.....`T.....text....w.....x..... ..`MSSMIXER.G.....H...|..... ..`.rdata..%.....@..@.data.....F.....@....rsrc...X.....@..@.reloc..tW.....X.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\NMDllHost.exe

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116720
Entropy (8bit):	5.889271571414613
Encrypted:	false
SSDEEP:	3072:g3nqpX2l6OhctR+lCTD01Lcy4J93TnCx86:L2W1oy4J93TCT
MD5:	DBF787BD6E5CE77FB34FF281A144EB96
SHA1:	50B7799ECCA566BE35429828245D44CB04AD8885
SHA-256:	CCBACEEA04837229C95C08274C747ABE069279AFB990DDD89EC743C42ADC0AD9
SHA-512:	07949EC3882D9CB6E2341CE60C6E911F24463B01F484C037E65A2A8F3495543A096B632E01F8480D03FF388D1E811ECF760155F97F1D5329785C506603BB18A7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.L.u.L.u.LF.bL.u.LF.aL.u.LF.dL.u.LF.`L.u.L..,L.u.L..<L.u .L.u.L.t.Lu.|L.u.L...L.u.Lu.`L.u.Lu.fL.u.Lu.cL.u.LRich.u.L.....PE..L.....U.....@.....@.....E.....p..... .....`...8.....0&..@.....text..... ..`.rdata...N.....P.....@..@.data...p...`.....T.....@....shared..... .....^.....@....rsrc...p.....`.....@..@.reloc...K.....L...d.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Stemningssvingning\Urgently.Suk

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	ASCII text, with very long lines (52812), with no line terminators
Category:	dropped
Size (bytes):	52812
Entropy (8bit):	2.691443133069214
Encrypted:	false
SSDEEP:	768:w3MHvSSEEEE422O9Py2Ve76uBu+O3+xpnY/A8o9kxErpEEEbYRx+KmGSBAM07byk:bvS53XH/Y/A8opMr07bnr
MD5:	4C6FAD70762561B0D38AA152C52796A8
SHA1:	9FAFD1E9CF41E5482AC7960F7F0C20AB5B703D30
SHA-256:	C7CC1E08C3B0850EF02E7F4371D71918B55686581FDE5D124149884EE56C8F4F
SHA-512:	721DC72FF2153615343BCEC4B408337E8BD5012C234237F2005C43C48D1179DEDC1606014DE6659F5A22BC9116C2348C1AD5B05BF128D60572EEAE9346E06EE
Malicious:	false
Preview:	0000750000008400004300353535353500000DF0000006300858500 8D8D000000000000B7B7008F006100E2E2000000D3004600005D5D00F80000A10000E5E5E5E5E5E500000000DCDCDC000B0B0000F7F700000000D9D9D9D9D900000000000000B700EFEF0000B2B200DFDFDF0000DADA000000EEEEEEEEEEEEEEEE00670000050000E700D3000092929292000000 6E000083000B0B0B0017001D0000E700DF00DF00424242000073005B00BDBDBD00000000C6C60000323200000073006E6E005F5F000000BC00003000005B5B5B0015151515151500898989898990000002C2C0000960000202020000DA0000FD00C2005F000B0B0B002C000000BE00000000D40000DE005656565600393900000000000000000222200464646 00A0A0A000626200E5E5E500000000005D5D0000DA00000000323200DE008500003636363636360000000000001111000006D6D6D00D300FE00007C0000006000005D008181818181007B00777700A3000000C2006900B6B600C900005555555550040000036360090000002A00000000004A4A000000ADAD00B300000F000000002F2F2F00DC0034343400000000BCBC0000006F000061002C000010100000000000 4E4E4E4E008900FB00212100000000700000 4800A9001400CC000000000000000042424200E8000000007700000000500000000A900000000A2A2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\SourceCodePro-ExtraLight.otf

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	127080
Entropy (8bit):	7.036042013030407
Encrypted:	false
SSDEEP:	3072:Tz0LOC7z/0cS/Uz0+Gp+dtsVaHGg0IADoQg4RAxL2+p:s7z/0jUz0+GsdBHGg9cg4mvp
MD5:	9ECC8DF598E9EDDE1072942D344CC0CF
SHA1:	9FF240AB48EB7E97237E25D8C6F8CD738BA97CAA
SHA-256:	D945E1C81A59A434E36EEDEF21E64B61CC6901A9E43936AF79C20BDBF57592B1
SHA-512:	09978B7AF39B541C13F5E628BAF789E9FD1635258C74379351612451022D53B38B9F78DA7A74C19BA0FFB7B0C93B63C69EFCFC36285EFBCAF3678ADE7D423AD0
Malicious:	false
Preview:	OTTO.....`BASEe.].....FCFF 0.....Ft..i.DSIG.....`....GDEF.....GPOS.s.....vGSUB..]....T...JOS/2.....P...`cmap.spB.....3fhead..h.....6hhea.3.....$...$hmtx:C<... .....Bmaxp. P....H....nameCt.....:post...3..FT... .....JC_.<.....L.:...$.....X.L.L.....P.. ....X.....X...K...X...^.2..... ....8.....ADBO... . .....`..... ....J.~.....$.....<.....H.....T.....`.....l.....&.~.....&.....*.....6.....D.*.....:.n.....2.....$..... .....D.*.....4.....R.....4.....d.l.....0.....4.....4.....2.(..... .Z.....4.z..... ..&.....8.....J.....\.....$.n..... .....,.....0.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\cs.txt

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	9204
Entropy (8bit):	5.371514089173945
Encrypted:	false
SSDEEP:	192:iRJ98lWxEb5BvGIrd+mc1OTno+SXhbSIm1JjSvcQpK/w:ijK0GeIrQmEOTno+SXox1JjmpKo
MD5:	641B90F9AEDFC68486D0D20B40F7ECA6
SHA1:	0A683DD844534905336784FADD80498AFE26F6FA
SHA-256:	87A4B9369FD51D76C9032C0E65C3C6221659E086798829072785BE589E55B839
SHA-512:	567CB9F6C31D196A171E5A9C2726A39A9B3D351AC92D4ACF8624213A68C9033ACC31AFAAAD82AA9F5359F32D3A0CA40522E151B8370D553A41ABEB6A6E097078
Malicious:	false

Preview:	.;!@Lang2@!UTF-8!..; 4.30 : Milan Hrub...; 4.33 : Michal Molhanec..; 9.07 : Ji.. Mal.k..; 15.00 : Kry.tof .ern...;..;..;..;..;..;..;..0..7-Zip..Czech...e.tina..401..OK..Storno.. .....&Ano..&Ne..Zav..&t..N.pov.da....Po&kra.ovat..440..Ano na &v.echno..N&e na v.echno..Zastavit..Spustit znovu..&Pozad...P&op.ed...Po&zastavit..Pozastaveno..Jste si jist., .e to chcete stornovat?..500..&Soubor...pr&avy..&Zobrazen...&Obl.ben...&N.stroje..N.po&v.da..540..&Otev..t..Otev..t u&vnit...Otev..t &mimo..&Zobrazit..&Upra vit..&P.ejmenovat..Kop.rovat &do.....P.&esunout do.....Vymaza&t..&Rozd.lit soubor.....&Slou.it soubory.....Vlast&nosti..Pozn.mk&a..Vypo..tat kontroln. sou.et..Porovnat so ubory..Vytvo.it slo.ku..Vytvo.it soubor..&Konec..Odk.zat..&Alternate Streams..600..Vybrat &v.e..Zru.it v.b.r v.e..&Invertovat v.b.r..Vybrat.....Zru.it v.b.r.....Vybrat podle typu.. Zru.it v.b.r podle typu..700..&Velk. ikony..&Mal. ikony..&Seznam..&Podrobn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\figuranternes.Han

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	218305
Entropy (8bit):	7.337101777894853
Encrypted:	false
SSDEEP:	3072:PdqWTzg/gzZ9xRpRmib28JUBTE+vAsGolsJAsJ7Z/aKespGgyfZrl:HOaZ1nv9J2l+veZiKe2i
MD5:	DF0C864AD6FE636F3AD391B04A408AC7
SHA1:	B0072D5406BA66EDD9F6A1A443D56378BDA688C5
SHA-256:	A802EB02B9345615A947C6B8B57441D7DEBD4300FFEAFC16623CE18F68CABBF2
SHA-512:	2AA97CC2724CA1309B3594F552BAF227CCB7B6F73B29E612A9779D987E9FBE0E41F7CE765083AE16CD3CEC84B826A401279D69200D1AE3A0722B4E3CC73107C
Malicious:	false
Preview:	.....kkk.....****...u.....|.....44...e..... .DD..TTT.....""".....UU...[[[.....<<.....qq.....l.....1.*.....4.....f..... .....(.....{{.....1.....q....66.....:.....mmm.....55.'.....111...99.x.LLLLL.....~.....""...)).....#..... .....@@.b.....4.0....&.....|.....||.....ppp.8.....ww.....W..&...*.....`````.....~.....O.,,.....C.....F.....\.....HH HHHHH.....o.....^^...d.....ff..... ..D.....I....W.....\.....y..F....ppp..r.....)).....".....o.....9.22.....~~~.QQQ .....C.....6.....~~.....

C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\AdvSplash.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.76010720109437
Encrypted:	false
SSDEEP:	96:HqNXqwK188CgAtXvZBkjDf0yf9ysrtWp2wol:HAqrg1XvZB6kYtWp2
MD5:	88C3BA1802AEF228541820767453E058
SHA1:	4F3AEFB9E4EC27CB49973CB19BD968E54A2BA676
SHA-256:	2722555EC1F72523774B64D25FD4C2B460000BFE82140876D6100DC4FB1F62B1
SHA-512:	718790339E13B53553AFDE6968AE10CDA7B47CBDBFC82599116C8B5B1E8FBBA259F0CE6781908BE027360132A0ABE057DF2FFA7072212ACDA96BFF535E241582
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....P$..E.... ..d.....@..$..... ..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\System.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.767999234165119
Encrypted:	false
SSDEEP:	192:cPtkumJX7zBE2kGwfy9S9VkPsFQ1MZ1c:N7O2k5q9wA1MZa
MD5:	C9473CB90D79A374B2BA6040CA16E45C
SHA1:	AB95B54F12796DCE57210D65F05124A6ED81234A
SHA-256:	B80A5CBA69D1853ED5979B0CA0352437BF368A5CFB86CB4528EDADD410E11352
SHA-512:	EAFE7D5894622BC21F663BCA4DD594392EE0F5B29270B6B56B0187093D6A3A103545464FF6398AD32D2CF15DAB79B1F133218BA9BA337DDC01330B5ADA804D7B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.953363965326294
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:	invoice.exe
File size:	861416
MD5:	f111934675c34cca18d9d76fc34a2e40
SHA1:	6c54e0fbae03df56fee84195f3deb4d2ebd8d8c1
SHA256:	c627b8bb6c4ea0cf03aa2d209d0ecc53ff9784283328dabd44c1675aef0939c2
SHA512:	48b825550b320ebfcccc4260e359ffedad7675913ee7e7a62bd62a3839fd20c8f7cafb9a6e6bb8d7d8a2164674019b696c8851362c0a6b69f4dde8b1da3dc84c
SSDEEP:	12288:cJAEzBf4FZZmubGJ6vVZgj9Zp4RVkdXALai8ZpP7MxhGmeLJfRriFm4gCb5vr:cJBf4guba6voj9mOdXALN8bP7MxhVP5
TLSH:	090523919D24D01ACFCB1A32C6E0AAF51FA93D1DF546350FAB103DDE7AB3016992E1D8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L...2.uY.....d...|.....

File Icon

Icon Hash:	185d7c3f1d094720

Static PE Info

General

Entrypoint:	0x4031f1
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:	0x59759532 [Mon Jul 24 06:35:30 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:	3abe302b6d9a1256e6a915429af4ffd2

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Levnendes@Printstnings.Gum, OU="Berlinsk Absorptively Uncatholicise ", O=Toffy, L=Parbrook, S=England, C=GB
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	• 5/4/2022 1:03:57 AM 5/3/2025 1:03:57 AM
Subject Chain	• E=Levnendes@Printstnings.Gum, OU="Berlinsk Absorptively Uncatholicise ", O=Toffy, L=Parbrook, S=England, C=GB
Version:	3

Thumbprint MD5:	56C9BA7DFEC92471D18B65DEBADFD264
Thumbprint SHA-1:	791103B8F445F30749CC09454489D8932043151F
Thumbprint SHA-256:	12660D9C667AA56EF5F4D3C7A46C00BBF32786E1EDB7C6D1BB2EFDC10DDE5337
Serial:	292387F23D7D31A4C4A61C828EB508755809B6A4

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A0h]
call dword ptr [0040809Ch]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F40Ch], eax
je 00007F8F7CA0DE63h
push ebx
call 00007F8F7CA10F1Ah
cmp eax, ebx
je 00007F8F7CA0DE59h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007F8F7CA10E96h
push esi
call dword ptr [00408098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F8F7CA0DE3Dh
push 0000000Ah
call 00007F8F7CA10EEEh
push 00000008h
call 00007F8F7CA10EE7h
push 00000006h
mov dword ptr [0042F404h], eax
call 00007F8F7CA10EDBh
cmp eax, ebx
je 00007F8F7CA0DE61h
push 0000001Eh
call eax
test eax, eax
je 00007F8F7CA0DE59h
or byte ptr [0042F40Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4D8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax

Instruction
push ebx
push 00429830h
call dword ptr [00408178h]
push 0040A188h

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	0x8534	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x41000	0x219c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xd02c0	0x2228	
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	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6254	0x6400	False	0.6676171875	data	6.4338643172916266	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1354	0x1400	False	0.4599609375	data	5.236269898436511	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25518	0x600	False	0.4557291666666667	data	4.044625496015545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x30000	0x11000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x41000	0x219c8	0x21a00	False	0.8901312732342007	data	7.609648735329348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x41418	0x1224f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x53668	0x6259	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0x598c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x5be70	0x2466	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0x5e2d8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x5f380	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x60228	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x60ad0	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x61138	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x616a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x61b08	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x61df0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x61f18	0x120	data	English	United States
RT_DIALOG	0x62038	0x11c	data	English	United States
RT_DIALOG	0x62158	0xc4	data	English	United States
RT_DIALOG	0x62220	0x60	data	English	United States
RT_GROUP_ICON	0x62280	0xae	data	English	United States
RT_VERSION	0x62330	0x354	data	English	United States
RT_MANIFEST	0x62688	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

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

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: invoice.exe PID: 2144, Parent PID: 3528

General

Target ID:	0
Start time:	14:21:38
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice.exe
Imagebase:	0x400000
File size:	861416 bytes
MD5 hash:	F111934675C34CCA18D9D76FC34A2E40
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfE50D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B61	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B61	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4055DB	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4055DB	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4055DB	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsfE5AA.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	40559B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\AdvSplash.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055DB	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055DB	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\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	6	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\figuranternes.Han	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Ath_CoexAgent.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Stemningssvingning	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Stemningssvingning\Urgently.Suk	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\Mss32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\NMDllHost.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\SourceCodePro-ExtraLight.otf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\cs.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\icon-ui.icns	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\lang-1059.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Diskofils	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\prepository\Diskofils\Justiciaryship	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\prepository\Diskofils\Justiciaryship\vmusbmouse.cat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	284	4055DB	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	286	4055DB	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	286	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	285	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Jordebog	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Jordebog\Personeity89	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Jordebog	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	285	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Jordebog\Personeity89	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	285	4055DB	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2A	CreateFileA
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405B2A	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsfE50D.tmp	success or wait	1	40346A	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp	success or wait	1	40575C	DeleteFileA

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\nsfE5AA.tmp\AdvSplash.dll	0	5632	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 2b fd 59 16 6f fd 37 45 6f fd 37 45 6f fd 37 45 6f fd 36 45 46 fd 37 45 fd fd 6a 45 66 fd 37 45 3b fd 07 45 6d fd 37 45 fd fd 33 45 6e fd 37 45 52 69 63 68 6f fd 37 45 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 00 fd 75 59 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 08 00 00 00 0a 00 00 00 00 00 00 60 11 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$+Yo7Eo7Eo7Eo6 E F7EjEf7E;Em7E3En7ERi cho7EPELuY!`	success or wait	1	405BBF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\prepository\figuranternes.Han	0	32768	00 00 00 00 00 00 00 00 6b 6b 6b 00 1a 1a 00 fd 00 00 00 00 00 2a 2a 2a 2a 00 fd 00 75 00 00 07 07 00 fd 00 00 00 00 fd 00 00 fd 00 00 fd 00 00 00 fd 00 00 00 fd fd 00 00 7c 00 00 00 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 fd fd 00 fd 00 00 34 34 00 00 00 65 00 00 fd fd 00 00 fd fd fd 00 00 00 20 20 00 44 44 00 00 54 54 54 00 00 fd 00 11 00 00 00 fd fd fd 00 00 0f 0f 00 00 22 22 00 00 1c 00 00 fd fd fd 00 00 00 fd fd 00 0f 0f 0f 0f 0f 0f 0f 0f 00 00 00 fd 00 00 00 00 00 55 55 00 00 00 5b 5b 5b 00 00 00 fd 00 00 3c 3c 00 fd fd 00 00 00 00 00 00 71 71 00 00 fd 00 00 fd 00 00 00 6c 00 fd fd fd 00 00 00 00 00 00 00 fd 00 00 fd fd 00 00 00 31 00 2a 00 fd 00 00 00 00 00 34 00 00 fd fd 00 00 00 00 66 00 fd fd 00 00 fd fd 00 00 00 09 00 00 fd 00 fd 00 00 00 00	kkk****u|44e DDTTT""UU[[[<<qql1*4f	success or wait	12	405BBF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Ath_CoexAgent.exe	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 fd 1b 6d 5a fd 7a 03 09 fd 7a 03 09 fd 7a 03 09 fd fd 7e 09 fd 7a 03 09 fd fd 6e 09 18 7a 03 09 fd fd 6d 09 fd 7a 03 09 fd 02 fd 09 fd 7a 03 09 fd 7a 02 09 1a 7a 03 09 fd fd 71 09 fd 7a 03 09 fd fd 7f 09 fd 7a 03 09 fd fd 7b 09 fd 7a 03 09 52 69 63 68 fd 7a 03 09 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 28 fd 50 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 08 00 00 70 03	MZ@!L!This program cannot be run in DOS mode.$mZzzz~znzmzzzz qzz{zRichzPEL(Pp	success or wait	14	405BBF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Stemningssvingning\Urgently.Suk	0	32768	30 30 30 30 37 35 30 30 30 30 30 30 38 34 30 30 30 30 34 33 30 30 33 35 33 35 33 35 33 35 33 35 30 30 30 30 44 46 30 30 30 30 30 30 36 33 30 30 38 35 38 35 30 30 38 44 38 44 30 30 30 30 30 30 30 30 30 30 30 30 42 37 42 37 30 30 38 46 30 30 36 31 30 30 45 32 45 32 30 30 30 30 30 30 44 33 30 30 34 36 30 30 30 30 35 44 35 44 30 30 46 38 30 30 30 30 41 31 30 30 30 30 45 35 45 35 45 35 45 35 45 35 30 30 30 30 30 30 30 30 44 43 44 43 44 43 30 30 30 42 30 42 30 30 30 30 46 37 46 37 30 30 30 30 30 30 30 30 44 39 44 39 44 39 44 39 44 39 30 30 30 30 30 30 30 30 30 30 30 30 30 30 42 37 30 30 45 46 45 46 30 30 30 30 42 32 42 32 30 30 44 46 44 46 44 46 30 30 30 30 44 41 44 41 30 30 30 30 30 30 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 30 30 36 37 30 30 30 30 30	000075000000840000430035353535350000DF00000063008585008D8D000000000000B7B7008F006100E2E2000000D3004600005D5D00F80000A10000E5E5E5E5E500000000DCDCDC000B0B0000F7F700000000D9D9D9D9D900000000000000B700EFEF0000B2B200DFDFDF0000DADA000000EEEEEEEEEEEEEEEE006700000	success or wait	2	405BBF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\Mss32.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 4e fd 6c 71 0a fd 02 22 0a fd 02 22 0a fd 02 22 0a fd 03 22 fd fd 02 22 68 fd 11 22 0d fd 02 22 fd fd 0c 22 10 fd 02 22 65 fd 09 22 0b fd 02 22 65 fd 08 22 6b fd 02 22 fd fd 04 22 0b fd 02 22 fd fd 07 22 0b fd 02 22 5e fd 32 22 03 fd 02 22 5e fd 33 22 1a fd 02 22 fd fd 06 22 0b fd 02 22 52 69 63 68 0a fd 02 22 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 23 fd fd 3c 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Nlq""""""h""""e ""e"k""""""^2""^3""""Rich"PEL#<	success or wait	14	405BBF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\NMDllHost.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 14 fd 1f fd 75 fd 4c fd 75 fd 4c fd 75 fd 4c 46 fd 62 4c fd 75 fd 4c 46 fd 61 4c fd 75 fd 4c 46 fd 64 4c fd 75 fd 4c 46 fd 60 4c fd 75 fd 4c fd 0d 2c 4c fd 75 fd 4c fd 0d 3c 4c fd 75 fd 4c fd 75 fd 4c fd 74 fd 4c 75 fd 7c 4c fd 75 fd 4c fd fd 04 4c fd 75 fd 4c 75 fd 60 4c fd 75 fd 4c 75 fd 66 4c fd 75 fd 4c 75 fd 63 4c fd 75 fd 4c 52 69 63 68 fd 75 fd 4c 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$uLuLuLFbLuLFaLuLFdLuLF`LuL,LuL<LuLuLtLu|LuLL uLu`LuLufLuLucLuLRichuL	success or wait	6	405BBF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\SourceCodePro-ExtraLight.otf	0	30168	4f 54 54 4f 00 0e 00 fd 00 03 00 60 42 41 53 45 65 1e 5d fd 00 01 fd 18 00 00 00 46 43 46 46 20 30 10 fd fd 00 00 46 74 00 01 69 0f 44 53 49 47 00 00 00 01 00 01 fd 60 00 00 00 00 08 47 44 45 46 fd 0d fd fd 00 01 fd fd 00 00 02 fd 47 50 4f 53 fd 73 fd fd 00 01 e0 00 00 14 76 47 53 55 42 01 fd 5d 05 00 01 fd 54 00 00 1d 4a 4f 53 2f 32 fd 12 70 00 00 01 50 00 00 00 60 63 6d 61 70 07 73 70 42 00 00 12 fd 00 00 33 66 68 65 61 64 19 fd 68 fd 00 00 00 fd 00 00 00 36 68 68 65 61 06 33 00 fd 00 00 01 24 00 00 00 24 68 6d 74 78 3a 43 3c fd 00 01 fd fd 00 00 0c 42 6d 61 78 70 06 20 50 00 00 00 01 48 00 00 00 06 6e 61 6d 65 43 74 19 00 00 01 fd 00 00 11 3a 70 6f 73 74 fd fd 00 33 00 00 46 54 00 00 00 20 00 01 00 00 00 02 09 fd fd 04 4a 43 5f 0f 3c fd 00 03 03	OTTO`BASEe]FCFF 0FtiDSIG`GDEFG POSsvGSUB]TJOS/2P`c mapspB3fhea dh6hhea3$$hmtx:C<Bma xp PHnameCt:post3FT JC_<	success or wait	6	405BBF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\cs.txt	0	9204	ff 3b 21 40 4c 61 6e 67 32 40 21 55 54 46 2d 38 21 0d 0a 3b 20 20 34 2e 33 30 20 3a 20 4d 69 6c 61 6e 20 48 72 75 62 fd 0d 0a 3b 20 20 34 2e 33 33 20 3a 20 4d 69 63 68 61 6c 20 4d 6f 6c 68 61 6e 65 63 0d 0a 3b 20 20 39 2e 30 37 20 3a 20 4a 69 59 ed 20 4d 61 6c e1 6b 0d 0a 3b 20 31 35 2e 30 30 20 3a 20 4b 72 79 61 74 6f 66 20 0c 65 72 6e fd 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 30 0d 0a 37 2d 5a 69 70 0d 0a 43 7a 65 63 68 0d 0a 0c 65 61 74 69 6e 61 0d 0a 34 30 31 0d 0a 4f 4b 0d 0a 53 74 6f 72 6e 6f 0d 0a 0d 0a 0d 0a 0d 0a 26 41 6e 6f 0d 0a 26 4e 65 0d 0a 5a 61 76 59 ed 26 74 0d 0a 4e e1 70 6f 76 1b 64 61 0d 0a 0d 0a 50 6f 26 6b 72 61 0d 6f 76 61 74 0d 0a 34 34 30 0d 0a 41 6e 6f	;!@Lang2@!UTF-8!; 4.30 : Milan Hrub; 4.33 : Michal Molhanec; 9.07 : Ji Malk; 15.00 : Krytof ern;;;;;;;07-ZipCzechetin a401OKStorno&Ano&Ne Zav&tNpovda Po&kraovat440Ano	success or wait	1	405BBF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\prepository\Antimodernly\trever\Hovedinteressers\icon-ui.icns	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 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 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil	success or wait	1	405BBF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\prepository\Antimodernly\trever\Hovedinteressers\lang-1059.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 fd fd 3c fd fd fd 52 fd fd fd 52 fd fd fd 52 fd 40 fd fd fd 52 fd 40 fd 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 0a 5c 29 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 00 00 00 00 50 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$<RRR@R@PRRichRPEL\)b!P	success or wait	7	405BBF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Diskofils\Justiciary ship\vmusbmouse.cat	0	10376	30 fd 28 fd 06 09 2a fd 48 fd fd 0d 01 07 02 fd fd 28 75 30 fd 28 71 02 01 01 31 0f 30 0d 06 09 60 fd 48 01 65 03 04 02 01 05 00 30 fd 07 68 06 09 2b 06 01 04 01 fd 37 0a 01 fd fd 07 59 30 fd 07 55 30 0c 06 0a 2b 06 01 04 01 fd 37 0c 01 01 04 10 fd fd 56 fd 07 fd 5c 42 fd fd 1e fd fd fd 2a 17 0d 32 30 30 36 32 34 30 38 31 34 34 37 5a 30 0e 06 0a 2b 06 01 04 01 fd 37 0c 01 02 05 00 30 fd 03 4e 30 fd 01 fd 04 52 41 00 41 00 31 00 36 00 35 00 45 00 32 00 41 00 33 00 39 00 38 00 35 00 45 00 34 00 41 00 41 00 35 00 41 00 39 00 32 00 35 00 33 00 38 00 38 00 32 00 31 00 32 00 31 00 34 00 42 00 31 00 30 00 38 00 33 00 35 00 32 00 33 00 44 00 42 00 46 00 00 00 31 fd 01 4f 30 40 06 0a 2b 06 01 04 01 fd 37 0c 02 01 31 32 30 30 1e 08 00 46 00 69 00 6c 00 65 02 04	0(*H(u0(q10`He0h+7Y0U0+7V\B*20 0624081447Z0+70N0RA A165E2A3985 E4AA5A92538821214B1 083523DBF1O 0@+71200File	success or wait	1	405BBF	WriteFile
C:\Users\user\AppData\Local\Temp\nsfE5AA.tmp\System.dll	0	11264	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 29 fd fd fd 6d fd 6d fd 6d fd fd bd 6b fd 6d fd 7e b3 6e fd fd 6a fd 39 4c fd 69 fd 0e 16 fd 6c b3 52 b8 fd 6c fd 52 69 63 68 6d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 07 fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$)mmmkm~j9illRichPELuY!	success or wait	1	405BBF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\invoice.exe	unknown	512	success or wait	357	405B90	ReadFile
C:\Users\user\Desktop\invoice.exe	unknown	4	success or wait	2	405B90	ReadFile
C:\Users\user\Desktop\invoice.exe	unknown	4	success or wait	58	405B90	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Stemningssvingning\Urgently.Suk	unknown	1	success or wait	1023	405B90	ReadFile
C:\Users\user\Desktop\invoice.exe	unknown	4	success or wait	2	405B90	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hose11	success or wait	1	405E48	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hose11\Carnel146	success or wait	1	405E48	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hose11\Carnel146\Poly	success or wait	1	405E48	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hose11\Carnel146\Poly\Hedonophobia	success or wait	1	405E48	RegCreateKeyExA
HKEY_CURRENT_USER\Software\InstallDir32	success or wait	1	405E48	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Lejekasserner	success or wait	1	405E48	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hose11\Carnel146\Poly\Hedonophobia	Konsekvensmager	expand unicode	%Paleontol%\Installant\Laurbrkransens.und	success or wait	1	40245E	RegSetValueExA
HKEY_CURRENT_USER\Software\InstallDir32	Path	unicode	256	success or wait	1	40245E	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Lejekasserner	Fortrnelsens	dword	1	success or wait	1	40245E	RegSetValueExA

Disassembly

No disassembly