ID: 829095
Sample Name: o6OaOfrAQs
Cookbook: default.jbs
Time: 20:21:30
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

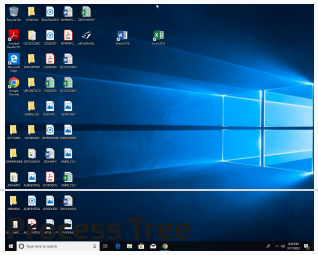
Windows Analysis Report

o6OaOfrAQs.exe

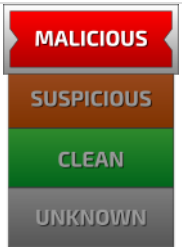
Overview

General Information

Sample Name:	o6OaOfrAQs.exe (renamed file extension from none to exe, renamed because original name is a hash value)
Original Sample Name:	cf9a08d65a0b4..
Analysis ID:	829095
MD5:	049ecad45875...
SHA1:	12aabeb19083...
SHA256:	cf9a08d65a0b4..
Infos:	



Detection



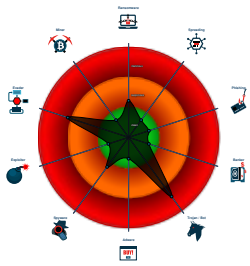
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Sample file is different than original …
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Contains functionality to dynamicall…
- Found dropped PE file which has no…

Classification



- **System is w10x64**
- o6OaOfrAQs.exe (PID: 5080 cmdline: C:\Users\user\Desktop\o6OaOfrAQs.exe MD5: 049ECAD4587538C292E3EBEEE5947EB5)
- **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
00000000.00000002.833642960.000000000341C000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: o6OaOfrAQs.exe PID: 5080	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

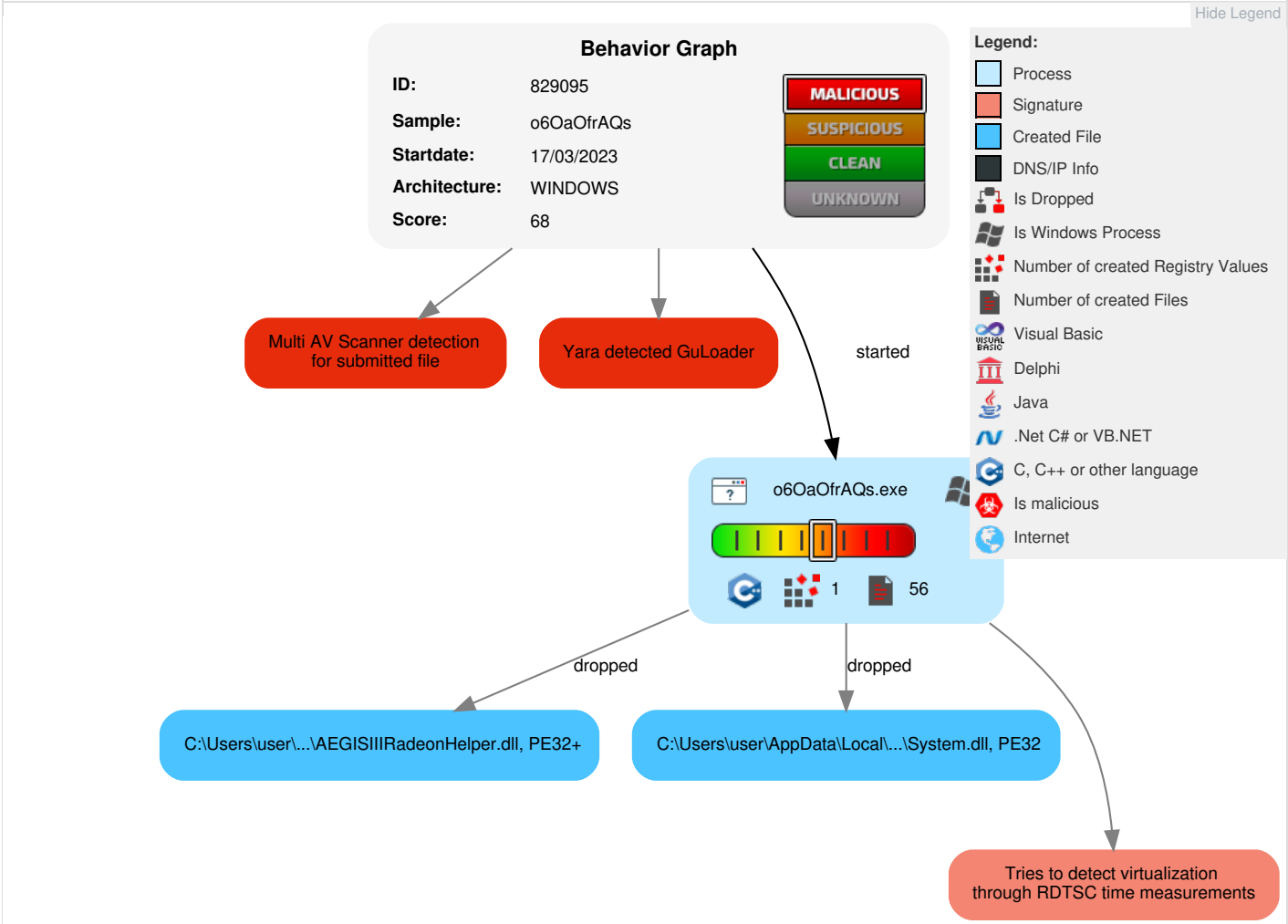
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	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	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

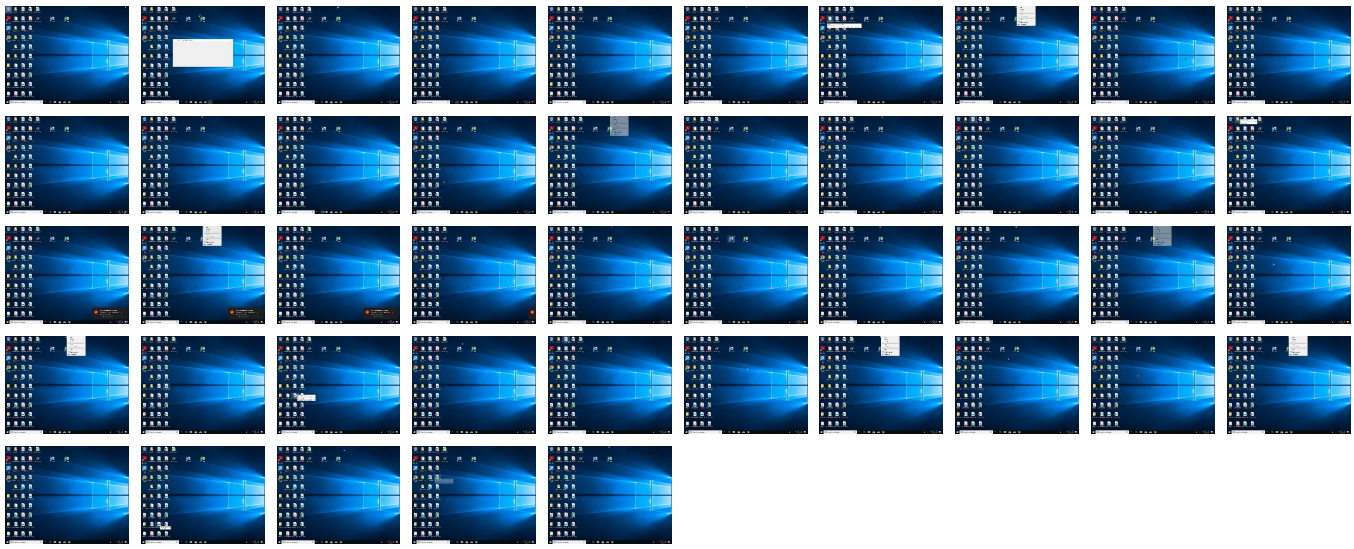
Behavior Graph



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
o6OaOfrAQs.exe	51%	ReversingLabs	Win32.Trojan.Nemesis	
o6OaOfrAQs.exe	29%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsf929A.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsf929A.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\AEGISIIIRadeonHelper.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.o6OaOfrAQs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
0.0.o6OaOfrAQs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	o6OaOfrAQs.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	o6OaOfrAQs.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829095
Start date and time:	2023-03-17 20:21:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
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:	o6OaOfrAQs.exe (renamed file extension from none to exe, renamed because original name is a hash value)
Original Sample Name:	cf9a08d65a0b472b1ed84638a09d39d741f34e9cd2641092141a9bf1a5f796a6
Detection:	MAL
Classification:	mal68.troj.evad.winEXE@1/17@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.5% (good quality ratio 84.2%) • Quality average: 88.2% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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\Kontos.ini

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.838039816898156
Encrypted:	false
SSDEEP:	3:7KG/LmI/cXQQLQIfLBJXmgxv:OG/LmI/cXQQkIP2I
MD5:	FB5EE2C0CAC332EC8390F50016EF0769
SHA1:	11D9FB52FE5289140B9D52A38B56F99512B3A3A7
SHA-256:	C557AFE51AB22916E3423820A09D3805BF9DCDCECBEC4FE8DE2C67FB023BA631
SHA-512:	87CCEA7B203B8BFC4E21544FE4FE9693AF230E246C450E673410565791DFE8257E30354772FDCC114C7068D9295FDB491E9B52D1A3B490C0756E568B70B95C0A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	[Bedrock]..Interthing=user32::EnumWindows(i r1 ,i 0)..

C:\Users\user\AppData\Local\Temp\nsf929A.tmp\System.dll

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	11776
Entropy (8bit):	5.832316471889005
Encrypted:	false
SSDEEP:	192:4PtkiQJr7jHYT87RfwXQ6YSYtOuVDi7IsFW14Ll8CO:H78TQlgGCDp14LGC
MD5:	B0C77267F13B2F87C084FD86EF51CCFC
SHA1:	F7543F9E9B4F04386DFBF33C38CBED1BF205AFB3
SHA-256:	A0CAC4CF4852895619BC7743EBEB89F9E4927CCDB9E66B1BCD92A4136D0F9C77
SHA-512:	F2B57A2EEA00F52A3C7080F4B5F2BB85A7A9B9F16D12DA8F8FF673824556C62A0F742B72BE0FD82A2612A4B6DBD7E0FDC27065212DA703C2F7E28D199696F66E
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....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....oZ.....!..... .....(.....0.....`.....@.....2.....0..P.....P.....0..X..... .....text...O..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\AEGISIIIRadeonHelper.dll

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34016
Entropy (8bit):	6.1021284380541925
Encrypted:	false
SSDEEP:	384:JP7a6wQdSCVWSdoEdXjYmxzfkfIwuWR7UPMEdxsTStsBdMQJK2wKucYkcuhV3:N7a6eiHdFdr7W5UPMgy+OBG2X90uhV3
MD5:	4FC7FC174E80C178225C2509027DF961
SHA1:	9FF62413EC0DD462F5F016EBC804F1D736D24796
SHA-256:	866B31DD39B97DEDAFD0FBD5672639EE91B47AD319C47816B4F6D01BFF93FF8C
SHA-512:	29261B9ABC4AF2F51C05B61A37721BC737B411530361A4B48A7BFFAB0F8263EA75BFD51B6E6E94E91E1D02DC442B534C3334B05FD8324E7CF307FA08179A1ED9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.oPZ.oPZ.oPS..PR.oP..nQX.oP..jQK.oP..kQR.oP..lQ X.oP).nQY.oPZ.nPt.oP..fQY.oP..oQ[.oP..P[.oPZ..P[.oP..mQ[.oPRichZ.oP.....PE..d....5;a....." .....0...:.....F....`..... ..\.....].....H.....f.....H....O..p.....@P.....@..p.....text.....0..... ..`.rdata...#...@...$...4.....@..@.data...@....p..... X.....@....pdata.....Z.....@..@.rsrc...H.....^.....@..@.reloc..H.....d.....@..B..... .....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Profetiske.Byg

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	data
Category:	dropped
Size (bytes):	297815
Entropy (8bit):	6.803960139750454
Encrypted:	false
SSDEEP:	6144:J35PGszPFp+EB9h18KeMJwYQl/w+ByCHqLBmv:J3FGsz93N8Kp60Bg
MD5:	12DF13549A2F50FB06EAAC92D2F36C05
SHA1:	5E1CD0421664E97B44B2C26960F4D298DAED0C99
SHA-256:	4EE38AAF3380FB3D7C4F57800A1692175C1D772E3A11028874CF2D8F5DC599F2
SHA-512:	6DD5811B457913D37B922904678A508A1762CDA447C195A660457B19D6302DB8E21586AFF0F22D41D73514CA926FEFE8554777EB558BD321ABF5B76C06527848
Malicious:	false
Preview:	.....T.....h.....@...KK.....[.....W.....b.....F.....,.....DD.....WW.....[.....P.'.....hhh.....^^....JJ....x.....F.....aaa..... .....!.....IIII.....WW.i.....\\.....q.22.....m...555.....m..7.k.....m.....c.QQ.....,.....cc.....?..xxx.....4.....^.....]].444.XX.....ggg.....]....jjjjj..77.....bbb...<<.....++.....XX.....!!..qqq.....@.....eeee.....[.....00.A.....H.yyyyy.. ...FFFFF..kk.555.....lll...H.....ssss...MM..j.....G...^^.....~.....PP..... .....III.....}}}.....""".....))...UU...l.))))).....++...%%.....######....hhh.. .....::..^.5.....(((.....n..".....zzzzzz.....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Sankekort.Sch209

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe

File Type:	data
Category:	dropped
Size (bytes):	42836
Entropy (8bit):	4.578518141395867
Encrypted:	false
SSDEEP:	768:AGQ+v3ebyf4b4Yv6Dub2I+MxA83BMUBaPqbIvcbYIrf:NQ+WApD42MxBMMaPqbZbYIrf
MD5:	3DAD0F9AF0356D18A46167665A352768
SHA1:	E5D083D2224DE4FC9105CB966CF3A53F9BB7D3C0
SHA-256:	8A124F4091887491B8FABE0C0C694B95C2D76F68FB4E9292C59FA5971074899C
SHA-512:	7CD0CF5AF5B79A146F22A2D68CC3500AF6068F1BFA48B5730E2C2236201E4B6B7CCED4DBB9121A525F41FC63C07403D1CB40F9267FBF81C5FFC2CB4FA6221E98
Malicious:	false
Preview:	.....WWW.....T..00.....A.....>>>.lll.....NNNN.....&.....s.$$$.....++.;;;;.....TT.....l.o.....ll.....vv.....+.....V....'.>.....a.....y.l...{{{.11.<...333.....6666....ee....._.....5.....88.....%%..<.....R.....]]]].....888.....a.n..C.....>.....P.....;;.....HHH.....bb.....eee.....QQ..cc..`.....b.w.....--.....GGG...JJJ.U.....uu.VV....v..ii. .....FF.....K.....1.....44444.....QQQ....,//.....w.....ll.....SS....(.....H.....B.....OOOO.....__....l.....}..//.vvvv....ii.....~~~..EEE..MM.....L.@@.....G.....:.....888.....))).....?.....FF.....DDDD.....@@@@@.....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Hjtideligholdelser\Liechtensteiner\Systemopstninger\pan-start-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	140
Entropy (8bit):	5.529383944212929
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllDM9vFW0p/sXm1MMos9DwlTYTbklt/sbp:6v/lhPysx8vFW0pkX4iZlTYTI3Ebp
MD5:	4308BBBAB1DB146494AE5ABB07B8E6DB
SHA1:	58121574EEB070E26DDD75A964F3548E176E58A4
SHA-256:	EFB732049C674EB25BFCB2FA0CBCC45D24190BF1479C054647F424B31E34C828
SHA-512:	41C9B37516F8D6AB7155F890EE36C26FE4161383A93BFBF696AB18292774C3556642E898361D21CECCBFEFFAF5814495CFAC2C74791E02F068B055BD3AD87DE
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....CIDAT8.c`.J..R..(...\.`..2.Y3...k.i.....b..PN.....J.@6.I.`.Pd..A.....O...D....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Hjtideligholdelser\Liechtensteiner\Systemopstninger\printer-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.834297280344084
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllPhF1MzoQxJrN7djpdXLImeR/mV2kg1p:6v/lhPysx1MzoQxlRZbCRaip
MD5:	38D787F55E22FB591135F9250CD259D4
SHA1:	0E135B0E1CA49A6E43DB4CB7596FAEA022E23924
SHA-256:	1ED839B015A67CAB9948469975411D982A96314CE82851EA2F9F6BB8D733A002
SHA-512:	4E21AB54B7110B4CD2EBC0E2CF6DF3F8C7C988495BCCA76949BC3C5EB669A793FCCDA5CB4DDB7B627A21734BD181FE44670757144CC2A007FCB695405F08EC2B
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....JIDAT8.c`..0b..O..&J]@5....tR.>.....`.8.(6....-Z....a..&..3 ....4...<.....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Idolatrous\Kaes\pt-br.txt

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	9515
Entropy (8bit):	5.04214621707661
Encrypted:	false
SSDEEP:	192:icoGT04mzNN8hYivh5gtE/PkjY09fdNQuQ:ibGg4mzNhi4tEHoDfHQuQ
MD5:	7B02E1AE16E2E709D7C97DE560B4DBE9

SHA1:	191A54644417F7D36F5CB4182DCDB3737D74BE51
SHA-256:	DA0B58F52BBC131F967942D1D8E9DE1B5721AE864BC21852A0AD4062332297CB
SHA-512:	4F689F854DB3F766B5E53CE2F19E9F8293C075EE3F9B18098EB05B352F2EC95DF85E49A78540781EB531BCE60C7B1F7890F1FE3C65200DEC3CB908E90FB827A1
Malicious:	false
Preview:	.;!@Lang2@!UTF-8!..; : Francisco Jr..; 4.37 : Fabricio Biazzotto ..; 18.05 : Atualizado por Felipe..;..;..;..;..;..;..;..0..7-Zip..Portuguese Brazilian..Portugu.s Brasileiro..401..OK..Cancelar.....&Sim..&N.o..&Fechar..Ajuda....&Continuar..440..Sim pra &Todos..N.o pra T&odos..Parar..Reiniciar..&Em 2. plano..&Em 1. plano..&Pausar..Pausado..Voc. tem certeza que voc. quer cancelar?..500..&Arquivo..&Editar..&Visualizar..F&avoritos..&Ferramentas..&Ajuda..540..&Abrir..Abrir &por Dentro..Abrir p&or Fora..&Visualizar..&Editar..Re&nomear..&Copiar Para.....&Mover Para.....&Apagar..&Dividir arquivo.....Com&binar arquivos.....P&ropriedades..Comen&t.rio..Calcular checksum..Diff..Criar Pasta..Criar Arquivo..S&air..Link..&Correntes Alternantes..600..Selecionar &Tudo..Desmarcar Tudo..&Inverter Sele..o..Selecionar.....Desmarcar...Selecionar por Tipo..Desfazer sele..o por Tipo..700...co&nes Grandes...c&ones Pequenos..&Lista..&Detalhes..730..Desorganizado..Visualiza..o

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Ravingly\Magnetoplasmadynamics\godsvognen\avatar-default-symbolic.svg

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	266
Entropy (8bit):	4.986245244009802
Encrypted:	false
SSDEEP:	6:tI9mc4slzc8SRIKMNo/aMhFl1OkUjq5eKVrGDVfqKlNK+:t4C8LKMuyMhPobjoprGDRlj
MD5:	8B727826F9D8C0C7C954EDE912CB0DEB
SHA1:	1518AA80747326B5353C22D32E57A33D61285119
SHA-256:	0783A7F518D3879C8F0F50B45FBD779A98652469E9B7C659CE41F14D1629D334
SHA-512:	0ABB243F9D1E0B6EDA0CB25D35C3449AB2B5B83078208F11B876A27FF11FF70B79F8BA97D4DA3AED21A8314C75FB2174D9378AF59B57DCB99DFF681D9AAB8561
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <path d="M8 1a3 3 0 100 6 3 3 0 000-6zM6.5 8A4.49 4.49 0 002 12.5V14c0 1 1 1 1 1h10s1 0 1-1v-1.5A4.49 4.49 0 009.5 8z" style="marker:none" color="#bebebe" overflow="visible" fill="#2e3436"/>.</svg>.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\be.txt

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12193
Entropy (8bit):	4.4720152705808935
Encrypted:	false
SSDEEP:	192:i2PDEeaNB1PmcptkcDHxbTvPnc67bMxQxGx4ch/JuLQRcg/oN96bPNljYiYr197:ikDFKBFmcPLx3HPnIsqrJuqcgAN96b87
MD5:	3C21135144AC7452E7DB66F0214F9D68
SHA1:	B1EC0589D769EAB5E4E8F0F8C21B157EF5EBB47D
SHA-256:	D095879B8BBC67A1C9875C5E9896942BACF730BD76155C06105544408068C59E
SHA-512:	0446A0E2570A1F360FD8700FD4C869C7E2DBB9476BBDEC2526A53844074C79691542B91455343C50941B8A6D5E02A58EE6AA539CC4C4AE9CF000B4034EF663E
Malicious:	false
Preview:	.;!@Lang2@!UTF-8!..; : Kirill Gulyakevitch..; 9.07 : 2011-03-15 : Drive DRKA..;..;..;..;..;..;..;..0..7-Zip..Belarusian.....401..OK.....&.....&....&.....&.....440..... ... &..... ... .&.....&.....&.. ....&..... ....?..500..&.....&.....&.....&.....&.....&.....540..&..... ..... &..... .&.....&.....&.....&..... .....&..... .....&.....&..... .....&.'..... .....&.....&..... .....Diff..&..... .

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\changes-allow-symbolic.svg

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	998
Entropy (8bit):	5.186938379246791
Encrypted:	false
SSDEEP:	24:t4CBGD0QNRWLLxo2em0yKbRAecFxV0/wXK:gDrc0NtAecFiH
MD5:	CB1EEE7BDB582B756D0F68EF02D6D96D
SHA1:	9E9B0F25BC472EF1C1C13EEAC12FD11C4CC0D2D9
SHA-256:	20EA767E852A8EBF2C5BA16D56CBAE10BD09D6CBA89B372A57EAA973AD3281B4
SHA-512:	E22FAEAE78D244A0F4E7215B31125D5AA4FD66C0720B0DE61D12084EAB879D7A9E231CCD5CD431417115B0945B450DC348DA400D67DB1898513B7BD6B9C274DB
Malicious:	false

Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#bebebe" fill="#474747"><path d="M3 9h10c.554 0 1 .446 1 1v3c0 .554-.446 1-1 1H3c-.554 0-1-.446-1-1v-3c0-.554.446-1 1-1z" style="marker:none" overflow="visible"/><path d="M7 0s-.709-.014-1.447.356C4.814.725 4 1.666 4 3v3h2V3c0-.667.186-.725.447-.855C6.71 2.014 7 2 7 2h2s.291.014.553.145c.261.13.447.188.447.855v8h2V3c0-1.333-.814-2.275-1.553-2.644C9.71-.014 9 0 9 0z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M2 12h12v4H2z" style="marker:none" overflow="visible"/></g></svg>

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\dotnet.api

Process:	C:\Users\user\Desktop\o6OaOfrAQs.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
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">.. ..body{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;margin: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\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\ebook-reader.png

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	555
Entropy (8bit):	7.499536740374189
Encrypted:	false
SSDEEP:	12:6v/7anZhFxDEKwjAq0kaO/yvSL6T1pjNngLpzPanwmB9HE4JqSjF:5bDEPxdqKLmpqLdynw29kEqSZ
MD5:	BFF011148B773FA44B9A9BB029E8CC52
SHA1:	F2B838927E320D12649CEFDEA3AFE383C6650D7C
SHA-256:	B21DE7B432A7A67544D007ECC0FDD95F8E8C6129AF558A32102EE04C08635653
SHA-512:	A57C83AEE0E1F4C530D2F5B90589C31FD6E2FF8F62F998963284218FAC5EE164BCA7A619A9597DC3E2ECD0095A2CF04467E89EDF86700E1A90B3DF60B5121C9B
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.....A....v...b.m.A..Q..Q..UD5.F.m.....fs{9.}...V.`....%.kt....R...+%7.}p..@.}:..u466`.6uu.tvv...N6....D"Q.....po".;.4....W..g.b..\.~?...<.../....$..5.....r.+..ah...F;.H.`b ....4.[...k.6.<..Kk.m[h..x`...R...z{.H.....Oax.e..{.....w._...c._>..6..T*HY.1! e.#....G.....{.AB..l.K"..P(..j..$.R.}L.5.....@.>.....X...hE....L.."L.....=~..7n.2.,RJ.01.....B.AWW..<q.....Ng.,../.Z...+...N].r.5.EB.p$..!,....,.....SW.TD+U...K...ee._.N*.[..`..1q..v\#6..?;7..4..3....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\emblem-photos-symbolic.svg

Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	680
Entropy (8bit):	5.109191824773878
Encrypted:	false
SSDEEP:	12:t4CP5GEA9xl7jhz4AeW02KdTwWjhz4AeW02KdTPqkoop4p:t4CBGEAgF4AeW0/N4AeW0/Zqg4p
MD5:	379690952AAA576521D51249D404CBCD
SHA1:	61A8A95B0454422AA47379CF983B99FFDD839439
SHA-256:	EAD402FB0B85DB153356EC695016FD4F2C4031367D8ED6D1C1EF5FF4F28A8DE8
SHA-512:	35B6BC866C3D02A2486D3447C82405103DE89D46940F7FE44A7009E714BBA57FBE601EEC939C3206ADB06FB31C4FD1D3822A0ED52A346ACFDE5908643432F92
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" fill="#474747"><path d="M13 5v2h1v5H4v2h12V5z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" font-weight="400" font-family="Sans" overflow="visible"/><path d="M0 2v9h12V2zm2 2h8v5H2z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" font-weight="400" font-family="Sans" overflow="visible"/><path d="M3 7c2.32 1 3.045-1.66 6 0v1H3z" style="marker:none" overflow="visible" opacity=".35"/></g></svg>

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\font-select-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	220
Entropy (8bit):	6.546211943247282
Encrypted:	false
SSDEEP:	6:6v/lhPysde0C1jngP3V95D2tOA/RDvhpLUxbVp:6v/7jC1zi3Sr/hW
MD5:	C84EE7522C124892455BB09DEBCF9340
SHA1:	AF87A2A5688346A3902762DD250328B7EF224620
SHA-256:	E0A3BD6FE1A1BAEFFE04BCA2980ADF755F888E31DCE3686B16C5DAC4202A38C8
SHA-512:	3BEED79366F15CD075781F677C0C9E84081D2189D1FB541A34AA25980B48701A3D93DC550E4ABEB550EFBE3167B1CAB8338E22F4603C6A71936876FBA75FAD5 8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...=..P.../z.Q..Kx....l.b.)...x.....t.....Y~.).....7.....W.xk.'A...u.....%..!k.k5.|E=+X..,,a.S.H4p*D8.8(FH.a..5.x...%.....7..8s:.. .....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes\Gyrite\network-wired-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	144
Entropy (8bit):	5.708279548998072
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllAoSF1/LvgStjP9f9uvJYUo+/JHt//sup:6v/lhPysKo21/Lvlt7V9+YUouJH1/jp
MD5:	1ED278AD206D6EA33FF787DD326E0FC5
SHA1:	8CFF7AD12FC0E5545E71D05879A0245BEDAF4D46
SHA-256:	CC88E76F7C7D2E5B07E49D1F2AD88F8BAFC0542EB11CEB2B2FFF235C87AB4417
SHA-512:	7291085B6153C02EDBF679CDDB93B97DBB74943F216EB622CE9722E02613269F626F8A7A5BE8DA683153E9AEE22C40ED7264E8A0ED62A99F477E2B96642596B F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....GIDAT8.c`..0...O.Z&J]0.. ...&u]..5?.....b....Q.E./.....t@..,....)1..,b...#.=....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Unrivalled\Nonexhaustively\Snaffle\Stealthful\LogoCanary.png	
Process:	C:\Users\user\Desktop\o6OaOfrAQs.exe
File Type:	PNG image data, 600 x 600, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	16669
Entropy (8bit):	7.836876926418697
Encrypted:	false
SSDEEP:	384:dg1Ew+1FT+/6trrKWzge5jh2xmalhctpNy:W1E1c6tru1CUYa4tDy
MD5:	F80867A421C85C6E2865CF85FF7C4B02
SHA1:	C3EAB6B7E92646FE3407B2B3C5AFFE13A7873C48
SHA-256:	BCAA3B1333919176137D4DE4B1E3F31126159B12F959D7277BD8537B95139BD3
SHA-512:	06B51E660AEE86FC3BB068C6DEA046920E04F86B8EDD02E640EAC619F0F0D7E87E5CAE5BE1390CEBC5DFE70AA13BAB1710176E88C9D1C859182629D429745D 78
Malicious:	false
Preview:	.PNG.....IHDR...X...X.....f.....tEXtSoftware.Adobe ImageReadyq.e<..@.IDATx.....\.}..../...].{`.....D.\..u.....#..V.eW.G>"W....V..d..IVU".:.D<$J.....{q/.....`0g./..z....A.`. .?..p....M....._'...L...]~.....;.....,..... ....X.....@`.. .....@`...,..... ....X.....@`.. .....@`...,.....X.....@`.. .....@`...,.....X..... .....@`..., ...X..... .....@`...,.....X..... .....@`...,.....X..... .....@`...,.....X..... .....@`...,.....X...,..... .....@`...,.....X...,..... ....~.....N...@...C{..o.?2.....x...?_....sC..O8...n..J.ttbv9. ..w~...ym..O.....vq"f..qrjt9... ..].S..Hz.gf}.,.Sm!...>..Xh..:S.};d.....2..?.....2...1..ep...K.{.?..@`.7=...7U..C.....S...6....|a.}]..._..d...._.....+__..JS.....X.u...;..Q.x.z9...eP5f.H..nnz. &h...4.kz.....&....o)..=..x.=...y ....6i...wL.....Y(.2NRP..J...HL/K#^izqpbUp}...q...g....."....4R..#.VFrR|.LF>w~.Pm..\..4.5t{.-..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

Entropy (8bit):	7.56953186638099
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:	o6OaOfrAQs.exe
File size:	335976
MD5:	049ecad4587538c292e3ebeee5947eb5
SHA1:	12aabeb19083dd114b7b94c836b031de3945d2c9
SHA256:	cf9a08d65a0b472b1ed84638a09d39d741f34e9cd2641092141a9bf1a5f796a6
SHA512:	12092128f6b2f6ea6ab86a7b1812e550e598dfecd43a240bd1ffc0bd15ff9c24e3c9bb40a4273ad706b9a7a7ad890b1c708c42cc23ec359626f5024b36db03ce
SSDEEP:	6144:DDk9dhfzelxlIPuHBXZOEz5hN4EAnKQo4N7kqZ7t+roIbvS:U9u3lWHBXZTENnKza7kqZ5+rh6
TLSH:	7D6401913AE0D467FC5A4630CAA5E5F3D2A1FE04C916C18373647F6F7D322419922EBA
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...+.oZ.....`.....

File Icon

Icon Hash:	08c2b0d8cc64b046

Static PE Info

General

Entrypoint:	0x4031d6
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:	0x5A6FED2B [Tue Jan 30 03:57:31 2018 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=Brooking183@Flydes25.Dyr, OU="Magtbalancerne Regnvejrsdagene Intensives ", O=Skizofren, L=Onalaska, S=Wisconsin, 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	• 2/5/2023 9:25:21 AM 2/4/2026 9:25:21 AM
Subject Chain	• E=Brooking183@Flydes25.Dyr, OU="Magtbalancerne Regnvejrsdagene Intensives ", O=Skizofren, L=Onalaska, S=Wisconsin, C=US
Version:	3
Thumbprint MD5:	DE53E25C4A808A06A0CD944E65FB058D
Thumbprint SHA-1:	B1DD19494EAA53E29C92E68EB19E33CFABB34DE0
Thumbprint SHA-256:	12FF0462FE369CB81BB77B13ADFE3B705E7F71A5CFA614B370A8D6D63719C06F
Serial:	6CA44E753450CEC7C37D62FEA0B835456441D271

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi

Instruction
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A0h]
call dword ptr [0040709Ch]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042370Ch], eax
je 00007F25A0E28E43h
push ebx
call 00007F25A0E2BF1Ah
cmp eax, ebx
je 00007F25A0E28E39h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007F25A0E2BE96h
push esi
call dword ptr [00407098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F25A0E28E1Dh
push 0000000Ah
call 00007F25A0E2BEEEh
push 00000008h
call 00007F25A0E2BEE7h
push 00000006h
mov dword ptr [00423704h], eax
call 00007F25A0E2BEDBh
cmp eax, ebx
je 00007F25A0E28E41h
push 0000001Eh
call eax
test eax, eax
je 00007F25A0E28E39h
or byte ptr [0042370Fh], 00000040h
push ebp
call dword ptr [00407044h]
push ebx
call dword ptr [00407288h]
mov dword ptr [004237D8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407178h]
push 00409188h

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	0x7428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x36000	0xa3c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x51650	0xa18	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5f0d	0x6000	False	0.6649169921875	data	6.450520423955375	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1248	0x1400	False	0.4275390625	data	5.007650149182371	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1a818	0x400	False	0.6376953125	data	5.129587811765307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x24000	0x12000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x36000	0xa3c0	0xa400	False	0.0760766006097561	data	1.8822021165260459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x36268	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x365d0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 0	English	United States
RT_DIALOG	0x3fa78	0x144	data	English	United States
RT_DIALOG	0x3fbc0	0x13c	data	English	United States
RT_DIALOG	0x3fd00	0x120	data	English	United States
RT_DIALOG	0x3fe20	0x11c	data	English	United States
RT_DIALOG	0x3ff40	0xc4	data	English	United States
RT_DIALOG	0x40008	0x60	data	English	United States
RT_GROUP_ICON	0x40068	0x14	data	English	United States
RT_MANIFEST	0x40080	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

DLL	Import
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: o6OaOfrAQs.exe PID: **5080**, Parent PID: **3528**

General

Target ID:	0
Start time:	20:22:24
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\o6OaOfrAQs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\o6OaOfrAQs.exe
Imagebase:	0x400000
File size:	335976 bytes
MD5 hash:	049ECAD4587538C292E3EBEEE5947EB5
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: 00000000.00000002.833642960.000000000341C000.00000040.00001000.00020000.00000000.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	4055E0	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsi8D88.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B66	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	7	4055E0	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	7	4055E0	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	7	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Dykereeve	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Profetiske.Byg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\AEGISIIIRadeonHelper.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Sankekort.Sch209	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Unrivalled	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Unrivalled\Nonexhaustively	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Unrivalled\Nonexhaustively\Snaffle	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Unrivalled\Nonexhaustively\Snaffle\Stealthful	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Unrivalled\Nonexhaustivel y\Snaffle\Stealthful\LogoCanary.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Ravingly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Ravingly\Magnetoplasmadynamics	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Ravingly\Magnetoplasmadynamics\godsvognen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Ravingly\Magnetoplasmadyn amics\godsvognen\avatar-default-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Tilrettelggelsernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\be.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\changes-allow-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\dotnet.api	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\ebook-reader.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\emblem-photos-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\font-select-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\network-wired-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Hjtideligholdelser	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Hjtideligholdelser\Liechtensteiner	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Hjtideligholdelser\Liechtensteiner\Systemopstninger	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Hjtideligholdelser\Liecht ensteiner\Systemopstninger\pan-start-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Hjtideligholdelser\Liecht ensteiner\Systemopstninger\printer-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Idolatrous	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Idolatrous\Kaes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055E0	CreateDirectoryA
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Idolatrous\Kaes\pt-br.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf929A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B66	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	4055E0	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	4055E0	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	4055E0	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	4055E0	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	4055E0	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsf929A.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	4055A0	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsf929A.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B2F	CreateFileA
C:\Users\user\AppData\Local\Temp\nsf929A.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405B2F	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsi8D88.tmp	success or wait	1	40344D	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsf929A.tmp	success or wait	1	405761	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\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Te lescopiform\Bestridende\Profet iske.Byg	0	32768	00 00 00 00 00 fd 00 fd 00 54 00 00 00 00 00 fd 00 00 00 68 00 fd fd fd fd 00 00 fd fd fd 00 00 fd 00 00 fd 00 00 fd fd 00 00 00 40 00 00 00 4b 4b 00 00 fd 00 00 fd 00 00 00 5b 00 00 0d 0d 0d 00 57 00 00 00 00 00 00 62 00 00 fd fd fd fd fd 00 00 fd 00 fd fd fd fd 00 00 46 00 00 fd fd fd fd 00 00 00 fd 00 fd 00 fd fd 00 2c 00 00 00 00 1b 1b 1b 00 44 44 00 00 00 fd fd 00 00 57 57 00 00 fd 00 fd 00 12 12 00 fd fd fd 00 fd fd 00 00 00 00 5b 00 00 00 00 00 00 fd fd fd 00 50 00 27 00 00 00 fd 00 fd fd 00 00 68 68 68 00 fd 00 0b 00 fd 00 5e 5e 00 fd 00 00 4a 4a 00 00 00 00 78 00 00 fd 00 00 00 00 46 00 fd fd fd fd 00 61 61 61 00 00 1e 00 fd fd 00 00 fd 00 00 fd 00 00 00 fd fd fd fd 00 00 00 00 00 fd 00 00 00 21 00 00 00 00 00 0f 00 00 06 00 fd 00 49 49	Th@KK[WbF,DDWW[P'h hh^^JJxFaaa!II	success or wait	13	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Te lescopiform\Bestridende\AEGISI IIRadeonHelper.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 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 1e fd 01 03 5a fd 6f 50 5a fd 6f 50 5a fd 6f 50 53 fd fd 50 52 fd 6f 50 08 fd 6e 51 58 fd 6f 50 08 fd 6a 51 4b fd 6f 50 08 fd 6b 51 52 fd 6f 50 08 fd 6c 51 58 fd 6f 50 29 fd 6e 51 59 fd 6f 50 5a fd 6e 50 74 fd 6f 50 fd fd 66 51 59 fd 6f 50 fd fd 6f 51 5b fd 6f 50 fd d0 50 5b fd 6f 50 5a fd fd 50 5b fd 6f 50 fd fd 6d 51 5b fd 6f 50 52 69 63 68 5a fd 6f 50 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$ZoPZoPZoPSPR oP nQXoPjQKoPkQRoPlQX oP)nQYoPZnPt oPfQYoPoQ[oPP[oPZP[o PmQ[oPRichZoP	success or wait	2	405BC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Sankekort.Sch209	0	32768	00 fd fd fd 00 57 57 57 00 fd 00 00 fd 00 00 54 00 00 30 30 00 fd 00 00 00 00 00 00 00 fd fd 00 41 00 00 00 00 00 00 fd 00 fd 00 00 00 3e 3e 3e 00 6c 6c 6c 00 08 08 00 fd 00 00 4e 4e 4e 4e 00 fd fd fd fd 00 12 00 26 00 00 00 fd 00 00 00 1e 1e 1e 00 73 00 24 24 24 00 00 00 00 09 09 09 00 00 00 02 02 00 00 00 00 fd fd fd 00 00 00 00 00 fd fd fd 00 fd fd 00 15 15 15 00 00 2b 2b 00 3b 3b 3b 3b 00 00 fd fd fd 00 fd 00 00 00 00 fd 00 00 00 00 00 12 00 54 54 00 08 08 08 00 00 00 00 6c 00 6f 00 00 00 00 00 fd 00 00 00 00 6c 6c 00 00 00 fd 00 00 00 76 76 00 00 fd 00 fd 00 00 fd 00 00 00 00 00 00 2b 00 fd fd 00 fd 00 fd fd fd 00 00 fd 00 00 56 00 00 00 fd 00 27 00 3e 00 1f 1f 1f 00 61 00 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 fd fd fd 00 00 79 00 21 00 00 00 7b	WWWT00A>>>lllNNNN&s$$$++;;;;TTlollvv+V'>ay!{	success or wait	3	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Unrivalled\Nonexhaustivel y\Snaffle\Stealthful\LogoCanary.png	0	16669	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 58 00 00 02 58 08 06 00 00 00 fd 66 fd fd 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 fd 65 3c 00 00 40 fd 49 44 41 54 78 fd fd fd 09 fd 5c fd 7d fd fd fd fd 2f fd fd fd 5d 1c 7b 60 0f fd fd 83 14 fd fd 44 fd 5c 1f fd 75 fd 11 fd 0e fd fd 23 d5 fd 56 b1 65 57 1c 47 3e 22 57 fd fd fd fd 56 12 fd 64 fd 12 49 56 55 22 fd 3a fd 44 3c 24 4a b4 fd fd 14 fd 7b 71 2f 00 fd fd fd 18 60 30 67 1f 2f fd fd 7a fd fd fd fd 41 fd 60 00 20 3f 1f fd 70 fd fd fd fd 4d fd fd 17 fd fd fd fd 5f fd 27 fd 1f fd 4c 00 00 fd 5d 7e fd fd fd fd fd 3b 0e 00 00 e7 fd 10 00 00 08 2c 00 00 fd 05 00 20 fd 00 00 10 58 00 00 02 0b 00 40 60 01	PNGIHDRXXftEXtSoftwareAdobe ImageReadyqe<@IDATx\}/]{`D\u#VeW G>"WVdIVU":D<$J{q/`0g/zA`?pM_'L]~;, X@`	success or wait	1	405BC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Ravingly\Magnetoplasmadyn amics\godsvognen\avatar-default-symbolic.svg	0	266	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 0a 20 20 20 20 3c 70 61 74 68 20 64 3d 22 4d 38 20 31 61 33 20 33 20 30 20 31 30 30 20 36 20 33 20 33 20 30 20 30 30 30 2d 36 7a 4d 36 2e 35 20 38 41 34 2e 34 39 20 34 2e 34 39 20 30 20 30 30 32 20 31 32 2e 35 56 31 34 63 30 20 31 20 31 20 31 20 31 20 31 68 31 30 73 31 20 30 20 31 2d 31 76 2d 31 2e 35 41 34 2e 34 39 20 34 2e 34 39 20 30 20 30 20 30 30 39 2e 35 20 38 7a 22 20 73 74 79 6c 65 3d 22 6d 61 72 6b 65 72 3a 6e 6f 6e 65 22 20 63 6f 6c 6f 72 3d 22 23 62 65 62 65 62 65 22 20 6f 76 65 72 66 6c 6f 77 3d 22 76 69 73 69 62 6c 65 22 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"> <path d="M8 1a3 3 0 100 6 3 3 0 000-6zM6.5 8A4.49 4.49 0 002 12.5V14c0 1 1 1 1 1h10s1 0 1-1v-1.5A4.49 4.49 0 009.58z" style="marker:none" color="#bebebe" overflow="visible" fill="#2e3436	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\be.txt	0	12193	ff 3b 21 40 4c 61 6e 67 32 40 21 55 54 46 2d 38 21 0d 0a 3b 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3a 20 4b 69 72 69 6c 6c 20 47 75 6c 79 61 6b 65 76 69 74 63 68 0d 0a 3b 20 20 39 2e 30 37 20 3a 20 32 30 31 31 2d 30 33 2d 31 35 20 3a 20 44 72 69 76 65 20 44 52 4b 41 0d 0a 3b 0d 0a 3b 0d 0a 3b 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 42 65 6c 61 72 75 73 69 61 6e 0d 0a 11 35 3b 30 40 43 41 3a 30 4f 0d 0a 34 30 31 0d 0a 4f 4b 0d 0a 10 34 3c 35 3d 30 0d 0a 0d 0a 0d 0a 0d 0a 26 22 30 3a 0d 0a 26 1d 35 0d 0a 26 17 30 47 4b 3d 56 46 4c 0d 0a 14 30 3f 30 3c 3e 33 30 0d 0a 0d 0a	;!@Lang2@!UTF-8!; : Kirill Gulyakevitch; 9.07 : 2011-03-15 : Drive DRKA;;;;;;;;;07-ZipBelarusian401OK&&&	success or wait	1	405BC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrit e\changes-allow-symbolic.svg	0	998	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 63 6f 6c 6f 72 3d 22 23 62 65 62 65 62 65 22 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 33 20 39 68 31 30 63 2e 35 35 34 20 30 20 31 20 2e 34 34 36 20 31 20 31 76 33 63 30 20 2e 35 35 34 2d 2e 34 34 36 20 31 2d 31 20 31 48 33 63 2d 2e 35 35 34 20 30 2d 31 2d 2e 34 34 36 2d 31 2d 31 76 2d 33 63 30 2d 2e 35 35 34 2e 34 34 36 2d 31 20 31 2d 31 7a 22 20 73 74 79 6c 65 3d 22 6d 61 72 6b 65 72 3a 6e 6f 6e 65 22 20 6f 76 65 72 66 6c 6f 77 3d 22 76 69 73 69 62 6c 65 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 37 20 30 73 2d 2e 37 30 39 2d	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#bebebe" fill="#474747"><path d="M3 9h10c.554 0 1 .446 1 1v3c0 .554-.446 1-1 1H3c-.554 0-1-.446-1-1v-3c0-.554.446-1 1-1z" style="marker:none" overflow="visible"/><path d="M7 0s-.709-	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrit e\dotnet.api	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	405BC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\ebook-reader.png	0	555	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 01 fd 49 44 41 54 78 01 fd fd 03 fd 1d 41 00 fd fd 7f 76 fd f6 fd 62 8c 6d fd 41 11 fd 51 1b fd 51 15 08 55 44 35 fd 46 fd 6d fd fd fd fd fd 66 73 7b 39 fd 7d 0f fd 7f 56 02 60 52 fd fd fd 25 fd 6b 74 fd 10 02 fd 52 0a fd 08 2b 25 37 fd 7d 70 fd 07 40 0b 7d 3a 10 0a 75 34 36 36 60 fd 36 75 75 fd 74 76 76 fd fd fd 4e 36 fd fd df fd 44 22 51 fd fd fd fd fd fd 70 6f 22 1e 3b 0d 34 08 fd fd fd 57 51 11 67 fd 62 fd fd 5c fd 7e 3f fd fd fd 3c 7f fd fd 2f fd fd 1e 00 fd 24 fd fd 35 fd fd fd fd 03 fd fd fd fd fd fd 56 fd fd 09 04 02 18 09 fd 72 fd 2b 14 0a 61 68 fd fd fd 46 3b 03 48 fd 60 62 20 18 0c fd 05 34 fd 5b fd fd fd	PNGIHDRaIDATxAvbmAQQUD5Fmfs{9}V`%ktR+%7}p@}:u466`6uutvvN6D"Qpo";4Wgb\~?</$5r+ahF;H`b 4[	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\emblem-photos-symbolic.svg	0	680	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 63 6f 6c 6f 72 3d 22 23 30 30 30 22 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 33 20 35 76 32 68 31 76 35 48 34 76 32 68 31 32 56 35 7a 22 20 73 74 79 6c 65 3d 22 6c 69 6e 65 2d 68 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 2d 69 6e 6b 73 63 61 70 65 2d 66 6f 6e 74 2d 73 70 65 63 69 66 69 63 61 74 69 6f 6e 3a 53 61 6e 73 3b 74 65 78 74 2d 69 6e 64 65 6e 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 73 74 61 72 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 2d 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 74 72 61 6e 73 66 6f	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" fill="#474747"><path d="M13 5v2h1v5H4v2h12V5z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transfo	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrite\font-select-symbolic.symbolic.png	0	220	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 3d 0a fd 50 10 04 fd 2f 7a 04 51 02 fd 4b 78 05 fd fd 19 6c fd 62 fd 20 29 fd fd 03 78 00 fd fd 1b 08 fd 17 fd 74 fd fd fd fd fd fd 59 7e 1e 29 fd fd 14 fd fd fd 37 fd 05 fd fd 7f fd 57 fd 78 6b fd 27 41 1b fd 0e 75 10 16 fd 79 fd fd fd 7d fd 25 99 fd 21 6b fd 6b 35 fd 7c 45 3d 2b 58 fd fd 2c 2c 61 13 53 fd 48 34 70 2a 44 38 fd 38 28 46 48 11 61 fd fd 35 fd 78 16 04 fd 25 fd fd fd fd fd 37 0d fd 38 73 3a 03 fd 14 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8=P/zQKxlb)xtY~)7Wxk'Au%!kk5|E=+X,,aSH4p*D88(FHa5x%78s:IENDB`	success or wait	1	405BC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Tilrettelggelsernes\Gyrit e\network-wired-symbolic.symbo lic.png	0	144	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 47 49 44 41 54 38 fd 63 60 fd 10 30 fd 10 fd 4f fd 5a 26 4a 5d 30 0c 0c 20 04 fd 05 26 75 5d fd 1c 35 3f 18 18 18 fd fd 07 62 00 07 11 fd 51 fd 45 15 2f 10 fd 2a 1b fd 74 40 fd 01 2c 0c 0c 0c 1f 29 31 00 00 2c 62 08 09 fd 23 fd 3d 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dGIDAT 8c`0OZ&J]0 &u]5? bQE/t@,)1,b#=IENDB`	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Hjtideligholdelser\Liecht ensteiner\Systemopstninger\pan-start-symbolic.symbolic.png	0	140	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 43 49 44 41 54 38 fd 63 60 18 4a fd fd 52 fd fd 28 fd fd fd 5c 03 60 fd fd 32 00 59 33 fd 06 fd 6b fd 69 00 13 0e 03 fd fd 62 1b 2e 50 4e fd 0b 08 fd 06 4a 0d 40 36 fd 6c 03 60 fd 50 64 00 10 41 08 00 fd fd 1f 4f fd fd fd 44 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dCIDAT 8c`JR(\`2Y3 kib.PNJ@6l`PdAODIEND B`	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Hjtideligholdelser\Liecht ensteiner\Systemopstninger\printer-symbolic.symbolic.png	0	147	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 4a 49 44 41 54 38 fd 63 60 fd 10 30 62 11 fd 4f fd 1e 26 4a 5d 40 35 fd fd 01 fd 74 52 fd 3e 06 06 fd 7f 08 fd 1b 17 60 fd 38 0c 28 36 fd 05 fd fd 2d 5a fd 01 fd fd 61 2e 0f 26 fd 0f 33 20 fd 19 fd fd 34 fd 06 0c 3c 00 00 fd fd 1a fd 83 fd fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dJIDAT8 c`0bO&J]@5tR>`8(6- Za.&3 4<IENDB`	success or wait	1	405BC4	WriteFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Idolatrous\Kaes\pt-br.txt	0	9515	ff 3b 21 40 4c 61 6e 67 32 40 21 55 54 46 2d 38 21 0d 0a 3b 20 20 20 20 20 20 20 3a 20 46 72 61 6e 63 69 73 63 6f 20 4a 72 0d 0a 3b 20 20 34 2e 33 37 20 20 3a 20 46 61 62 72 69 63 69 6f 20 42 69 61 7a 7a 6f 74 74 6f 20 0d 0a 3b 20 20 31 38 2e 30 35 20 3a 20 41 74 75 61 6c 69 7a 61 64 6f 20 70 6f 72 20 46 65 6c 69 70 65 0d 0a 3b 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 50 6f 72 74 75 67 75 65 73 65 20 42 72 61 7a 69 6c 69 61 6e 0d 0a 50 6f 72 74 75 67 75 ea 73 20 42 72 61 73 69 6c 65 69 72 6f 0d 0a 34 30 31 0d 0a 4f 4b 0d 0a 43 61 6e 63 65 6c 61 72 0d 0a 0d 0a 0d 0a 0d 0a 26 53 69 6d 0d 0a 26 4e e3 6f 0d 0a 26 46 65 63 68 61 72 0d 0a 41 6a 75 64 61 0d 0a 0d 0a 26 43 6f 6e 74 69 6e 75	;!@Lang2@!UTF-8!; : Francisco Jr; 4.37 : Fabricio Biazzotto ; 18.05 : Atualizado por Felipe;;;;;;;;07-ZipPortu guese BrazilianPortugus Brasil eiro401OKCancelar&Sim &No&Fecha rAjuda&Continu	success or wait	1	405BC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf929A.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 69 72 2a fd 2d 13 44 fd 2d 13 44 fd 2d 13 44 fd fd 0f 4a fd 2a 13 44 fd 2d 13 45 fd 3e 13 44 fd fd 1c 19 fd 2a 13 44 fd 79 30 74 fd 29 13 44 fd 4e 31 6e fd 2c 13 44 fd fd 33 40 fd 2c 13 44 fd 52 69 63 68 2d 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e fd 6f 5a 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 fd 28 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$ir*-D-D-DJ*D-E>D*Dy0t)DN1n,D3@,DRich-DPELoZ.! (	success or wait	1	405BC4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\o6OaOfrAQs.exe	unknown	512	success or wait	135	405B95	ReadFile
C:\Users\user\Desktop\o6OaOfrAQs.exe	unknown	4	success or wait	42	405B95	ReadFile
C:\Users\user\Desktop\o6OaOfrAQs.exe	unknown	4	success or wait	2	405B95	ReadFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Sankek ort.Sch209	unknown	1	success or wait	277	405B95	ReadFile
C:\Users\user\Desktop\o6OaOfrAQs.exe	unknown	4	success or wait	2	405B95	ReadFile
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstruktu rdnr\Dykereeve\Jackbsningen\Telescopiform\Bestridende\Profetiske.Byg	unknown	12627968	success or wait	1	74372A81	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Shabbyish	success or wait	1	405E4D	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Shabbyish\Retablerings	success or wait	1	405E4D	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Shabbyish\Retablerings	Aphetism	binary	13 E1 C1	success or wait	1	402464	RegSetValueExA

Disassembly

No disassembly