ID: 828570
Sample Name: Royalistic.exe
Cookbook: default.jbs
Time: 10:37:08
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

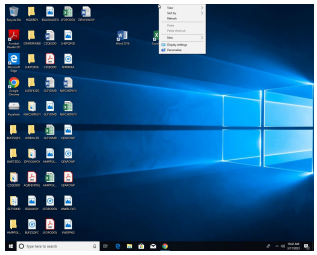
Windows Analysis Report

Royalistic.exe

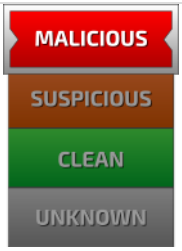
Overview

General Information

Sample Name:	Royalistic.exe
Analysis ID:	828570
MD5:	d14335f61c99a..
SHA1:	f82f3481619be...
SHA256:	08cabec4d012...
Infos:	



Detection



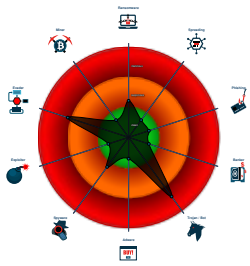
GuLoader

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
- PE file does not import any functions
- Drops PE files
- Contains functionality to shutdown /…
- Binary contains a suspicious time s…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Contains functionality to dynamicall…
- Found dropped PE file which has no…

Classification



Process Tree

- **System is w10x64**
- Royalistic.exe (PID: 5700 cmdline: C:\Users\user\Desktop\Royalistic.exe MD5: D14335F61C99A9B8A2D5E87CDF83CDD0)
- **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
00000000.00000002.834425818.0000000000677000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000000.00000002.834648652.0000000004EF6000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

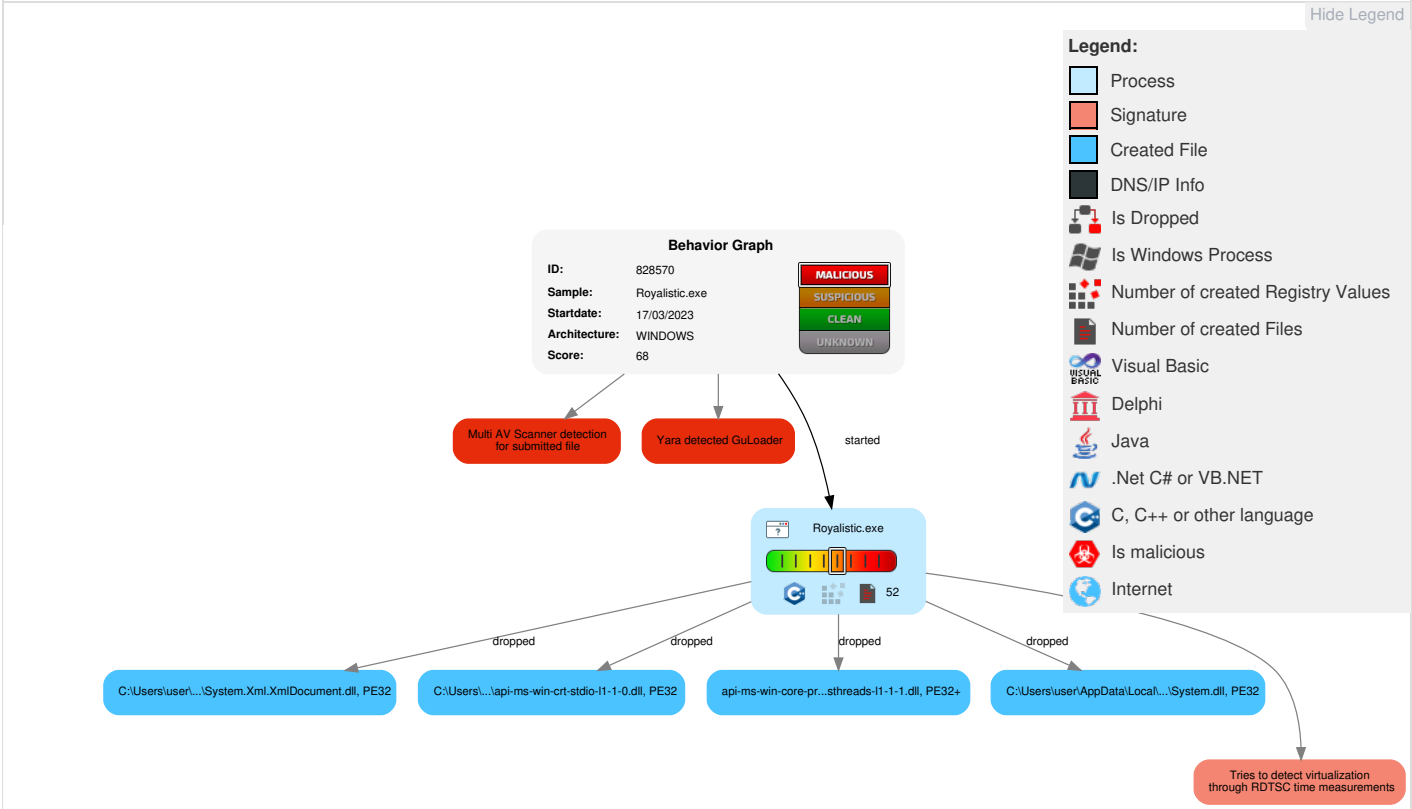
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

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

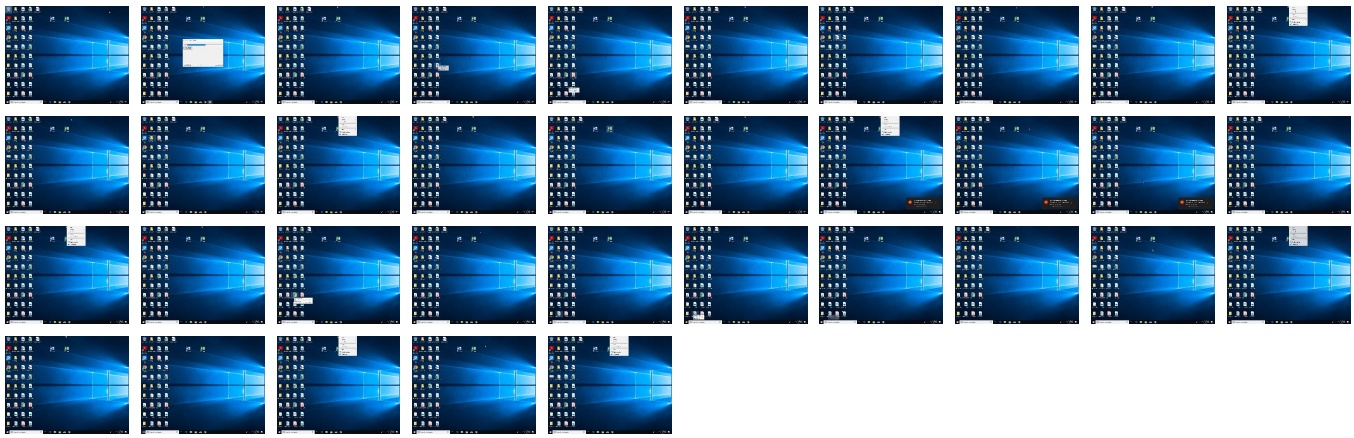
Behavior Graph



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
Royalistic.exe	26%	ReversingLabs	Win32.Trojan.Generic	
Royalistic.exe	51%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\System.Xml.XmlDocument.dll	0%	ReversingLabs		

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://jimmac.musichall.czif	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://jimmac.musichall.czif	x-office-spreadsheet.png.0.dr	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	Royalistic.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Royalistic.exe	false		high
http://https://github.com/dotnet/runtime	System.Xml.XmlDocument.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828570
Start date and time:	2023-03-17 10:37:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
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:	Royalistic.exe
Detection:	MAL
Classification:	mal68.troj.evad.winEXE@1/16@0/0

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.7% (good quality ratio 84.3%) • Quality average: 86.8% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp\System.dll

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.024446974480565
Encrypted:	false
SSDEEP:	192:Vm9rQDenC9VrcK7REgSWOprANupQYLRszDDH/d9CWlXo7U6Wxf:QJQEaVAK7R9SfpjpQYLRszfH/d9CWB1j
MD5:	E23600029D1B09BDB1D422FB4E46F5A6
SHA1:	5D64A2F6A257A98A689A3DB9A087A0FD5F180096

SHA-256:	7342B73593B3AA1B15E3731BFB1AFD1961802A5C66343BAC9A2C737EE94F4E38
SHA-512:	C971F513142633CE0E6EC6A04C754A286DA8016563DAB368C3FAC83AEF81FA3E9DF1003C4B63D00A46351A9D18EAA7AE7645CAEF172E5E1D6E29123AB864E7AC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../@t.k!..k!..k!..9T..l!.. Y..l!..k!..x!...T..o!...T..j!...T..j!...T..j!..Richk!....PE..L.....c....."!....."....@.....p.....@.....@.....A..P.....`.....@..X.....text...+!....."..... ..`.rdata.....@.....&.....@..@.data...D....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Afdelingskontorer.Ate

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	data
Category:	dropped
Size (bytes):	263441
Entropy (8bit):	7.470128360205037
Encrypted:	false
SSDEEP:	6144:gW2L2lxw6CfR2hGhddAkBtTCNwQn4Sp5U2JvkCmLO6ta4Rh40FdmxMDoOz:gMHw9SGh1D6ndCtLO6s4R2eOMTz
MD5:	ED053E4B81682B3CEF98A00C188F9191
SHA1:	7824184CA7B4588B9665CF5D6ECDF3E6A20820C7
SHA-256:	64A7608273D8284E67F338F8B77230B0EF14C342747CE6C3F8792F567BC99498
SHA-512:	51C4089DE4328B5C37B759CF98FCDE4838C67413CF0F0EE8EB1D9CD6BB129A41C686BEC3DD424B553725C84787671FAE3F9E037C436E8D7D5B8F28F7D42CBE7D
Malicious:	false
Reputation:	low
Preview:	.....?...s.....0.....'.....bbb.....>>.....II..}}.....;;;.....kk.....iiii.....XXXXX....qqq....iiii..++.....YY...00.....s.....7...EEE.....M.....&.....\\\\...../.....O.....6.....fff.....f.....AA.....^^^.....TT...*.....$.....=.....MM.....g.....O.....].xx.....aa.....gg.....CC.p.....BB.rr.....E....www.....xx....D.....'.....G.b....dd.....,,.....h.....6.*.....h.....RRR.0..."....3.....B.55....ee.BB.....?.....-.22.....A.....e.```....5....yy.DD.....b.....dddd..HH.....-.....lll.....2.....=.....#.....NN.....PPP.....ee.....c.....^^.T.....

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Affaldsproblem\x-office-spreadsheet.png

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	546
Entropy (8bit):	6.786347340342328
Encrypted:	false
SSDEEP:	12:6v/7X0ZKjCVdCyXM8OYSd/AuKoOjTOH6BMLHEMA:C0oCDMUaAutUTQ60HED
MD5:	D4AEA6CA7A8B03C62C36FF2AEBE20C6C
SHA1:	F0BB798B40E4CA170ECFBD72161EF7796B58B444
SHA-256:	EC1222609F69FE70F55C1817535B0138A295EB7C71CCC443D7B3ACAA44537B5B
SHA-512:	9912AC7388A0138E809D8E25F4EE90B5952D8B4063969A79BCEB2C5E8A312878897BEF56FF3BBB0185A815262C343984D9C3113B5B5C2D0069716891110A0DFD
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....(-.S....sBIT.....O.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtAuthor.Jakub Steiner.../....tEXtDescription.mimetypes7..d...!tEXtSource.http://jimmac.musichall.czif.^....PLTE.....P..Z.....W....tRNS.....RSYs.....=^....iIDAT.W..G..@...!c ....,....YKM....c..~:s...I...U..\O..f...,..5..+.@....E.....b.B..H^..V..*.8\.r?....".z.....IEND.B`.

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	19208
Entropy (8bit):	7.005927948691754
Encrypted:	false
SSDEEP:	384:dtUDfIeFrW1hWC5OZkum0GftpBjVzm3Sx56lgCoha6LDF:dteFuJoVijz1HB
MD5:	D699333637DB92D319661286DF7CC39E
SHA1:	0BFFB9ED366853E7019452644D26E8E8F236241B
SHA-256:	FE760614903E6D46A1BE508DCCB65CF6929D792A1DB2C365FC937F2A8A240504

SHA-512:	6FA9FF0E45F803FAF3EB9908E810A492F6F971CB96D58C06F408980AB40CBA138B52D853AA0E3C68474053690DFAFA1817F4B4C8FB728D613696B6C516FA0F51
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e..... ..PE..d....." .....0.....4....`.....`..... .....=.....T..... .....rdata.....@..@.rsrc..... .....@..@..... ....

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24328
Entropy (8bit):	6.867867660778997
Encrypted:	false
SSDEEP:	384:/ZpFVhHW1hWxgYBm0GftpBjMm3SNlndaYhpn3p:boEVi6DBp
MD5:	D5166AB3034F0E1AA679BFA1907E5844
SHA1:	851DD640CB34177C43B5F47B218A686C09FA6B4C
SHA-256:	7BCAB4CA00FB1F85FEA29DD3375F709317B984A6F3B9BA12B8CF1952F97BEEE5
SHA-512:	8F2D7442191DE22457C1B8402FAAD594AF2FE0C38280AAAFC876C797CA79F7F4B6860E557E37C3DBE084FE7262A85C358E3EEAF91E16855A91B7535CB0AC832E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. .....G.....!.....0.....@.....@.....a.....0.....".=.....T.....text... a..... ..`.rsrc.....0.....@..@v.....G.....8...d...d.....G.....d.....G.....RSDS9uG.l..k..y.....api-ms-win-crt-stdio-l1-1-0.pdb.....d....rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....G....^.....(..... .....<...y.....)...h..... ...].....H... .....)...D...^...v.....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\drive-multidisk.png

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	569
Entropy (8bit):	7.482468865601557
Encrypted:	false
SSDEEP:	12:6v/7QkFqDaHfvZFpa7O/oH5kGxVI7F2bk7jv0E1YpA0sVrgY:x8qeH7MQ+px2qqj5Y60mr7
MD5:	B0C0FEE6A573A2776A013307457B6556
SHA1:	95157DA2FAD0902832E25CBEBE3EE4E58C265346
SHA-256:	1A41F703735FD48EE79E423993B2C6695E326269F7A61304DFF4796F59977FF2
SHA-512:	28CDDB1071E69145AC1845EC573618EC6268FDEF795B0F3638EB1DEC834C8FE0FC65517D9ED784F81F67535F25333FC986BD9C9B3AAB73BCE4C42837C81E16C
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.}R..A.....:...}...8.n.m..d.|..Sk.X.....{m....8...1.l...m..vn..G.....n.o..W,]..f.H..h....[.%.c.b.0...w.}../.~.F&.A.....s..ql....k%.....]..!.....R`..I..$.> @.F.F(.....a....b...;o.&L.. ...*e....&....?.....Q.V.%...-J)<~...d.V.\...E....m..L...E..b..<...k.....}.....p<.G...U.b..V.].R.V\....J.8}.,x..dT.9..!~.T?xp..... .N...c."...G.. .@..R..H.p..E .GR.....J...7.t.od.....p.%.iG.+v..\.....&\k...s.....T...}.....e0..e?I..{L..Vm.0u..f.....%c.~q.m\.,...Y..U`..O.h.p.9h%..).X...m...i@.8....IEND.B`.

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\System.Xml.XmlDocument.dll

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16024
Entropy (8bit):	6.768484247043723
Encrypted:	false
SSDEEP:	384:EVgGf2BiWOsWql//uPHRN7/2WF//dJR9ztBcvM:EVgGL4lXM/2WF//dj9zUvM
MD5:	1FED3E9E68967F0903F43CF955EC8EAE
SHA1:	DA9D98424E2BB2AE625E9EBEBD90AD4B7F007CA4

SHA-256:	B861237F55766E286E7008AC4B1E5CE88E88FDF7741EF9C6B00540E1765390F3
SHA-512:	F030383C4D933EC13EE1E892654AEEFD5C722BE25461472639DF49FA0E165AC470BFB901A0A062CA145A6B693C607E279CDBA2A144E62A5B9D2FD6E99994336 4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B....."!..0.....+... .....@.. ..... `.....\|+..O....@.....(...`.....*..8..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc .....`.....@..B.....+.....H..... .....P .....;??5.$|BdQ..h.X.3\...!..@...C.3.qS.....rS.....?D...f...../....'.ov5..N.q.|.FB..:....: .z!.rL.Q.... ...F&.....0."....+.$_BSJB.....v4.0.30319.....`.....#~..\.....#Strings....H.....#GUID...X.....#Blob.....3.....#.....P./...../.....O.. .....\...2.....g.....p...../.....

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\accessories-diction

ary.png

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	639
Entropy (8bit):	7.594477595602655
Encrypted:	false
SSDEEP:	12:6v/7xXsWeAITRagJSezSlTm4lpuXLJNux3NdHbvHR+d0FKHrHPnwF4LWbf7H:wlNVSo4gud4NxbvxI0erv04Lcf7H
MD5:	B8367F3483C54EFE19D1426A98402829
SHA1:	F9E9A067BFE5F2A3A4AE1C93D519B8B8792719C9
SHA-256:	0791574192B5767D904619B1F6BB30B3A5101FBD51F8C259C2CFFF078C7ECECD
SHA-512:	A4C0E3D1CAA4A828B9160D4936F5E11E42AFE00A9A611A0814884BBA9E18A691D16B142F5A23E2AEE11708C72AADAAB78F19733E1E541BD19E64437AC6E43A ED
Malicious:	false
Preview:	.PNG.....IHDR.....a...FIDATx.....\k..7.....1k7...km...6..]...3....5....9.w....(3..2'...`..27X^S.XV.....Gck.\cKu...q...)...9..sYu~YYU~p|r4..../..k.%.%.....s...A_.q~x.. ]P..h4.....LKC(.B . g2...0..z.....X.I..6...B.....J...i..n.|>.D.`}/.I..@-.c.....VP..F'..$.s.$M...a.V..=6._i).:.....!....$..IR...3h.r.@q8@k+..i./.\p> ..ccs...F-I{.n'..JE...C@qE.).....I.+i....pE .b...D.Zr..m,.)!.H ..HY.(..t....uF.!.....H.....iBck5.....y..hk#S0.....,..H..n..a.Z.....\a.d..Y.7..oi.\%>.....165tl.L818j.c.....p.V..j..2....g?...=....._.z....;....?Vw.....^...;|...../....w..... .?...=.....IEND.B`.

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Laboratories53\x-office-address-book-symbolic.svg

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	2059
Entropy (8bit):	5.063551723274034
Encrypted:	false
SSDEEP:	24:t4CpYL7lyKbRAecFxMGMaMlF6Yi36fRMTXoUfQBjWlu4lZ715ByKbRAecFxMGMM:fNtAecFJM/FiqfQpQipvBNtAecFJMM
MD5:	5447BF4EF18181AA69BEC4978E312549
SHA1:	4843AA2388FE80EE474F399061C6FDBB547BC2BA
SHA-256:	EC1CDEAD87BAD12FACA206F03D6748ED11F3A50FF32E8AD341BD44A3A44D6075
SHA-512:	611A25E6FE93CFA74DF01200914D730BB608B6EB05BDB8E77F13416800B45468D4067C8516C734B8C602EF4EFEF4B90D045B7456AA2BAF243526C8145BBA3D4 D
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M3 1C1 1 1 3 1 3h11v11H1s0 2 2 2h9s.459.014.947-.23C13.436 15.524 14 14.832 14 14V3c0-.833-.564-1.525-1.053-1.77C12.46.986 12 1 12 1z" 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" color="#000" font-weight="400" font-family="sans-serif" overflow="visible" fill-rule="evenodd"/><path d="M.5 4h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1z"/><path d="M7.285 5.004A3.506 3.506 0 004

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel\Homoplasy\Wice\AMD.Power.Processor.ppkg

Process:	C:\Users\user\Desktop\Royalistic.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">.. ..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\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-new-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	200
Entropy (8bit):	6.353867134664978
Encrypted:	false
SSDEEP:	6:6v/lhPys1AhcwQnKFxLsaV0MSFw6YB1L5jp:6v/7RgFKBE1L5N
MD5:	B1E1142D7EF33AD94E80A7394C036540
SHA1:	D05408C3B4360DE12D0B7A1CCB04A27E946FD517
SHA-256:	9572648AC9CA12A253EFBFB3DB0160C56CBFAAC3157779285642FAEB1D86CA94
SHA-512:	18AC511A1916E99780BAB5D3CEDBCA816932D88A4230F8FFADE5C17DBF1511840033D5A05322B0AA3EE4D30A9105D2F211C84C46DDFAAA71008444669CB65A F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..Q.. .D_...F....t..>d!jS....pa.....F`....t9.....D.`.{`M.7`H..2' >.xS.9W.|..@[...;T5..Q.... .Y.q.._-..F#F...n..W..8.L'A...!.....IEND.B`.

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-templates-symbolic.svg

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	963
Entropy (8bit):	5.12784027591558
Encrypted:	false
SSDEEP:	24:t4CptM48A8A8F+yEcGZrGF19XQzyKbRAecFxMGM7:B8A8A8F+yEcGYFmNtAecFJM7
MD5:	F5A69E814CB5E7713E3C624942DE1DA5
SHA1:	2919A07D2792295111CF54AF23742CEE14337B10
SHA-256:	06D97F580D3709C0EA0E2705425C621A17FF97CF3A449B468D2976BA0D55EFEB
SHA-512:	ABC0F7671B316DC01152253639319BED058C20D4E8C56F6D23B67AF6584F39E5F3191D97FD8F135C259E5BD7FE032939528A93029D747061500DFAE14C135D55
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747" fill-rule="evenodd"><path d="M3 9h1v1H3zm-1 1h1v1H2zm1 1h1v1H3zm-1 1h 1v1H2zm1 1h1v1H3zm-1 1h1v1H2zm2 0h1v1H4zm2 0h1v1H6zm2 0h1v1H8zm2 0h1v1h-1zm-7 1h1v1H3zm2 0h1v1H5zm2 0h1v1H7zm2 0h1v1H9zm2 0h1v1h-1zm1-1h1v1h-1z" style="marker:none" color="#000" overflow="visible"/><path d="M3 1a1 1 0 00-1 1v7h2V3h5.086L12 5.914V14h2V5.5a1 1 0 00-.293-.707l-3.5-3.5A1 1 0 0 09.5 1z" 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" color="#000" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M9 2v4h4z "/></g></svg>

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\printer-printing-symbolic.svg

Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	295
Entropy (8bit):	4.922153835627764
Encrypted:	false
SSDEEP:	6:tI9mc4slzcWER4W6UmUuksJtjdU0tytlN8uFWOXM2KchvXa7BGl0/:t4CDqW6zUmjW0ktl+sd1a7BM0/
MD5:	611C311204F39AB0E7F3CC8A0264246A
SHA1:	9E4A3BEA0DE6D11491E5AA69A61E1FF051D79DED
SHA-256:	1E6C4120B833698852CF451D0B5F8FCA83CD5591EA73EBC3C918547B67FBEB34
SHA-512:	919628653C7441CC4F82C7177D5A6EBBB86686A4E15435A21201B1D77B325808435323FA9FF906E6DB4D612ACEB1C00AC89B0571181D1F521636943EFE25EEF0
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2 4c-.5 0-1 .5-1 1v4c0 .5.5 1 1 1h1V8h10v2h1c.5 0 1-.5 1-1V5c0-.5-.5-1-1-1zm2-3v2h8V1z" fill="#2e3436"/><path class="success" d="M4 9v5h8V9zm2.99.998l2.03.011-.01 1 2.003-.01L8.03 13 5 11l2.002.011z" fill="#33d17a"/></svg>

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\screen-shared-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	254
Entropy (8bit):	6.643831924508014
Encrypted:	false
SSDEEP:	6:6v/lhPysJ/dh3z6yXtAMoWACcF/byM2TnmLzU/Jqj84up:6v/7p/dh7tfbAC0uM2ygR94c
MD5:	0DFD6D9ADF93297702595FA9A5D9A7AF
SHA1:	23A4AAE7E34232870AACF6B48B24377EA16519C6
SHA-256:	8CB87F7A9BFFD886E5931B865AB5731DF7CDD7D2768DA05808FE2D40027ED9C1
SHA-512:	880643F4BFD6F660B272EE93D38EE2513F26197053E41DF4AFE3FEC77FDBC0A087B295256451A1FB83ABAC594E6A0A585C2619D3DD400AF1DB49035E23FE555F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8.....0.E_.H. L..4...t.t.....R....SD....EN.lr..|....l.`!.@.x`.)...Z...`\7.....4 5..$.`AL.....B]b...y`...g.4..l.;.NL7.p.^.i*.....:.(.S...P. .e.....@.<...#.K....f...x~...$.C.....IEND.B`.

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\AsMultiLang.ini	
Process:	C:\Users\user\Desktop\Royalistic.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.737590272626814
Encrypted:	false
SSDEEP:	6:SIMYmm7jVYNEiJuXLIM/Cnjkq5cKYAbSJ94r1WR0rD1pulzV+ML6JyMx:SI0m7pYNEiJuXLIM6hcKc6curfQzxOf
MD5:	D96836E1DD4D151DA0687D7251B528DB
SHA1:	CCF444F32EDE194FCDE18BB32EBFCCF921E7CB30
SHA-256:	C013CFD743455DFFDBB614EA966EEC32977D7CBF096DD4A95081E7A650E8E6B9
SHA-512:	2442D9289CD7E741FF74DD99BEF39EBA7562B94DC153C3C4C4F7642455FFB0879330BC0C59B888F39A352C1C58418995F8AA319FB3BBA110B57FF7EE0A8751EF
Malicious:	false
Preview:	[Languages]..1028 = TChinese..3076 = TChinese..5124 = TChinese..2052 = SChinese..4100 = SChinese..30724 = SChinese..1034 = Spanish..3082 = Spanish..1046 = Portuguese..2070 = Portuguese..1043 = Dutch..1031 = German..1033 = English..1036 = French..1040 = Italian..1041 = Japanese..1049 = Russian..1055 = Turkish. .1042 = Korean..1029 = Czech..1035 = Finnish..1044 = Norwegian..1053 = Swedish

C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\PSReadline.psd1	
Process:	C:\Users\user\Desktop\Royalistic.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">.. ..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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.493705345043699
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:	Royalistic.exe
File size:	385376
MD5:	d14335f61c99a9b8a2d5e87cdf83cdd0
SHA1:	f82f3481619be8f9f11d76638db3107b1d332912
SHA256:	08cabec4d0127fb3e6530b04448cb3539c2b8f28988e60499c2dbbfe475206df
SHA512:	9d94b9bc836b9bb292b4e2b0ef83f1632fceb712bf60bdb3127ffaca3b4c2dcbe4aeb3f5ad3c712a47111d81c650b1a44a55e0e26f0f3f83e6727f8556d11ea2
SSDEEP:	6144:hGemq9vVMEHIx0Sc149PSjEeUlbojewwn1QuMQylhWsqfXatqMFJZV2H4ktcA8a:hmK9MNx0Sc149KAeyyeZ1QiyeVX8zHYX
TLSH:	E384F121F128BCCAD60358F01DBDA61051E5DFED80D5450D6ABA328994F239778AFF2E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....Oa.....f..... ...3.....@

File Icon

Icon Hash:	0355ccaeb2fe5500

Static PE Info

General

Entrypoint:	0x4033b3
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:	0x614F9D8B [Sat Sep 25 22:07:07 2021 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:	5f0c714c36e6cc016b3a1f4bc86559e4

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=squeaked@Dipsas.Ge, OU="Skumringstimes subhalid Cocitizen ", O=Alveolariform, L=Saint-Georges-de-Luzen\xe7on, S=Occitanie, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 8/13/2022 8:32:24 AM 8/12/2025 8:32:24 AM
Subject Chain	• E=squeaked@Dipsas.Ge, OU="Skumringstimes subhalid Cocitizen ", O=Alveolariform, L=Saint-Georges-de-Luzen\xe7on, S=Occitanie, C=FR
Version:	3
Thumbprint MD5:	7AB231DCE5C6FFAD69D73B26E510B330
Thumbprint SHA-1:	78B2E08127E635C646392C64AE8048CE0274B9EB
Thumbprint SHA-256:	D5FDEC97888AB854DBF29C2F3CDDD20DE4CEEBF3C0264DBC1620ACC59A819E35
Serial:	6A4A99A1737DDB2714130F7ACA2C5BCFD03D4200

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
sub esp, 00000220h
push esi
push edi
xor edi, edi
push 00008001h
mov dword ptr [ebp-10h], edi
mov dword ptr [ebp-04h], 0040A198h
mov dword ptr [ebp-08h], edi
mov byte ptr [ebp-0Ch], 00000020h
call dword ptr [004080B8h]
mov esi, dword ptr [004080BCh]
lea eax, dword ptr [ebp-000000C0h]
push eax
mov dword ptr [ebp-000000ACh], edi
mov dword ptr [ebp-2Ch], edi
mov dword ptr [ebp-28h], edi
mov dword ptr [ebp-000000C0h], 0000009Ch
call esi
test eax, eax
jne 00007FEA38B584B1h
lea eax, dword ptr [ebp-000000C0h]
mov dword ptr [ebp-000000C0h], 00000094h
push eax
call esi
cmp dword ptr [ebp-000000B0h], 02h
jne 00007FEA38B5849Ch
movsx cx, byte ptr [ebp-0000009Fh]
mov al, byte ptr [ebp-000000ACh]
sub ecx, 30h
sub al, 53h
mov byte ptr [ebp-26h], 00000004h
neg al
sbb eax, eax
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-000000B0h], 02h
jnc 00007FEA38B58494h
and byte ptr [ebp-26h], 00000000h
cmp byte ptr [ebp-000000ABh], 00000041h
jl 00007FEA38B58483h
movsx ax, byte ptr [ebp-000000ABh]
sub eax, 40h
mov word ptr [ebp-2Ch], ax
jmp 00007FEA38B58476h
mov word ptr [ebp-2Ch], di
cmp dword ptr [ebp-000000BCh], 0Ah
jnc 00007FEA38B5847Ah
and word ptr [ebp+00000000h], 0000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcf000	0x14bf8	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5d730	0xa30	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.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	0x65ba	0x6600	False	0.6783088235294118	data	6.475278602230841	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1382	0x1400	False	0.4626953125	data	5.262676635269928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x48538	0x600	False	0.4615885416666667	data	4.125526322488032	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x53000	0x7c000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xcf000	0x14bf8	0x14c00	False	0.16929828689759036	data	4.457664961464067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xcf250	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 0	English	United States
RT_ICON	0xdfa78	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	English	United States
RT_ICON	0xe2020	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	English	United States
RT_ICON	0xe30c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	English	United States
RT_DIALOG	0xe3530	0x100	data	English	United States
RT_DIALOG	0xe3630	0x11c	data	English	United States
RT_DIALOG	0xe3750	0xc4	data	English	United States
RT_DIALOG	0xe3818	0x60	data	English	United States
RT_GROUP_ICON	0xe3878	0x3e	data	English	United States
RT_MANIFEST	0xe38b8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked

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

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: Royalistic.exe PID: 5700, Parent PID: 3528

General

Target ID:	0
Start time:	10:38:05
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\Royalistic.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Royalistic.exe
Imagebase:	0x400000
File size:	385376 bytes
MD5 hash:	D14335F61C99A9B8A2D5E87CDF83CDD0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000000.00000002.834425818.0000000000677000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.834648652.0000000004EF6000.00000040.00001000.00020000.00000000.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	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nst18DB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E4D	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	9	4058C7	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	9	4058C7	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	9	4058C7	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	9	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Afdelingskontorer.Ate	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel\Homoplasy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel\Homoplasy\Wice	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel\Homoplasy\Wice\AMD.Power.Processor.ppkg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\AsMultiLang.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\PSReadline.psd1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\System.Xml.XmlDocument.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\accessories-dictionary.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\drive-multidisk.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-new-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-templates-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\printer-printing-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\screen-shared-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Laboratories53	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Laboratories53\x-office-address-book-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Affaldsproblem	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Affaldsproblem\x-office-spreadsheet.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E4D	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	4058C7	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	4058C7	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	4058C7	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4058C7	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	4058C7	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsk1BF9.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	405887	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E16	CreateFileA
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	290	405E16	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nst18DB.tmp	success or wait	1	4036F5	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp	success or wait	1	405A48	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Afdelingskontorer.Ate	0	26481	00 00 fd 00 00 00 fd fd 00 00 00 00 fd fd 00 3f 00 fd 00 73 00 00 00 fd 00 00 00 30 00 fd 00 fd fd fd 00 fd 00 fd 00 00 fd 00 08 00 00 fd fd 00 27 00 00 00 03 03 00 62 62 62 00 00 fd 00 00 00 fd 00 00 00 fd 00 1e 00 3e 3e 00 00 fd fd 00 49 49 00 00 7d 7d 00 fd fd 00 00 fd fd fd fd 00 00 00 3b 3b 3b 00 fd 00 00 00 00 6b 6b 00 00 00 00 00 69 69 69 69 00 fd fd 00 fd 00 58 58 58 58 58 00 00 00 00 71 71 71 00 fd fd 00 69 69 69 69 00 00 2b 2b 00 1f 1f 1f 00 59 59 00 00 00 30 30 00 00 00 00 fd 00 73 00 00 fd fd 00 37 00 fd 00 45 45 45 00 00 00 fd fd 00 fd 00 00 00 00 00 00 fd fd fd 00 00 4d 00 00 fd 00 fd 00 26 00 fd 00 fd 00 5c 5c 5c 5c 00 fd fd fd 00 00 00 00 2f 00 00 fd fd 00 00 00 fd fd 00 4f 00 00 00 00 00 fd 00 fd fd fd 00 00 00 00 36 00 fd fd 00 00 00 00 66	? s0'bbb>>II}};;;kkiiiiXXXXXqqq iiii++YY00s7EEEM&\\\\O6f	success or wait	14	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel\Homoplasy\Wice\AMD.Power.Processor.ppkg	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	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\AsMultiLang.ini	0	398	5b 4c 61 6e 67 75 61 67 65 73 5d 0d 0a 31 30 32 38 20 20 20 3d 20 54 43 68 69 6e 65 73 65 0d 0a 33 30 37 36 20 20 20 3d 20 54 43 68 69 6e 65 73 65 0d 0a 35 31 32 34 20 20 20 3d 20 54 43 68 69 6e 65 73 65 0d 0a 32 30 35 32 20 20 20 3d 20 53 43 68 69 6e 65 73 65 0d 0a 34 31 30 30 20 20 20 3d 20 53 43 68 69 6e 65 73 65 0d 0a 33 30 37 32 34 20 3d 20 53 43 68 69 6e 65 73 65 0d 0a 31 30 33 34 20 3d 20 53 70 61 6e 69 73 68 0d 0a 33 30 38 32 20 3d 20 53 70 61 6e 69 73 68 0d 0a 31 30 34 36 20 3d 20 50 6f 72 74 75 67 75 65 73 65 0d 0a 32 30 37 30 20 3d 20 50 6f 72 74 75 67 75 65 73 65 0d 0a 31 30 34 33 20 3d 20 44 75 74 63 68 0d 0a 31 30 33 31 20 3d 20 47 65 72 6d 61 6e 0d 0a 31 30 33 33 20 3d 20 45 6e 67 6c 69 73 68 0d 0a 31 30 33 36 20 3d 20 46 72 65 6e 63 68 0d	[Languages]1028 = TChinese3076 = TChinese5124 = TChinese2052 = SChinese4100 = SChinese30724 = SChinese1034 = Spanish3082 = Spanish1046 = Portuguese2070 = Portuguese1043 = Dutch1031 = German1033 = English1036 = French	success or wait	1	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\PSReadline.psd1	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	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\System.Xml.XmlDocument.dll	0	16024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 42 ad fd 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 30 00 00 0c 00 00 00 08 00 00 00 00 00 00 fd 2b 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 5d 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELB"!0+ @ `	success or wait	1	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\accessories-dictionary.png	0	639	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 02 46 49 44 41 54 78 01 fd fd 03 fd 5c 6b 14 fd 37 fd fd 0d eb fd 18 fd 11 fd 31 6b 37 fd fd 1b 6b 6d fd fd fd 36 f6 fd 5d fd fd fd 33 fd fd fd fd 35 fd fd fd fd 39 fd 77 fd fd e4 fd 28 33 fd fd 32 27 fd fd fd 60 fd fd 32 37 58 5e 53 fd 58 56 fd fd fd fd fd fd 47 63 6b fd 5c 63 4b 75 fd fd fd 71 fd fd fd 29 fd fd fd 39 fd fd 73 59 75 7e 59 59 55 7e 70 7c 72 34 16 0e fd fd 2f fd 1b 6b fd 25 fd 25 fd fd 0e 06 03 fd fd fd fd fd 73 fd fd 1c 41 5f 19 71 7e 78 fd 2e 5d 50 fd fd 68 34 fd fd fd fd fd fd fd fd 4c 4b 43 28 14 42 20 10 20 67 32 fd 04 fd 30 fd 08 7a fd fd fd fd fd fd 0e 58 fd 49 fd fd 36 fd 18 fd 42 fd fd 13 fd fd 4a fd fd a6 69	PNGIHDRaFIDATx\k71k7km6]359w(3 2'`27X^SXVGck\cKuq)9sYu~YYU~p| r4/k%%sA_q~x.]Ph4LKC(B g20zXI6BJi	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll	0	19208	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 33 41 0b fd 77 20 65 fd 77 20 65 fd 77 20 65 fd 18 44 65 fd 76 20 65 fd 18 44 61 fd 75 20 65 fd 18 44 fd fd 76 20 65 fd 18 44 67 fd 76 20 65 fd 52 69 63 68 77 20 65 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 fd fd 17 08 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0c 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$3Aw ew ew eDev eDau eDv eDgv eRichw ePEd"	success or wait	1	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll	0	24328	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 33 41 0b fd 77 20 65 fd 77 20 65 fd 77 20 65 fd 18 44 65 fd 76 20 65 fd 18 44 61 fd 75 20 65 fd 18 44 fd fd 76 20 65 fd 18 44 67 fd 76 20 65 fd 52 69 63 68 77 20 65 fd 50 45 00 00 4c 01 02 00 fd 1b fd 47 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 0c 00 1c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$3Aw ew ew eDev eDau eDv eDgv eRichw ePELG!0	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\drive-multidisk.png	0	569	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 02 00 49 44 41 54 78 01 7d 52 fd 9c 41 10 fd 0f fd fd 3a 06 fd fd 7d fd 39 fd 38 b6 6e fd 6d fd fd 64 19 7c 18 fd 53 6b fd 58 fd fd fd fd 3a 7b 6d fd fd fd fd 38 13 1d c1 31 06 6c 1a 1c fd 6d fd fd 76 6e 1b 0c 47 0d fd 15 fd fd fd 6e fd 6f fd fd 57 2c 5d fd fd 66 fd 48 fd fd 68 fd fd 15 fd 5b 20 fd 25 fd 63 fd 62 fd 30 fd fd fd 77 fd 7d fd 06 2f 15 7e fd 46 26 fd 41 fd 0a fd fd fd 73 fd 11 71 6c fd 24 fd fd 6b 25 fd fd fd fd 02 fd 5d fd 05 21 fd fd 1f 04 fd 11 52 60 fd fd 49 fd fd 24 fd 3e 40 fd 46 18 46 28 fd fd 10 fd 04 61 fd fd 1f fd 62 fd fd 58 3b 6f 0e 26 4c fd fd 20 08 fd 00 2a 65 fd fd 02 fd 26 fd fd fd 02	PNGIHDRaIDATx}RA:}8n md|SkX{m81 lmvnGnoW,]fHh[%cb0w}/~F&Asqlk %]!R`I$>@FF(ab;o&L *e&	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-new-symbolic.symbolic.png	0	200	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 7f 49 44 41 54 38 fd 53 51 0a fd 20 10 44 5f fd 15 fd 46 fd fd ce fd 74 fd fd 3e 64 21 6a 53 fd fd fd fd 70 61 fd fd fd fd fd 46 60 07 fd fd 04 74 39 fd 7f 09 fd fd 1c 44 fd 60 fd 7b 60 4d fd 37 60 48 01 14 32 27 20 3e 07 78 53 fd 39 57 18 7c fd 7f 40 5b fd 13 fd 3b 54 35 08 fd 51 e0 fd fd 18 20 fd 59 1c 71 0f fd 5f 2d fd fd 46 23 46 fd fd 10 6e 01 fd 57 fd 01 38 01 4c 27 41 fd 09 fd 21 16 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8 Q D_Ft>d!jS paF`t9D`{`M7`H2' >xS9W|@[;T5Q Yq_- F#FnW8L'A!IENDB`	success or wait	1	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-templates-symbolic.svg	0	963	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 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 20 66 69 6c 6c 2d 72 75 6c 65 3d 22 65 76 65 6e 6f 64 64 22 3e 3c 70 61 74 68 20 64 3d 22 4d 33 20 39 68 31 76 31 48 33 7a 6d 2d 31 20 31 68 31 76 31 48 32 7a 6d 31 20 31 68 31 76 31 48 33 7a 6d 2d 31 20 31 68 31 76 31 48 32 7a 6d 31 20 31 68 31 76 31 48 33 7a 6d 2d 31 20 31 68 31 76 31 48 32 7a 6d 32 20 30 68 31 76 31 48 34 7a 6d 32 20 30 68 31 76 31 48 36 7a 6d 32 20 30 68 31 76 31 48 38 7a 6d 32 20 30 68 31 76 31 68 2d 31 7a 6d 2d 37 20 31 68 31 76 31 48 33 7a 6d 32 20 30 68 31 76 31 48 35 7a 6d 32 20 30 68 31 76 31	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747" fill-rule="evenodd"><path d="M3 9h1v1H3zm-1 1h1v1H2zm1 1h1v1H3zm-1 1h1v1H2zm1 1h1v1H3zm-1 1h1v1H2zm2 0h1v1H4zm2 0h1v1H6zm2 0h1v1H8zm2 0h1v1h-1zm-7 1h1v1H3zm2 0 h1v1H5zm2 0h1v1	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\printer-printing-symbolic.svg	0	295	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 70 61 74 68 20 64 3d 22 4d 32 20 34 63 2d 2e 35 20 30 2d 31 20 2e 35 2d 31 20 31 76 34 63 30 20 2e 35 2e 35 20 31 20 31 20 31 68 31 56 38 68 31 30 76 32 68 31 63 2e 35 20 30 20 31 2d 2e 35 20 31 2d 31 56 35 63 30 2d 2e 35 2d 2e 35 2d 31 2d 31 2d 31 7a 6d 32 2d 33 76 32 68 38 56 31 7a 22 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 73 75 63 63 65 73 73 22 20 64 3d 22 4d 34 20 39 76 35 68 38 56 39 7a 6d 32 2e 39 39 2e 39 39 38 6c 32 2e 30 33 2e 30 31 31 2d 2e 30 31 20 31 20 32 2e 30 30 33 2d 2e 30 31 4c 38 2e 30 33 20 31 33	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2 4c-.5 0-1 .5-1 1v4c0 .5.5 1 1 1h1V8h10v2h1c.5 0 1-.5 1-1V5c0-.5-.5-1-1-1zm2-3v2h8V1z" fill="#2e3436"/><path class="success" d="M4 9v5h8 V9zm2.99.998l2.03.011-.01 1 2.003-.01L8.03 13	success or wait	1	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\screen-shared-symbolic.symbolic.png	0	254	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 fd 0d fd 30 10 45 5f fd 48 fd 20 4c fd 00 34 0c fd 00 74 fd 74 fd fd 13 fd 05 52 fd fd fd fd 53 44 fd fd fd 0b 45 4e fd 6c 72 fd fd 7c fd fd fd fd 6c fd 60 21 15 40 05 78 60 fd 29 0f fd fd 5a 03 fd fd 60 5c 37 0d fd 12 b3 fd fd 34 20 35 fd 04 24 1b 60 41 4c fd 03 fd 03 1b 42 5d 62 fd fd 7f 79 60 07 fd 13 67 fd 34 fd 04 6c fd 3b fd 4e 4c 37 fd 70 00 5e fd 69 2a 1c 00 fd 02 fd fd fd 0a 3b 0d 28 0d 53 fd fd 1a 50 08 fd 65 04 1d fd 16 06 fd fd fd fd 40 0d 3c 19 fd fd 23 fd 4b fd 16 fd fd 66 fd fd fd 78 7e fd 02 fd 24 fd 43 05 fd fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT80E_H L4ttRS DENIr|I`!@x`)Z`\74 5$`ALB]by`g4I;NL7p^i*; (SPe@<#Kfx~$CIENDB`	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Laboratories53\x-office-address-book-symbolic.svg	0	2059	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 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 31 43 31 20 31 20 31 20 33 20 31 20 33 68 31 31 76 31 31 48 31 73 30 20 32 20 32 20 32 68 39 73 2e 34 35 39 2e 30 31 34 2e 39 34 37 2d 2e 32 33 43 31 33 2e 34 33 36 20 31 35 2e 35 32 34 20 31 34 20 31 34 2e 38 33 32 20 31 34 20 31 34 56 33 63 30 2d 2e 38 33 33 2d 2e 35 36 34 2d 31 2e 35 32 35 2d 31 2e 30 35 33 2d 31 2e 37 37 43 31 32 2e 34 36 2e 39 38 36 20 31 32 20 31 20 31 32 20 31 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 66 6f 6e 74	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M3 1C1 1 1 3 1 3h11v11H1s0 2 2 2h9s.459.014.947-.23C13.436 15.524 14 14.832 14 14V3c0-.833-.564-1.525-1.053-1.77C12.46.986 12 1 12 1z" style="line-height:normal;font	success or wait	1	405EAB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Affaldsproblem\x-office-spreadsheet.png	0	546	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 03 00 00 00 28 2d 0f 53 00 00 00 03 73 42 49 54 08 08 08 fd fd 4f fd 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 77 77 77 2e 69 6e 6b 73 63 61 70 65 2e 6f 72 67 fd fd 3c 1a 00 00 00 14 74 45 58 74 41 75 74 68 6f 72 00 4a 61 6b 75 62 20 53 74 65 69 6e 65 72 fd fd fd 2f 00 00 00 15 74 45 58 74 44 65 73 63 72 69 70 74 69 6f 6e 00 6d 69 6d 65 74 79 70 65 73 37 fd fd 64 00 00 00 21 74 45 58 74 53 6f 75 72 63 65 00 68 74 74 70 3a 2f 2f 6a 69 6d 6d 61 63 2e 6d 75 73 69 63 68 61 6c 6c 2e 63 7a 69 66 fd 5e 00 00 00 fd 50 4c 54 45 00 00 00 fd aa fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	PNGIHDR(-SsBITOpHYs+tEXtSoftwarewww.inkscape.org<tEXtAuthorJakub Steiner/tEXtDescriptionmimetypes7d!tEXtSourcehttp://jimmac.musichall.czif^PLTE	success or wait	1	405EAB	WriteFile
C:\Users\user\AppData\Local\Temp\nsk1BF9.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2f 40 74 fd 6b 21 1a fd 6b 21 1a fd 6b 21 1a fd 39 54 19 fd 6c 21 1a fd 20 59 1b fd 6c 21 1a fd 6b 21 1b fd 78 21 1a fd fd 54 1e fd 6f 21 1a fd fd 54 19 fd 6a 21 1a fd fd 54 1a fd 6a 21 1a fd fd 54 18 fd 6a 21 1a fd 52 69 63 68 6b 21 1a 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 4c fd 63 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$/@tk!k!k!9Tl!Yl!k!x!To!Tj!Tj!Tj!Richk!PELc"	success or wait	1	405EAB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Royalistic.exe	unknown	512	success or wait	243	405E7C	ReadFile
C:\Users\user\Desktop\Royalistic.exe	unknown	4	success or wait	2	405E7C	ReadFile
C:\Users\user\Desktop\Royalistic.exe	unknown	4	success or wait	43	405E7C	ReadFile
C:\Users\user\Desktop\Royalistic.exe	unknown	4	success or wait	2	405E7C	ReadFile
C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Afdelingskontorer.Ate	unknown	78622720	success or wait	1	73432C85	ReadFile

Disassembly

No disassembly