ID: 711461
Sample Name: dlawt.exe
Cookbook: default.jbs
Time: 07:22:08
Date: 28/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

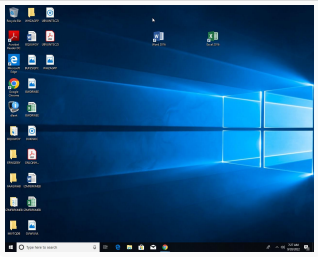
Windows Analysis Report

dlawt.exe

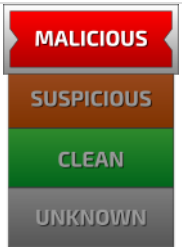
Overview

General Information

Sample Name:	dlawt.exe
Analysis ID:	711461
MD5:	cf313a27bceba3…
SHA1:	4ff90062880efe5..
SHA256:	d4fba0fc4c7c133..
Tags:	exe
Infos:	



Detection



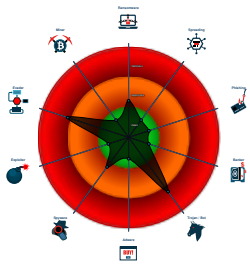
GuLoader

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

Signatures

- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- 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 call native …
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- dlawt.exe (PID: 4772 cmdline: "C:\Users\user\Desktop\dlawt.exe" MD5: CF313A27BCEBA36C7FA863BA1E935676)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.764563797.0000000003208000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Yara detected GuLoader

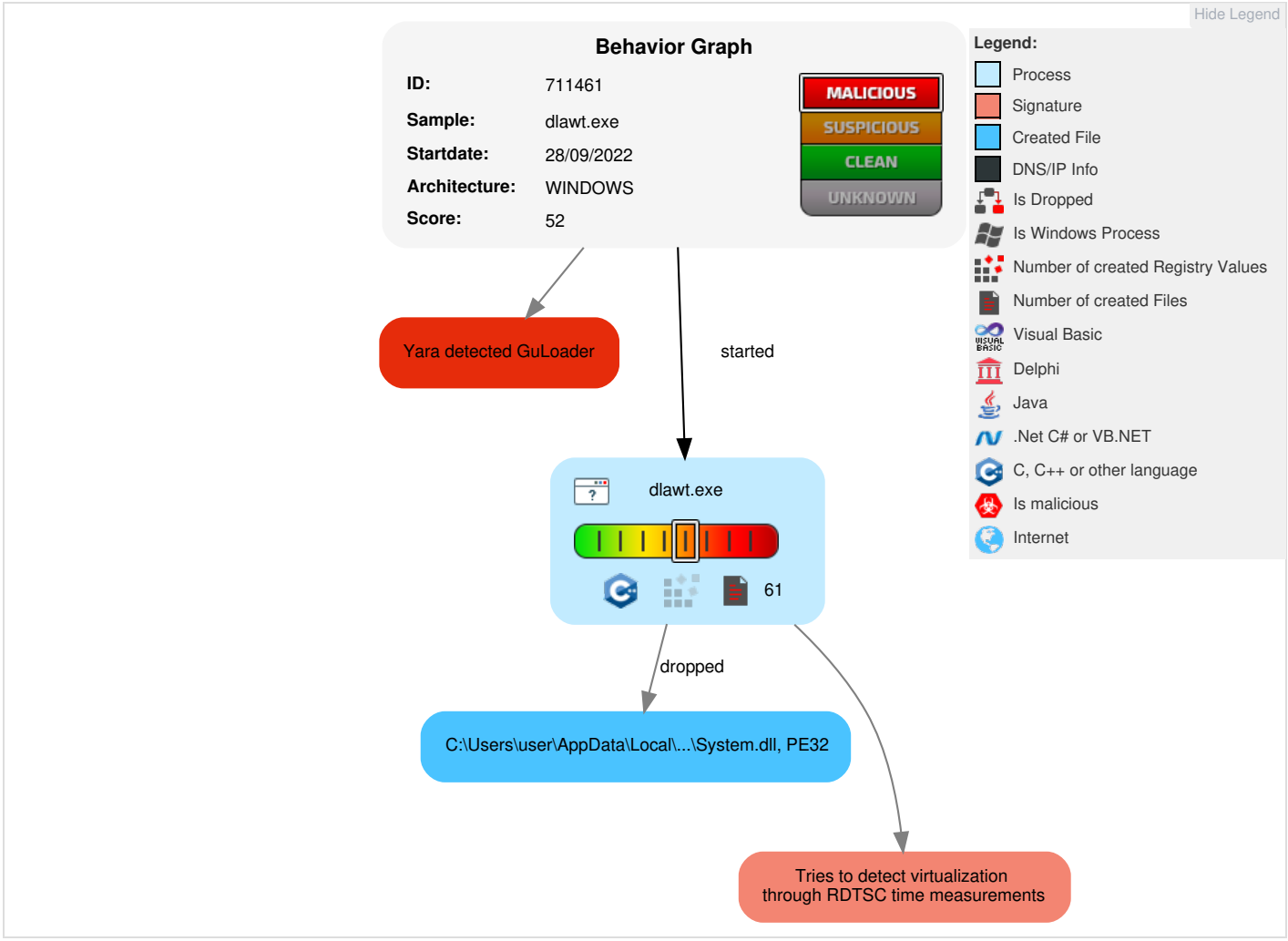
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	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 Software Packing	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

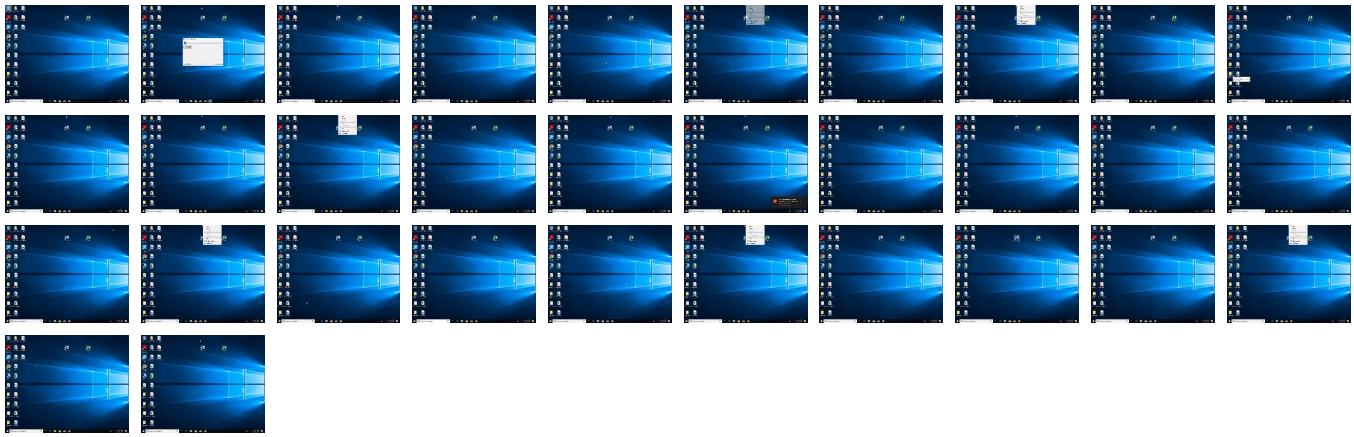
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dlawt.exe	3%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsq995B.tmp\System.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsq995B.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsq995B.tmp\System.dll	4%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.dlawt.exe.410ea0.1.unpack	100%	Avira	ADWARE/Adware.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://sun.com/2000/XMLSearch	0%	Avira URL Cloud	safe	
http://jimmac.musichall.czif	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://sun.com/2000/XMLSearch	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://creativecommons.org/licenses/by-sa/4.0/	folder-download.png.0.dr	false		high
http://openoffice.org/2000/chart	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://openoffice.org/2000/style	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://openoffice.org/2000/help	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://openoffice.org/2000/table	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://jimmac.musichall.czif	text-x-generic.png.0.dr	false	• Avira URL Cloud: safe	unknown
http://openoffice.org/2000/drawing	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://openoffice.org/2000/meta	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	dlawt.exe	false		high
http://openoffice.org/2000/text	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://openoffice.org/2000/datastyle	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://mozilla.org/MPL/2.0/.	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high
http://openoffice.org/2000/office	dlawt.exe, 00000000.00000003.243677360.0000000002953000.00000004.00000800.00020000.00000000.sdmp, idxcaption.xsl.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	711461
Start date and time:	2022-09-28 07:22:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 8s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dlawt.exe
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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.troj.evad.winEXE@1/24@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.7% (good quality ratio 84.6%) • Quality average: 87.6% • Quality standard deviation: 21.3%
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, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, login.live.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsq995B.tmp\System.dll

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.890541747176257
Encrypted:	false
SSDEEP:	192:X24sihno0bW+l97H4GB7QDs91kMtwtobTr4u+QHbazMNHT7dmNIEr:m8vJl97JeoxtN/r3z7YV
MD5:	75ED96254FBF894E42058062B4B4F0D1
SHA1:	996503F1383B49021EB3427BC28D13B5BBD11977
SHA-256:	A632D74332B3F08F834C732A103DAFEB09A540823A2217CA7F49159755E8F1D7
SHA-512:	58174896DB81D481947B8745DAFE3A02C150F3938BB4543256E8CCE1145154E016D481DF9FE68DAC6D48407C62CBE20753320EBD5FE5E84806D07CE78E0EB0C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 4%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....oZ.....!..... .....)....0.....`.....@.....2.....0..P.....P.....0..X. .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...x....@.....(.....@....reloc..~....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Algae62\plkkers\Reputation\network-cellular-4g-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	544
Entropy (8bit):	4.840636545565347
Encrypted:	false
SSDEEP:	12:t4CDqsLWbjUzkTWem7+0qoLIGYJJufPm3ioprGDRl+i:t4CdLWbjUgSl8sfPAnrGDRlN
MD5:	6CD1ED8B1D8500C9A1480425DA4282D6
SHA1:	F1B935DD259BCD198784C1C2FA6516230624C43B
SHA-256:	FAD0ECD186B6DEC11FBB094876E7381B2A097E1EF9D641527E3295132410EF44
SHA-512:	6BC432608A3630136E2E8E44F69A81B9C5F9FE479DA5DD3E35A77168A66F3C41D72DC0E49FB623E74B9527CF031FBBBE447213CE4C0FDFDA4A9AB410439977(1
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2.063 0A2.048 2.048 0 000 2.063v11.874C0 15.088.912 16 2.063 16h11.874A2.048 2.048 0 0016 13.937V2.063A2.048 2.048 0 0013.937 0zM2 3h2v4h1V3h2v10H5V9H4c-1 0-2-.842-2-2zm8 0h2c.833 0 1 .525.564 1.77 1.053.244.488.23.947.23.947v1h-2V5h-2v6h2V9h-1V7h3v4s.014.459-.23.947C13.525 12.436 12.833 13 12 13h-2s-.459.014-.947-.23C8.564 12.525 8 11.833 8 11V5s-.014-.459.23-.947C8.475 3.564 9.167 3 10 3z" style="marker:none" color="#bebebe" overflow="visible" fill="#2e3436"/></svg>

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer\CoverEdCtrl.manifest

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (923), with CRLF line terminators
Category:	dropped
Size (bytes):	983
Entropy (8bit):	5.440797719362896
Encrypted:	false
SSDEEP:	24:Jdt4VIWcqHQe22Hs7uYwL1z7m91q7LY7o94Iqw1q769C77o94Iqn+:3SIJeRXm9vowwXC/own+
MD5:	E70ABF046645F771B84F377FE86C6150

SHA1:	D05C4926656D80C1E3E34441BB1AAD6531FF3949
SHA-256:	E0257221F542666CFBCF5E9B9F0BF43A86BFBF363682586FF18AB77C2A76D4C4
SHA-512:	34501A7A7F14EF655817439CD5F8F1EB8A00A9057F5423B516D21205BFC6C5120208C19710A973FAEE4AE65454EAF0099870734F0F02AC1D54991DF5BFD0C005
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"><assemblyIdentity name="CoverEdCtrl" version="1.4.0.0"></assemblyIdentity><file name="CoverEdCtrl.ocx" hashalg="SHA1"><comClass clsid="{2C28E255-B7C9-4C5E-A66C-EFCB7F8561F0}" tlbid="{E9D0A918-D3A4-4E3D-9DFE-15BC69230416}" description="CoverEdCtrl Control"></comClass><typelib tlbid="{E9D0A918-D3A4-4E3D-9DFE-15BC69230416}" version="1.4" helpdir=""></typelib></file><comInterfaceExternalProxyStub name="_DCoverEdCtrl" iid="{7EDE47CE-3AA8-44B9-BF34-1B593C1C8783}" tlbid="{E9D0A918-D3A4-4E3D-9DFE-15BC69230416}" proxyStubClsid32="{00020420-0000-0000-C000-000000000046}"></comInterfaceExternalProxyStub><comInterfaceExternalProxyStub name="_DCoverEdCtrlEvents" iid="{1E2C8B29-7C8B-42A9-B9C8-5C0B908CB286}" tlbid="{E9D0A918-D3A4-4E3D-9DFE-15BC69230416}" proxyStubClsid32="{00020420-0000-0000-C000-000000000046}"></comInterfaceExternalProxyStub></assembly>

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer\Lakridset.bmp

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PC bitmap, Windows 3.x format, 72 x 399 x 24, image size 86184, cbSize 86238, bits offset 54
Category:	dropped
Size (bytes):	86238
Entropy (8bit):	6.474378163731263
Encrypted:	false
SSDEEP:	1536:HZsCm1/4YEWvb8KSlLJY9xgt0AES8FBgih+RgS2xdW:+Cm1/VEQ8JmxgOAEfEJ6JQ
MD5:	E74DE44364D6E680988FCDC9330819C6
SHA1:	83F2BE7EC78921A46367208266BE672E013699A6
SHA-256:	59713500232DE1455422E70BD5D77EC4DAFF2985A76A374DD60865A35F4C29BD
SHA-512:	909BD87C6EB242BAD068D7885169F614FC6CA9EC96C4A4801D806CE480CA7EA1883B6EBDFE0A75C9807FADE0021B24BC5529B6607C17C53084BA9FBA931F9E96
Malicious:	false
Reputation:	low
Preview:	BM.P.....6...(...H.....P.....a|.,|...@..Y.\0.o.....4pI..)..2lMm..84%<.....p....+.'!?..*7... dO.C.....3.Q.K.....qc.J.z....aMJ&.A.{...Qa...ItM.u.N....P[...5wh.{.y.)>....&C..K]...Mo.t.2....Z...$}.:+,/..mx4w.....K..M..c.Q.hVL.....Pg5.T.u.I..n.....6(D.....#..c..d}{.I...]..)\|^..t/.5.....c..o...v....;....-.....J]..,9.W.I.4;. gdw+.].....F..~....B..c.A.._../..<..1.6..Bk.a>...D.x.1.*..u...b1.....L....._ .....K...ET.R...q.s.!...(/..i8/....WH....b....(6.J.O.....3_...'.>!.0..,n.W...fg..W.b.+V..R}b.Y..F.....gQ.V..A...:....{<.bKI./..~G...a..7.?..?.9m=k..K9Gt...]f..H.... ..(../...:E..+.6R;.:.....pk.....e.G.%.8..\..U..*a]p...Z.`....J..{%.G!..[x..x....?q.E..\..?....\..5.._t27Q$(.{..m...j.:h..}..b.Q.....M.I....Bue.7.A]G-.f..e..B .&...4..-p..p....a.5...9...+.H.,...~..>...y[.:.8.....~k...B.S.t."......6.+....,.B..lY..&~..{.?.'.C8..k ....MM.....N/...Q..~..qV]......2.....k.2..v<.+JA...c.n...f

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Bacin\Besjlings\network-wireless-connected-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.826941536649534
Encrypted:	false
SSDEEP:	24:t4Cf9xjMJtMCl/HBa2XtRYXl5hHTlPKeTyH2ISNdIIqqVVYSNeISNkN4AeWlGMyf:lPY/b7D5JFSs1SFSON4Ae3MQRf
MD5:	896D9A7F865BFDDFA0442C0B44E73F23
SHA1:	6CB83C54EAADE1209F9877065C767BF1DC90B8A1
SHA-256:	85500E1D92C70F203CCA0945D774CD35848120DB46C553ECF3F3D3858DDC2494
SHA-512:	E921924AE3041757A240CCE91E2C4455F043D9AB330B8FA8EABA21E4494427D25BE25D7CE8A6313DEE711F743EBAA0AC678D317F7AD83E0F092901D304D5ECD2
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><defs><clipPath id="a"><path d="M-73-30l-7-7v-4.5h16.5v4.5l-7.5 7z" fill="none" stroke="#000"/></clipPath></defs><g fill="#474747"><path clip-path="url(#a)" d="M-72-38v1h1v-.969A12.13 12.13 0 00-72-38zm1 1v1h1v-1zm1 0h1v-.594a9.508 9.508 0 00-1-.218zm1 0v1h1v-1zm1 0h.5c-.165-.084-.327-.145-.5-.219zm0 1v1h1v-1zm1 0h1v1h1a7.865 7.865 0 00-2-1.719zm2 1v1h-1v1h-1v1h-1v1h-1v1h-1v-1h-1v1h-1v-1h-1v-1h-1v-1h-.563c-1.565 1.851-.437 4.376-.437 7 0 5.215 1.39 6 7 6s7-.784 7-6c0-2.374 1.296-5.441 0-7zm-13 0h1v-1h-.563c-.144.124-.3.242-.437.375zm1-1h1v-1h-.063a8.017 8.017 0 00-.937.563zm1-1h1v-.5c-.346.125-.68.303-1 .469zm1 0v1h1v-1zm1 0h1v-.938a8.79 8.79 0 00-1 .157zm1 0v1h1v-1zm1 1v1h1v-1zm1 1v1h1v-1zm1 0h1v-1h-1zm1 0v1h1v-1zm1 1v1h1v-1zm1 0h1v-1h-1zm-1 1h-1v1h1zm-1 1h-1v1h1zm-1 0v-1h-1v1zm-1 0h-1v1h1zm-1 0v-1h-1v1zm-1 0h-1v1h1zm-1 0v-1h-1v1zm0-1h1v-1h-1zm1 0v1h1v-1zm1 0h1v-1h-1zm1 0v

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen\audio-x-generic-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	195

Entropy (8bit):	6.350068028436895
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBll/0xEq2j5+j61kca4OSpTC7qtl2BeKlirjjBbEqY:6v/lhPysSEq2sca4OKocrSVp
MD5:	79B7B2040BFDFF36BEC2D20F727DFC7E
SHA1:	C31B14267B8B5DADC7151D82E8378D2CC5CB653A
SHA-256:	6B0807769D18D56DCC9AB666FC8A6F7160E9707C3BC02545EABDF16C5D4029B8
SHA-512:	6E042161CF966ABB32840AD937F257CB893D513EC0E2CE663BCAB9A02B9639F8B38F359FF3C8EEDA522D76DB7F60C1068303FC66FE17742660D7E6D9C892DF 6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....sBIT....|.d....zIDAT8.....0....W.t.....O>.....A.et.P.@(.O.&.26+....Mm..6.....g..'L.f...RrY.....G.op...sF....>c....u.0.....>^nyD;A.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen\changes-prevent-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	998
Entropy (8bit):	5.1868425916607555
Encrypted:	false
SSDEEP:	12:t4CP5GD09xmuPHoJdRnZopTi3b1USS0LLcXNo3F3iCydrkeYRAerAFFLAmP502Kp:t4CBGD0KvRW+Li+3FLyKbRAecFxV0/YK
MD5:	790B7AEF699FC380D50CFB583F09EF44
SHA1:	E8F31F4CC603DF24FF456271E8BEFEE8FBC588D6
SHA-256:	CD34406714AA8018144064852CE932016BE8FE06F1F0CEA06060B95F8E8E6D8E
SHA-512:	C5674F4F9AE8D78AE0E239E7AE0FD156B75D21CA9D2216D2B851D3BCA8239CFD62414C2165A3BFEC71F997D9AFD08EC821D8233A745BBD756E0F908F830566 B8
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#bebebe" fill="#474747"><path d="M3 7h10c.554 0 1 .446 1 1v3c0 .554-.446 1-1 1H3c-.554 0-1-.446-1-1V8c0-.554.446-1 1-1z" style="marker:none" overflow="visible"/><path d="M7 1s-.709-.014-1.447.355C4.814 1.725 4 2.667 4 4v4h2V4c0-.667.186-.725.447-.855C6.71 3.014 7 3 7 3h2s.291.014.553.145c.261.13.447.188.447.855v4h2V4c0-1.333-.814-2.275-1.553-2.645C9.71.986 9 1 9 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;marker:none" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M2 10h12v4H2z" style="marker:none" overflow="visible"/></g></svg>

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\dialog-information-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1626
Entropy (8bit):	5.0762260088454605
Encrypted:	false
SSDEEP:	24:t4Cpl+6kKDPeexH0BqyKbRAecFxMGMZLxdOUyKbRAecFxMGM+pMc:V7lH0BqNtAecFJM3fNtAecFJMu
MD5:	1A31C93C41C667E8802FCC6B0DB782D3
SHA1:	8436084E01D6B5D996A54D00E8AE95196865B928
SHA-256:	BA163884E8DBD085280F6D4FEF52AAB07A10CDC540E657B5AD16D9773FD31BBD
SHA-512:	7BCC9B6D0D3EE6D79A2AF8CCFA8734DF4AF5BCA6079110FA3B65FF10024A4F75C2BBCEF106086E36E4B3D293648EE4FBB23C4C49EA8EEBDBC84854DFCB4F F5EB
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#2e3436"><path d="M7.994 0a6.01 6.01 0 00-5.87 4.777c-.528 2.533.69 5.036 2.874 6.327l.002.898A1 1 0 006 13h4a1 1 0 001-.998l.002-.9c2.183-1.293 3.399-3.797 2.87-6.33A6.01 6.01 0 007.993 0zm.002 2c1.9 0 3.529 1.322 3.918 3.182a3.99 3.99 0 01-2.312 4.484 1 1 0 00-.6.914L9 11H6.998v-.418a1 1 0 00-.602-.914 3.992 3.992 0 01-2.314-4.484A3.99 3.99 0 017.996 2z" 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="M6 15c0 .554.446 1 1 1h2c.554 0 1-.446 1-1v-1H6z"/><path d="M6.992 5.994a.5.5

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\drive-harddisk-solidstate-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	195

Entropy (8bit):	6.3462536867112
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBll/V2a02b5Ra2J6NJIMlbAytVqoL7+5KWtCYnscao:6v/lhPysma089QBbpqW7+oKs5HoE6Xjp
MD5:	5B6732EE14014007E6B0CAEB9AB35BAA
SHA1:	7F610426DD3E8560E4BFDDE6ECF8631068056B0E
SHA-256:	2E2BB0B7FD175718A6ED195A1C6F0D3D63AE0A23C75648BC5E8D86E6A738B839
SHA-512:	8AEC8F1F1FA122EC4829D65C0135D0A50A788C26C289655520353316D2A11781FC962A71A7237067EF7EF0B08DAFE9516B7EF39681B2FC3F733CA2010112E256
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....zIDAT8..A.. ..G.~$....S<...)..xv.....(d.@..pt"]^.R.(..i.tv...$..j.j....o.j..e..&.`.].?A}.m....`."..i.+....2.....]...,'..R1..[.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-download.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	575
Entropy (8bit):	6.830970971637153
Encrypted:	false
SSDEEP:	12:6v/7X0Z7HBwN1+swFlzkNqwnN14aVOX24G2uXGtIEsltGeBm65Yc:C0BqEZqQQRuXG5saexR
MD5:	576892D2CBC2392CDED574CF9F87E9A3
SHA1:	B7126CA4554CBAD5D3C76D3A4E6F4E62DB669D92
SHA-256:	987E50BDB1019E60084F4BBAFCD4F942FCC7451FE40C82A7CEEB1AF56134634B
SHA-512:	FEB9F46BBC9CD25FB6639E7B8E30BC3F3460A41D098C5CE2350B7B9134F163E7D63694D9F535944043A9B4E82885F714B2B5FC815CE41781EA9D9C4E8098C21
Malicious:	false
Preview:	.PNG.....IHDR.....(-.S....sBIT.....O.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Folder Icons.._.....tEXtAuthor.Lapo Calamandrei..*.. .RtEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb.....PLTE.....~..... .....(.....tRNS.@NS.....nIDAT.W].W..0.E.W.@#...5._ 1.....R....j..{.....c...-....t.D.y..[....g.H....G.t...s.3...lo...khL@..g....B.a.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-drag-accept-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1077
Entropy (8bit):	5.095013943036629
Encrypted:	false
SSDEEP:	24:t4tp46o5VC669yLUDgEyKbRAecFxMGMaM+uRM96Kcm:ea69yL0JNtAecFJMj86K/
MD5:	BDC8C62FEE436EFB83F7D75400F81F31
SHA1:	43DD187F46AD9D03DBE511C86C1F23C92AC66BCD
SHA-256:	2C754284C11A36DCEC407452C15B7DA77D6FA815B6F6F082D2DFB990CE9EFD83
SHA-512:	D3AF73024B8B6657145F0B680A03ED41BE5766D70CE5FFCC0834DB71CA309B522C4C8FD61122A51E9BE3B805CCC4D8CA6A9CD74BA77C5A2464342CE5FBA8165
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16.014" height="16"><g fill="#474747"><path d="M1.014 1a1 1 0 00-1 1v5.832a1 1 0 000 .326V13s-.014.459. 23.947C.49 14.436 1.182 15 2.015 15h1.832a1 1 0 00.326 0h9.842s.459.014.948-.23c.488-.245 1.052-.937 1.052-1.77v-2a1 1 0 00-1-1h-11a1 1 0 00-1 1v2h-1V9h11a1 1 0 001-1V4a1 1 0 00-1-1H8.428L6.721 1.293A1 1 0 006.014 1zm1 2H5.6l1.707 1.707A1 1 0 008.014 5h4v2h-10zm3 9h9v1h-9z" 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="M1.014 10h1s0-1 1-1l10-1V4h-5l-2-2h-5z" fill-rule="evenodd"/><p

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-visiting.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	479
Entropy (8bit):	7.424417664350709
Encrypted:	false
SSDEEP:	12:6v/7MEs8+zTCS6Fm0QqVI8FoWmlsV+qmw8pXAGsaFBbHWe1:KPEb6FmpqVI8Kbqm1Hb2e1

MD5:	74938AFFF1F75F97D08AEB730F2698B7
SHA1:	F370B7705F844460D39489E5D1F2B15FE2F2A441
SHA-256:	A8A2D4FCD192CE5924032EFF47738B7A730A0C4DEED8C7C7E8ECD75932E063D0
SHA-512:	0EF7E50D617D98D03DEF5F405CEBA8E7BDA21683F02C08635F30C204531E3CAAC6D861CCBC214C835952536553FC2E73414AE6E400FF0201A2A5416B74A8E11 5
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx...E..0..u.p..3d.Cd..c..%.#?.z.....0.U...../..o6.%..#2QH...F.L....r..o..vs7...&.....nN9g.. x...k.\(9.GqH....9...0m...`.V..V..J.....(..n.A....: .0.kt.`I...U.%...S...h.n.A&.`Tr.6l.;f.,X..l.9.0q...ck.5a..$.eDfX..^.8.E...8.....%.x\ft....e.....;0*$`.2..t..U..pD..8X....+0;..Y.d.+.#..\M.4...!..*.XJ.ux..R...1.....+2.....J ;...H(..E...#0.. [...Y.....Q...0../.u.o.A..3..,s.Ve.7O.[.....d.....w.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlb en\format-text-bold-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	183
Entropy (8bit):	6.003110793136093
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllTh9zFa7Z52Dkh4FdXeqepOl/7tPAc08XIEh64Za:6v/lhPys9zFwHC1FdXeqe4/5dJYEup
MD5:	F7DA2995933D894BDE84BCBFC78CC767
SHA1:	6B5808CC30A2366D3258F79C6719EB1C5C6FFB37
SHA-256:	EB0C26BA06BBA9D9980D1DDEA031141E5491931B8CAC5221B69FF2593A21F398
SHA-512:	58848192C7DBFFBEB6F3ACC56384089DDE9ADFAE31946AC5F66AA8593AF2A4BE411EEF06E225011B36CB9FA4EB8B3705E4D2404BCBB51C3885D8EB672E011 C6B
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....nIDAT8.c`...?.....\.`..TW.B5...Oa..$.....$.....5c..84....9..?..x...&4..4.1.F.=.z..j.Sr.....TI...}.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlb en\format-text-direction-symbolic-rtl.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1503
Entropy (8bit):	5.15394138748218
Encrypted:	false
SSDEEP:	24:t4CBGMMAhONiWGzFk1wgaqV4AeW0WRjgnRcG1IoAeW0ayyKbRAecFxV0L:gMmklOV4AeIRjacYIoAeQyNtAecFu
MD5:	1C15A6D0FA6065F5004770EA2876B446
SHA1:	BFDB465A2FC2B8BA60FC9BEE5CB03D65156F1D20
SHA-256:	DC5A830CBB258F5B7EB5422C7059F6A0578821D9549A9603CA3C22E4749B6F80
SHA-512:	02309FE57B9CA42D65FA9C4B93FCB6A003D698D0FC47EF03EEFCDA0163B7C715FC6438A3CED7164839EED3412EC40BA1CF35B88AF0A40D7774B93BE7F1879F 6C
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" font-weight="400" fill="#474747"><path d="M6 .05v2h6c.428 0 1 .613 1 1v1H8c-.92 0- 1.735.383-2.25.968A3.017 3.017 0 005 7.049c.006.72.27 1.453.781 2.032.513.578 1.31.968 2.22.968h7v-7a3 3 0 00-3-3zm2 6h5v2H8c-.398 0-.567-.11-.719-.282a1.144 1.144 0 01-.28-.719 1.11 1.11 0 01.25-.718c.144-.166.327-.282.75-.282z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-dec oration-line:none;text-transform:none;marker:none" font-size="xx-small" font-family="Sans" overflow="visible"/><path d="M4 15H3c-.265 0-.53-.093-.719-.281l-2-2L0 12.437v-.874l.281-.282 2-2C2.47 9.093 2.735 9 3 9h1v1c0 .265-.093.53-.281.719L2.438 12l1.28 1.281c.189.188.282.454.282.719v1z" style="line-height:normal;-inks cape-font-specification:'Bitstream Vera Sans';text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" font-family="Bitstream Vera Sans" overflow="visible"/>

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlb en\go-previous-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.455633152585391
Encrypted:	false
SSDEEP:	12:TMHdPnnl/nu3tlnpZo4iL+o0JWlzkmvtoWlz9vtoWlzKzmdwWlzFzmdwWlM:2dPnnxu3tlTtiL+rJPmvto0vtojzmdw6
MD5:	D3329B3FDCE276378BC23A2B04EFF6FA
SHA1:	1DF694D08D03F1C7C86AB6234507A9364EC5C4E8

SHA-256:	0D26FB049E369AAD5E7ED901B3A255317A4A465008E89026FDE9F624124E2599
SHA-512:	2C4624461FAC6CD5093B8B7818DA17B909A302A216364ABCDD467131EA2C49E2BDCA3E546F69030E4812439F86986F747688EA0F9732CAE053F697A8C3F08B0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 11.707031 2.707031 l -1.414062 -1.414062 l -6.707031 6.707031 l 6.707031 6.707031 l 1.414062 -1.414062 l -5.292969 -5.292969 z m 0 0"/>. <path d="m 11 15 h 1 v -1 h -1 z m 0 0"/>. <path d="m 11 2 h 1 v -1 h -1 z m 0 0"/>. <path d="m 11 3 c 0.554688 0 1 -0.445312 1 -1 s -0.445312 -1 -1 -1 s -1 0.445312 -1 1 s 0.445312 1 1 1 z m 0 0"/>. <path d="m 11 15 c 0.554688 0 1 -0.445312 1 -1 s -0.445312 -1 -1 -1 s -1 0.445312 -1 1 s 0.445312 1 1 1 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlb en\idxcaption.xsl

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	exported SGML document, ASCII text
Category:	dropped
Size (bytes):	2055
Entropy (8bit):	5.043971370492221
Encrypted:	false
SSDEEP:	48:iKmpXgIxs4ZL4Y8PsJmbW2KCkwR2+n+PfeWBvQFUijkv:irXvuqL4xJbWrCkwR2++HvBApa
MD5:	36DDA7FDA9AA693064A3E03F9619EABC
SHA1:	23385157B7C151A28582043097325BFE9A383A33
SHA-256:	DF70D7483EB94C2CB50FB27B838041732154D0EA74A3885199376083D103E9E1
SHA-512:	C89708B401E479A983471401E9118B80753E5CAF0B2B70C2D4B492BC0AD6F5BDFF83BD1B0B2592AF12553578535132C81CA944B5932397982EF6F2D8523B60F0
Malicious:	false
Preview:	. * This file is part of the LibreOffice project.. *. * This Source Code Form is subject to the terms of the Mozilla Public. * License, v. 2.0. If a copy of the MPL was not distr ibuted with this. * file, You can obtain one at http://mozilla.org/MPL/2.0/.. *. * This file incorporates work covered by the following license notice:. *. * Licensed to the Apac he Software Foundation (ASF) under one or more. * contributor license agreements. See the NOTICE file distributed. * with this work for additional information regardi ng copyright. * ownership. The ASF licenses this file to you under the Apache. * License, Version 2.0 (the "License"); you may not use this file. * except in compliance with the License. You may obtain a copy of. * the License at http://www.apache.org/licenses/LICENSE-2.0 ..-->.<xsl:stylesheet version="1.0" encoding="UTF-8". xm lns:xsl="http://www.w3.org/1999/XSL/Transform". xmlns:office="http://openoffice.org/2000/office". xmlns:style="http://open

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlb en\media-playback-stop-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.922475588787923
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slZRI/YF2tSKlNK+:TMHdPnnl/nu3i/YF2dlj
MD5:	51515176E0822E6A950F00D9D9D706C7
SHA1:	EAAE28C48278ACD0F21E151D7F0EEF081A0BF1C2
SHA-256:	2E2C14E0596E4025CED6E6AD5E1F4234A5571133D13F21DDBA129EB0E9888D84
SHA-512:	634737D9C8623D7C09A6AC5FD76CA8B2FBB2F1D808DB602F6F86A925F528BC0A0C2C075833881B870C85D34198AE2327A7DAF79256E329C243E9DAC7934C42E A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <path d="m 2 2 h 12 v 12 h -12 z m 0 0" fill="#2e3436"/>.</svg>.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlb en\media-playlist-repeat.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	393
Entropy (8bit):	7.253224688299237
Encrypted:	false
SSDEEP:	6:6v/lhPWjkm5nci9pR622u0WcKb36FQAYmzNPr+j3gh75lW4Y9LJkPSGzaujp:6v/7ykGP/R622uJQYmzNc3stULgSGz3
MD5:	159F75D26486E9FEEDA93F57380803D0
SHA1:	9CFCDF5399F93583658FABD4831BE1A77594B05D
SHA-256:	5E00C886D17CD45CF0B98961D9B3B8D74724F71FEB5B4B8B257903F991340289
SHA-512:	477FC795A7C786EF4BF52636776A5DE983126F5E85907FB3B17E451E7E76CC3FBEF2F9A585012DDDAC74F43B0D3F0FB24A66D21E330E6725A440FB7DFE68BFA 7

Malicious:	false
Preview:	.PNG.....IHDR.....a...PIDATx...r.1...J.K.m.mwX.n..6.....x...../...hii..F....0...S#...c....-....-..@"..`..n..l.Za..a2.a4....P....!....n.^.ad|...ylb.....=.;B{.N..@.[g&.N.%.....{.[..-.i.(T.....s.....J+..=.\P\^`.....R.....t..% #3..ss3..RAa..+(.R.@ZF.. 6!.56.bsg..$2:.O..%.Ul6.T*...._.u....^BXD...._...C...bc#nw.....}.....K..w...`.8.~...._.dS.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\mmapwarm.c

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	3303
Entropy (8bit):	5.0267368816625755
Encrypted:	false
SSDEEP:	96:mJC/HOLCKr1SGSU7RD5y/ArM1dE912magaMz8l4XL:mSOLCeSGS23y/ArwdE912AaMz8mXL
MD5:	EEF073B3246F0DFEB5DFCA21FC26E751
SHA1:	619609A2D26F70F5FD48B3AA8CFA70D5D3766C33
SHA-256:	8F65C71523910F166045BF312572139EE37E205D004EC7DAD18F9927DDF93242
SHA-512:	B2D9531BFF572CC87858E95FEB6AC1BF975014E3100BB5C94D3DCD47F32F17BE4AB1ECF676F0D6B912B26EC71C4482D95805FE3B0D72367F6BA3B2C83DD5D 3D
Malicious:	false
Preview:	/*.** 2017-09-18.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.********** **********.**.*/..#include "sqlite3.h".../*.** This function is used to touch each page of a mapping of a memory.** mapped SQLite database. Assuming that the system has sufficient free.** memory and supports sufficiently large mappings, this causes the OS .** to cache the entire database in main memory, making subsequent .** database accesses faster..**.** If the second parameter to this function is not NULL, it is the name of.** the specific database to operate on (i.e. "main" or the name of an.** attached database)..**.** SQLITE_OK is returned if successful, or an SQLite error code otherwise..** It is not considered an error if the f

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Isdkkede\Charterrejsens\phone-apple-iphone-symbolic.svg

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	247
Entropy (8bit):	4.812199066635378
Encrypted:	false
SSDEEP:	6:tI9mc4slzcWER4LtmRRRHczezSms2uP2/v2dz15OfF37G+Kb0/:t4CDqLE8iuaTH2S9A0/
MD5:	012B484EB1808137F586C2FB7AA4BA8B
SHA1:	2C806A12C553CF553FBCFEE0A838EF471E0C3C71
SHA-256:	8B7E4A5DFE6BE00896C2DFA8F4B0D8FA518AD6D14863FAED6F78F8A5F3CEE227
SHA-512:	4D34C17973FAEF9765B26AB7029594FBC8841297369A6BEEFBB500D699C0FCA0697EC843351F63E83A6868380117805DC9523E45BB1318D446BD18941DF6BD6A
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M5.469 1C4.648 1 4 1.648 4 2.469V13.53c0 .822.648 1.47 1.469 1.47h5.125c.82 0 1.469-.648 1.469-1.469V2.47c0-.821-.648-1.469-1.47-1.469zM5 2h6.063v11H5z" fill="#474747"/></svg>

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\preferences-desktop-theme.png

Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	768
Entropy (8bit):	7.659464891968236
Encrypted:	false
SSDEEP:	12:6v/7Eu8VOALuh4OxDgp/mAH70oNchloqoO2NwGqEtuDCwjhNSZnNDqffLmVkLCn2:W8VOALuhM/m2yhI1oOGFtuFjMNOEkLC2
MD5:	22BCEE5BDAEA3CE17736D209364FA9EB
SHA1:	E55FBBE241AED99FBBD4C400DCA8F2A4DBA60484
SHA-256:	9ACE40195DF0349BCE92B4C66360AD490F2BD6DD8A20286F329894311E881E58
SHA-512:	20968CEABB5094E350A232FFF9D017C07C1DA986A1371B4561E2CC4BAE5AC631A7FF7EDC53CAB0E9E7E55FF626FF4C4CD071334AECCB306B4B0ED31166A26 FDD
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.}.S.dW..w.....n.\c.h.].u.v...=m.M..O..Yk.3..izmu.._.7.....nb. ...Y.B+.....a.j}/t&..;...;....u..X.....4....JQ....S.y....v\....i.b...E..@m#.U.q.7.`.Z...w0..sT.\..@....}p...9K.U..y.Z.+.aN.....)/,..{....HHS[.F.....0g. :D..y.....ArZ.X\9m...\u....F..@v^....ce~.zy..Q...@y\.....k.....R\.$..8t...S...\x.aa.(..E..bXZMx...twD".G$.(.....$4.9 ".....p}q.T :..!..D]..... SJ&s.3.$-3y.....@.x"9...}<...Im...>I72..&._8s..._....%)..t..{ .....P.Q...P.GTL8.$..ToHph....N.....@ks3.....i2.dQx..!3....K.Rk[...J...r...kGn....pc..7....qu8..g.....+.(.,..i...._ ...{PXT...C.w,^.z.s.F..@Br,....epH .N;...W....|.b..H.T}8.[...m.R^...f.N.>..n...<.....u..[7b..w..|<V.....!..c.....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\text-x-generic.png	
Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	535
Entropy (8bit):	6.729117073271159
Encrypted:	false
SSDEEP:	12:6v/7X0ZKjCVdCyzM8OYSdMA4jT7MzhgkX9Ba0u9:C0oCHMU5AmT7i29
MD5:	FB3685DADAC64A7FF12E32A42A21C63A
SHA1:	81C46DFAB337E1AB02130316299A23C561472EE5
SHA-256:	99E5ADC5223AF5CDBB7BC70DA279DC9361AF8D130999F25DF7619AE8AFE546FF
SHA-512:	5DD0698358DDDC16E24E5719E893BDB35E2B45AF7096709190B60DA0408AF708FD66D7E0BB7D710A327168281658E6B11E391B53A5C45644A482AE7CB1F2C65
Malicious:	false
Preview:	.PNG.....IHDR.....(-.S....sBIT.....O.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtAuthor.Jakub Steiner.../....tEXtDescription.mimetypes7..d...!tEXtSource.http://jimmac.musichall.czif.^....PLTE.....tRNS.....RSYs.....=^....jIDAT..... .D.....ce....U.c]d...7.Q@..k$.0..t.H.fcz...7.8BSl.....*.....V...7|/.~~..,H.a...L!...'....JD..bF....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\user-offline.png	
Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	589
Entropy (8bit):	7.569592468279548
Encrypted:	false
SSDEEP:	12:6v/773gFN49te3X6GMop9P9sbgLVeMCJtgrsjztvVnSPKa0q:auQU7p9P9F8MCXg8tdntq
MD5:	B284550BD073CA666718742CFB1FEF48
SHA1:	D4DB8DB0D76A3CCB04343C6304EB171014180960
SHA-256:	0C53C237C34B3AF57C8D4613A95C32E6E7932D99444FB2B573233C16151B70F6
SHA-512:	F26A3D6D80D6983D0E26101ABDC90691D9FE9C24874BB67A0748E9120F7AE6C651F62C2E025A038FB497DA8C1558BF1E2D803BA9FDFAF9B69D82DE5D2F25D67
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.....Q..._.2S.U...l...b....m.m.....X[.=v..;3.....^>?.....\.|n..g.j.Z!._>3..... .%. ..a....%..s..A*,-.s.N.....P.~R.~...q...zw.ZU.....[..;7'..m.....Q.sn..}.;\..3*X.v9....$/_..n.-gH..:..Mk.).....FK..p....Ks..3...T.3r.d."e...8.N.Ai..Jk.<.....?.....T\....,4c..`.....o.H...2.....w.KU*."..&.S.VkK..oT}[XO...x).R.g.....a#.D.Fs..r.....)#;q..E.z.~...../H<.b.."...5.....S.....&.^1YL.as../.R-K^...}r.n.N.....@.....v:.n.K.o.)K....xNB.'233..L.A...R2..8...HJJjf0...Yi$.h.....F....~.....]...].....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\view-wrapped-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\dlawt.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	208
Entropy (8bit):	6.421066289233811
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllUxz3kooRKoNUOGIFVHR70DsyLkdFJfQWulhSzW/:6v/lhPysMfZIvHt0DHkTJfylh+fHqp
MD5:	05163D4844014A964497BFC51FCF417E
SHA1:	FFAF4C7AFE0299467846B874992D634FBD4FA437
SHA-256:	3EDEACF6ED0DD60A70B4D7ED1C4505932785F2E008D2FB5F0B53FB71C122676C
SHA-512:	43C7E5CBE38B6CA36387A0C11BA07082AB950B086379538101F741A292A18A528E7BE089DAC70A1CE0C78B3D59F85774546D357F3A7B3FF11DFDE43CE4EC939D
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..... .E_<...Ud@..'/N k.$....'?..}m..Z`..pE>.+9.....!f.IT.....n.}..i...o...`...0..B.Z....bU9@.._(.89.W.E_."...+]....4.>(.....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.702939705302498

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:	dlawt.exe
File size:	282224
MD5:	cf313a27bceba36c7fa863ba1e935676
SHA1:	4ff90062880efe58e6e26ded7f166c5786e201db
SHA256:	d4fba0fc4c7c1335a5b6be72e575a2a9a400a5fd9b0aed69389d4bba8fac7527
SHA512:	2f3608b90bbec011c4b5e659029166c3b8a2c7dccd30f7ca9da00897beef920060c9767e971010997b8edd2a0196e8d7acef8f048be0e1845d29dfc948c81f63
SSDEEP:	6144:ORlWobsEnfENQ+8m9+ubxlL5Y9CwTfFQ9:+X8NQ+8m9+ubxmRW9
TLSH:	6854D003FB8CC85BCD2509301272EA7996B5EEB41EB54B037E5D763EAC7B2428D1A315
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....oZ.....d...*.....

File Icon

Icon Hash:	f2e1e1e1e29ce439

Static PE Info

General

Entrypoint:	0x403359
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:	0x5A6FED2E [Tue Jan 30 03:57:34 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:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	OU="Flyvecertifikats Marantic ", E=Gennemgaar@Ethylamime96.Ch, O=ballelssere, L=Angers, S=Pays de la Loire, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/5/2021 4:11:48 PM 11/4/2024 3:11:48 PM
Subject Chain	• OU="Flyvecertifikats Marantic ", E=Gennemgaar@Ethylamime96.Ch, O=ballelssere, L=Angers, S=Pays de la Loire, C=FR
Version:	3
Thumbprint MD5:	2F2B34B547CC3D81835478C9667E4758
Thumbprint SHA-1:	C5566AA56BE27344FAE7A4A69F9E003360E7BF45
Thumbprint SHA-256:	E5781D4CFF5055733247474BECD116042294D0C169F0F5470CD1C7467C0C12F4
Serial:	3772290E2FB31093

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi

Instruction
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042A20Ch], eax
je 00007FF7ED143713h
push ebx
call 00007FF7ED1469C5h
cmp eax, ebx
je 00007FF7ED143709h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FF7ED14693Fh
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FF7ED1436ECh
push 0000000Ah
call 00007FF7ED146998h
push 00000008h
call 00007FF7ED146991h
push 00000006h
mov dword ptr [0042A204h], eax
call 00007FF7ED146985h
cmp eax, ebx
je 00007FF7ED143711h
push 0000001Eh
call eax
test eax, eax
je 00007FF7ED143709h
or byte ptr [0042A20Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [0042A2D8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216A8h
call dword ptr [00408188h]
push 0040A2C8h

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x59000	0x284b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x43028	0x1e48	.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	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x62a5	0x6400	False	0.658984375	data	6.431390019180314	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20318	0x600	False	0.4928385416666667	data	3.90464114821524	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x2e000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x59000	0x284b8	0x28600	False	0.46781274187306504	data	5.678738189394348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x59388	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x69bb0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x73058	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x784e0	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x7c708	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x7ecb0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x7fd58	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x806e0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x80b48	0xb8	data	English	United States
RT_DIALOG	0x80c00	0x100	data	English	United States
RT_DIALOG	0x80d00	0x11c	data	English	United States
RT_DIALOG	0x80e20	0xc4	data	English	United States
RT_DIALOG	0x80ee8	0x60	data	English	United States
RT_GROUP_ICON	0x80f48	0x76	data	English	United States
RT_VERSION	0x80fc0	0x1b4	data	English	United States
RT_MANIFEST	0x81178	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

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

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: dlawt.exe PID: **4772**, Parent PID: **5632**

General	
Target ID:	0
Start time:	07:23:00
Start date:	28/09/2022
Path:	C:\Users\user\Desktop\dlawt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dlawt.exe"
Imagebase:	0x400000

File size:	282224 bytes
MD5 hash:	CF313A27BCEBA36C7FA863BA1E935676
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: 00000000.00000002.764563797.0000000003208000.00000040.00000800.00020000.00000000.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	405844	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsk8C3A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DE8	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	7	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer\Lakridset.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer\CoverEdCtrl.manifest	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen\audio-x-generic-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen\changes-prevent-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\dialog-information-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\drive-harddisk-solidstate-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-download.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-drag-accept-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-visiting.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\format-text-bold-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\format-text-direction-symbolic-rtl.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\go-previous-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\idxcaption.xsl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\media-playback-stop-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\media-playlist-repeat.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\mmapwarm.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Algae62	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Algae62\plkkers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Algae62\plkkers\Reputation	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Algae62\plkkers\Reputation\network-cellular-4g-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Bacin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Bacin\Besjlings	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Bacin\Besjlings\network-wireless-connected-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Isdkkede	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Isdkkede\Charterrejsens	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405844	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Isdkkede\Charterrejsens\phone-apple-iphone-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\preferences-desktop-theme.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\text-x-generic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\user-offline.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\view-wrapped-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Local\Temp\nsq995B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DE8	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405844	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405844	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405844	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405844	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405844	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsq995B.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	405804	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq995B.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA6	CreateFileW
C:\Users\user\AppData\Local\Temp\nsq995B.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	405DA6	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsk8C3A.tmp	success or wait	1	403608	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsq995B.tmp	success or wait	1	4059C5	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer\Lakridset.bmp	0	24893	42 4d fd 50 01 00 00 00 00 00 36 00 00 00 28 00 00 00 48 00 00 00 fd 01 00 00 01 00 18 00 00 00 00 00 fd 50 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 61 7c fd 2c 6c fd fd 2e 40 fd fd 59 fd 5c 30 fd 6f fd 03 dc fd 0f 08 1f 0a 34 70 49 fd 0b 29 07 fd 32 6c 4d 6d 2e fd 38 34 25 3c fd 05 d6 fd fd fd fd 1d 70 fd 5b 18 0b 2b fd 27 21 3f fd 13 2a 37 fd fd b8 20 64 4f fd 43 09 fd 1c fd fd fd fd 33 fd 51 fd 4b fd 4c fd da 05 fd 82 08 71 63 14 4a fd 7a fd fd fd fd 61 4d 4a 26 12 41 fd 7b 19 fd fd 51 61 fd fd fd 49 74 4d fd 75 fd 4e fd fd fd d7 50 5b fd 1d fd 35 77 68 fd 7b fd 79 fd 29 3e fd fd fd 85 26 43 fd fd 4b 5d fd fd 03 4d 6f fd 74 14 32 fd fd 02 fd 5a 05 fd 1e 24 7d fd 3a 2b	BMP6(HPa|.I.@Y\0o4pI)2IMm.84%<p+'!?*7 dOC3QKqcJzaMJ&A{QaltMu NP[5wh{y)>&CK]Mot2Z$}:+	success or wait	4	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Arbejdskraftproblemer\CoverEdCtrl.manifest	0	983	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 31 22 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 6e 61 6d 65 3d 22 43 6f 76 65 72 45 64 43 74 72 6c 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 34 2e 30 2e 30 22 3e 3c 2f 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 3e 3c 66 69 6c 65 20 6e 61 6d 65 3d 22 43 6f 76 65 72 45 64 43 74 72 6c 2e 6f 63 78 22 20 68 61 73 68 61 6c 67 3d 22 53 48 41 31 22 3e 3c 63 6f 6d	<?xml version="1.0" encoding="UTF-8" standalone="yes"?> <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"> <assemblyIdentity name="CoverEdCtrl" version="1.4.0.0"> </assemblyIdentity><file name="CoverEdCtrl.ocx" hashalg="SHA1"><com	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen\audio-x-generic-symbolic.symbolic.png	0	195	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 7a 49 44 41 54 38 fd fd fd fd 0a fd 30 0c fd fd f1 57 13 74 fd fd fd 1e 04 4f 3e fd fd fd fd fd 41 0f 65 74 fd 50 fd 40 28 fd 4f fd 26 fd 32 36 2b fd fd fd fd 4d 6d 07 42 36 fd fd fd 1f fd 67 fd 1e 27 4c fd 66 fd fd fd 52 72 59 9d fd fd fd fd fd fd 47 09 6f 70 ef fd fd 73 46 fd 16 fd fd 3e 63 1f fd 2e fd 75 18 30 fd fd d4 0f fd fd 3e 5e 6e 79 44 3b 41 1f d0 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dzIDAT80WtO>AetP@(O&26+Mm6g'LfRrYGopsF>c.u0>^nyD;AIENDB`	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Baggesen\changes-prevent-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 37 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 56 38 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 31 73 2d 2e 37 30 39 2d 2e	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#bebebe" fill="#474747"><path d="M3 7h10c.554 0 1 .446 1 1v3c0 .554-.446 1-1 1H3c-.554 0-1-.446-1-1V8c0-.554.446-1 1-1z" style="marker:none" overflow="visible"/><path d="M7 1s-.709-.	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\dialog-information-symbolic.svg	0	1626	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 32 65 33 34 33 36 22 3e 3c 70 61 74 68 20 64 3d 22 4d 37 2e 39 39 34 20 30 61 36 2e 30 31 20 36 2e 30 31 20 30 20 30 30 2d 35 2e 38 37 20 34 2e 37 37 37 63 2d 2e 35 32 38 20 32 2e 35 33 33 2e 36 39 20 35 2e 30 33 36 20 32 2e 38 37 34 20 36 2e 33 32 37 6c 2e 30 30 32 2e 38 39 38 41 31 20 31 20 30 20 30 30 36 20 31 33 68 34 61 31 20 31 20 30 20 30 30 31 2d 2e 39 39 38 6c 2e 30 30 32 2d 2e 39 63 32 2e 31 38 33 2d 31 2e 32 39 33 20 33 2e 33 39 39 2d 33 2e 37 39 37 20 32 2e 38 37 2d 36 2e 33 33 41 36 2e 30 31 20 36 2e 30 31 20 30 20 30 30 37 2e	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#2e3436"><path d="M7.994 0a6.01 6.01 0 00-5.87 4.777c-.528 2.533.69 5.036 2.874 6.327l.002.898A1 1 0 006 13h4a1 1 0 001-.998l.002-.9c2.183-1.293 3.399-3.797 2.87-6.33A6.01 6.01 0 007.	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytrypta mine\Forlben\drive-harddisk-solidstate-symbolic.symbolic.png	0	195	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 7a 49 44 41 54 38 fd fd 41 0e fd 20 0c 04 47 13 7e 24 fd fd 0d fd 53 3c fd 07 fd 29 15 fd 78 76 fd fd 01 fd fd 1e 28 64 fd 40 04 12 70 74 22 5d 5e fd 52 1c 28 fd fd 69 fd 74 76 fd fd fd 24 fd fd 6a fd 6a fd fd cd 2e 6f 45 6a fd fd 65 fd fd 26 fd 60 fd 5d fd 3f 41 7d 02 6d fd fd fd 16 60 18 22 00 19 69 fd 2b fd 1a fd fd 32 05 0d fd fd fd 1a 5d fd 00 2c 00 27 fd 07 52 31 fd fd 5b fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dzIDAT8A G~$S<)xv (d@pt"]^R(itv$jj.oje&`]?A}m`"i+2],'R1[IENDB`	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytrypta mine\Forlben\folder-download.png	0	575	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 1a 74 45 58 74 54 69 74 6c 65 00 41 64 77 61 69 74 61 20 46 6f 6c 64 65 72 20 49 63 6f 6e 73 fd 07 5f fd 00 00 00 17 74 45 58 74 41 75 74 68 6f 72 00 4c 61 70 6f 20 43 61 6c 61 6d 61 6e 64 72 65 69 d1 1a 2a 00 00 00 52 74 45 58 74 43 6f 70 79 72 69 67 68 74 00 43 43 20 41 74 74 72 69 62 75 74 69 6f 6e 2d 53 68 61 72 65 41 6c 69 6b 65 20 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6c 69 63 65 6e	PNGIHDR(-SsBITOpHYs+tEXtSoftwa rewww.inkscape.org<tEXtTitleAdwaita Folder Icons_tEXtAuthorLapo Calamandrei*RtEXtCopyrightCC Attribution-ShareAlike http ://creativecommons.org/licen	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytrypta mine\Forlben\folder-drag-accept-symbolic.svg	0	1077	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 2e 30 31 34 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 31 2e 30 31 34 20 31 61 31 20 31 20 30 20 30 30 2d 31 20 31 76 35 2e 38 33 32 61 31 20 31 20 30 20 30 30 30 20 2e 33 32 36 56 31 33 73 2d 2e 30 31 34 2e 34 35 39 2e 32 33 2e 39 34 37 43 2e 34 39 20 31 34 2e 34 33 36 20 31 2e 31 38 32 20 31 35 20 32 2e 30 31 35 20 31 35 68 31 2e 38 33 32 61 31 20 31 20 30 20 30 30 2e 33 32 36 20 30 68 39 2e 38 34 32 73 2e 34 35 39 2e 30 31 34 2e 39 34 38 2d 2e 32 33 63 2e 34 38 38 2d 2e 32 34 35 20 31 2e 30 35 32 2d 2e 39 33 37 20 31 2e 30 35	<svg xmlns="http://www.w3.org/2000/svg" width="16.014" height="16"><g fill="#474747"><path d="M1.014 1a1 1 0 00-1 1v5.832a1 1 0 000 .326V13s-.014.459.23.947C.49 14.436 1.18215 2.015 15h1.832a1 1 0 00.326 0h9.842s.459.014.948-.23c.488-.245 1.052-.9371.05	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\folder-visiting.png	0	479	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 45 fd fd 30 10 fd 75 fd 70 0e fd 33 64 fd 43 64 fd fd 63 fd fd 25 fd 23 3f fd 7a fd fd fd 0e 17 fd fd fd 30 fd 55 fd fd fd fd fd fd 2f fd fd 6f 36 fd 25 fd fd 23 32 51 48 fd fd fd 46 fd 4c fd fd fd fd 72 fd fd 6f 13 fd 76 73 37 fd fd fd 26 11 fd fd fd fd 26 fd 6e 4e 39 67 1f fd 20 78 fd fd 04 6b 1f 5c 28 39 04 47 71 48 fd fd fd 9b 39 fd fd 05 30 6d 02 fd 46 60 fd 56 fd 19 56 fd fd 4a 1f fd fd ea fd 28 09 fd 6e fd 41 fd fd 1a fd 3a fd 30 00 6b 74 fd 60 6c 0b 0d 18 55 fd 25 fd a0 fd 53 02 fd fd 68 a7 6e fd 41 26 fd 60 54 72 04 36 6c fd 3b 66 fd 2c 58 7f 21 6c 12 39 fd 30 71 16 fd fd 63 6b 11	PNGIHDRaIDATxE0up3dCdc%#?z0U/o 6%#2QHFLrovs7&nN9gxk\(9GqH90m `VVJ(nA:0kt`lU%ShnA&` Tr6l;f,Xl90qck	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\format-text-bold-symbolic.symbolic.png	0	183	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 6e 49 44 41 54 38 fd 63 60 18 fd fd 3f 1e fd fd fd fd fd fd fd fd fd 5c 03 60 fd fd 54 57 05 42 35 fd fd fd 4f 61 12 fd 24 18 fd 1f fd fd fd fd fd fd fd fd 24 fd fd fd fd fd fd fd fd 0c fd fd fd 35 63 05 fd 38 34 fd fd 18 fd 39 03 fd 3f fd fd 78 01 fd 00 26 34 05 fd 34 0b 31 fd 46 06 3d fd 7a fd 1d 6a fd 53 72 0d 18 fd 00 00 fd 54 49 0a fd fd 7d fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dnIDAT8c`?\`TWB5Oa$$5c849?x&441F=zjSrTI}IENDB`	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\format-text-direction-symbolic-rtl.svg	0	1503	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 6f 6e 74 2d 77 65 69 67 68 74 3d 22 34 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 36 20 2e 30 35 76 32 68 36 63 2e 34 32 38 20 30 20 31 20 2e 36 31 33 20 31 20 31 76 31 48 38 63 2d 2e 39 32 20 30 2d 31 2e 37 33 35 2e 33 38 33 2d 32 2e 32 35 2e 39 36 38 41 33 2e 30 31 37 20 33 2e 30 31 37 20 30 20 30 30 35 20 37 2e 30 34 39 63 2e 30 30 36 2e 37 32 2e 32 37 20 31 2e 34 35 33 2e 37 38 31 20 32 2e 30 33 32 2e 35 31 33 2e 35 37 38 20 31 2e 33 31 2e 39 36 38 20 32 2e 32 32 2e 39 36	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" font-weight="400" fill="#474747"><path d="M6 .05v2h6c.428 0 1 .613 1 1v1H8c-.92 0-1.735.383-2.25.968A3.017 3.017 0 005 7.049c.006.72.271.453.781 2.032.513.578 1.31.968 2.22.96	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\go-previous-symbolic.svg	0	665	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 31 31 2e 37 30 37 30 33 31 20 32 2e 37 30 37 30 33 31 20 6c 20 2d 31 2e 34 31 34 30 36 32 20 2d 31 2e 34 31 34 30 36 32 20 6c 20 2d 36 2e 37 30 37 30 33 31 20 36 2e 37 30 37 30 33 31 20 6c 20 36 2e 37 30 37 30 33 31 20 36 2e 37 30 37 30 33 31 20 6c 20 31 2e	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <g fill="#2e3436"> <path d="m 11.707031 2.707031 l -1.414062 -1.414062 l -6.707031 6.707031 l 6.707031 6.707031 l 1.	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\idxcaption.xsl	0	2055	3c 21 2d 2d 0a 20 2a 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 70 61 72 74 20 6f 66 20 74 68 65 20 4c 69 62 72 65 4f 66 66 69 63 65 20 70 72 6f 6a 65 63 74 2e 0a 20 2a 0a 20 2a 20 54 68 69 73 20 53 6f 75 72 63 65 20 43 6f 64 65 20 46 6f 72 6d 20 69 73 20 73 75 62 6a 65 63 74 20 74 6f 20 74 68 65 20 74 65 72 6d 73 20 6f 66 20 74 68 65 20 4d 6f 7a 69 6c 6c 61 20 50 75 62 6c 69 63 0a 20 2a 20 4c 69 63 65 6e 73 65 2c 20 76 2e 20 32 2e 30 2e 20 49 66 20 61 20 63 6f 70 79 20 6f 66 20 74 68 65 20 4d 50 4c 20 77 61 73 20 6e 6f 74 20 64 69 73 74 72 69 62 75 74 65 64 20 77 69 74 68 20 74 68 69 73 0a 20 2a 20 66 69 6c 65 2c 20 59 6f 75 20 63 61 6e 20 6f 62 74 61 69 6e 20 6f 6e 65 20 61 74 20 68 74 74 70 3a 2f 2f 6d 6f 7a 69 6c 6c 61 2e 6f 72 67 2f 4d 50 4c 2f 32 2e	* This file is part of the LibreOffice project. * * This Source Code Form is subject to the terms of the Mozilla Public * License, v. 2.0. If a copy of the MPL was not distributed with this * file, You can obtain one at http://mozilla.org/MPL/2.	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\media-playback-stop-symbolic.svg	0	195	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 0a 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 32 20 32 20 68 20 31 32 20 76 20 31 32 20 68 20 2d 31 32 20 7a 20 6d 20 30 20 30 22 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 2f 3e 0a 3c 2f 73 76 67 3e 0a	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <path d="m 2 2 h 12 v 12 h -12 z m 0 0" fill="#2e3436"/> </svg>	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\media-playlist-repeat.png	0	393	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 50 49 44 41 54 78 01 53 fd 72 fd 31 14 fd fd 4a fd 4b 76 6d f6 6d 77 58 fd 6e fd fd 36 fd fd fd fd fd fd 78 fd 0b fd 13 fd 2f fd 7f 02 68 69 69 11 fd 46 fd fd fd fd 30 fd fd 13 53 23 fd fd 1b 63 13 13 13 fd 2d fd 7f fd fd 2d fd 2e 40 22 13 fd 60 fd fd 6e fd fd 6c fd 5a 61 fd fd 61 32 19 61 34 1a fd fd fd 50 b1 fd fd fd 21 fd fd fd fd 6e fd 5e 1c 61 64 7c 00 0e 2b 79 6c 62 08 0a fd 1c 03 fd 3d fd 3b 42 7b 03 4e fd 0f 40 fd 5b 67 26 fd 4e fd 25 fd 1d fd fd fd 14 7b fd 5b fd fd 2d 00 69 fd 28 54 fd 02 fd 0a fd fd 73 fd 01 fd 1f 1b 4a 2b 0b fd 3d fd 5c 50 5c 5e 60 fd fd 1a 0c 06 fd fd 01 52 fd 13 fd fd fd fd fd 74 fd fd 25 20 23 33	PNGIHDRaPIDATxr1JK mmwXn6x/hiiF0S#c--.@"`nlZaa2a4P!n^ad|ylb=;B{N@[g&N%{[-i(TsJ+=\P\^`Rt% #3	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Buyback\preguiltiness\Hydroxytryptamine\Forlben\mmapwarm.c	0	3303	2f 2a 0a 2a 2a 20 32 30 31 37 2d 30 39 2d 31 38 0a 2a 2a 0a 2a 2a 20 54 68 65 20 61 75 74 68 6f 72 20 64 69 73 63 6c 61 69 6d 73 20 63 6f 70 79 72 69 67 68 74 20 74 6f 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65 2e 20 20 49 6e 20 70 6c 61 63 65 20 6f 66 0a 2a 2a 20 61 20 6c 65 67 61 6c 20 6e 6f 74 69 63 65 2c 20 68 65 72 65 20 69 73 20 61 20 62 6c 65 73 73 69 6e 67 3a 0a 2a 2a 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 64 6f 20 67 6f 6f 64 20 61 6e 64 20 6e 6f 74 20 65 76 69 6c 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 66 69 6e 64 20 66 6f 72 67 69 76 65 6e 65 73 73 20 66 6f 72 20 79 6f 75 72 73 65 6c 66 20 61 6e 64 20 66 6f 72 67 69 76 65 20 6f 74 68 65 72 73 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 73 68 61 72 65 20 66 72 65 65 6c	/*** 2017-09-18**** The author disclaims copyright to this source code. In place of** a l egal notice, here is a blessing:**** May you do good and not evil.** May you find forgiveness for yourself and forgive others.** May you shar e freel	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Algae62\plkkers\Reputation\network-cellular-4g-symbolic.svg	0	544	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 2e 30 36 33 20 30 41 32 2e 30 34 38 20 32 2e 30 34 38 20 30 20 30 30 30 20 32 2e 30 36 33 76 31 31 2e 38 37 34 43 30 20 31 35 2e 30 38 38 2e 39 31 32 20 31 36 20 32 2e 30 36 33 20 31 36 68 31 31 2e 38 37 34 41 32 2e 30 34 38 20 32 2e 30 34 38 20 30 20 30 30 31 36 20 31 33 2e 39 33 37 56 32 2e 30 36 33 41 32 2e 30 34 38 20 32 2e 30 34 38 20 30 20 30 30 31 33 2e 39 33 37 20 30 7a 4d 32 20 33 68 32 76 34 68 31 56 33 68 32 76 31 30 48 35 56 39 48 34 63 2d 31 20 30 2d 32 2d 2e 38 34 32 2d 32 2d 32 7a 6d 38 20 30 68 32 63 2e 38 33 33 20 30 20	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2.063 0A2.048 2.048 0 000 2.063v11.874C0 15.088 .912 16 2.063 16h11.874A2.048 2.048 0 0016 13.937V2.063A2.048 2.048 0 0013.937 0zM2 3h2v4h1V3h2v10H5V9H4c-1 0-2-.842-2-2zm8 0h2c.833 0	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\Bacin\Besjlings\network-wireless-connected-symbolic.svg	0	1364	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 64 65 66 73 3e 3c 63 6c 69 70 50 61 74 68 20 69 64 3d 22 61 22 3e 3c 70 61 74 68 20 64 3d 22 4d 2d 37 33 2d 33 30 6c 2d 37 2d 37 76 2d 34 2e 35 68 31 36 2e 35 76 34 2e 35 6c 2d 37 2e 35 20 37 7a 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 20 73 74 72 6f 6b 65 3d 22 23 30 30 30 22 2f 3e 3c 2f 63 6c 69 70 50 61 74 68 3e 3c 2f 64 65 66 73 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 63 6c 69 70 2d 70 61 74 68 3d 22 75 72 6c 28 23 61 29 22 20 64 3d 22 4d 2d 37 32 2d 33 38 76 31 68 31 76 2d 2e 39 36 39 41 31 32 2e 31 33 20 31 32 2e 31 33 20 30 20	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><defs><clipPath id="a"><path d="M-73-30l-7-7v-4.5h16.5v4.5l-7.5 7z" fill="none" stroke="#000"/></clipPath></defs><g fill="#474747"><path clip-path="url(#a)" d="M-72-38v1h1v-.969A12.13 12.13 0	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\lsdkkede\Charterrejsens\phone-apple-iphone-symbolic.svg	0	247	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 35 2e 34 36 39 20 31 43 34 2e 36 34 38 20 31 20 34 20 31 2e 36 34 38 20 34 20 32 2e 34 36 39 56 31 33 2e 35 33 63 30 20 2e 38 32 32 2e 36 34 38 20 31 2e 34 37 20 31 2e 34 36 39 20 31 2e 34 37 68 35 2e 31 32 35 63 2e 38 32 20 30 20 31 2e 34 36 39 2d 2e 36 34 38 20 31 2e 34 36 39 2d 31 2e 34 36 39 56 32 2e 34 37 63 30 2d 2e 38 32 31 2d 2e 36 34 38 2d 31 2e 34 36 39 2d 31 2e 34 37 2d 31 2e 34 36 39 7a 4d 35 20 32 68 36 2e 30 36 33 76 31 31 48 35 7a 22 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 2f 3e 3c 2f 73 76 67 3e	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M5.469 1C4.648 1 4 1.648 4 2.469V13.53c0 .822.648 1.47 1.469 1.47h5.125c.82 0 1.469-.648 1.469-1.469V2.47c0-.821-.648-1.469-1.47-1.469zM5 2h6.063v11H5z" fill="#474747"/></svg>	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\preferences-desktop-theme.png	0	768	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 fd 49 44 41 54 78 01 7d fd 53 fd 64 57 18 fd 77 fd 7f fd fd fd fd fd fd 6e fd 5c 63 fd 68 f6 5d fd 75 fd 76 fd fd fd 3d 6d fd 4d fd 13 4f fd fd 59 6b fd 33 fd fd 69 7a 6d 75 1a fd 5f fd 37 fd fd fd fd fd 6e 62 fd 20 fd 08 00 59 09 42 2b fd fd fd fd 18 fd 61 fd 6a 7d 2f 74 26 fd fd 3b fd fd fd 3b fd fd 2e fd 75 fd 1a 58 18 0e fd fd fd fd 34 39 fd fd 19 4a 51 fd fd fd fd 53 fd 79 fd 0a 06 fd 76 5c fd fd fd fd 69 fd 62 fd 01 fd 45 fd fd 40 6d 23 05 55 fd 71 fd 37 fd 60 fd 5a fd fd fd 77 30 fd fd 73 54 fd 5c fd fd 40 fd fd fd 09 7d 70 fd fd fd 39 4b 15 55 fa fd 79 fd 5a fd 2b fd 61 4e 1d 00 fd fd fd 2c 29 2f 2c fd 1a 7b 0d 0e fd fd	PNGIHDRaIDATx}SdWwn\ch]uv=mMOY k3izmu_7nb YB+aj}/t&;;.uX4JQSy v\ibE@m#Uq7`Zw0sT\@}p9KUyZ+aN,)/,{	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\text-x-generic.png	0	535	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 fd fd	PNGIHDR(-SsBITOpHYs+tEXtSoftwarewww.inkscape.org<tEXtAuthorJakub Steiner/tEXtDescriptionmimetypes7d!tEXtSourcehttp://jimmac.musichall.czif^PLTE	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\user-offline.png	0	589	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 14 49 44 41 54 78 01 fd fd 03 fd 1c 51 10 fd 5f fd 32 53 fd 55 95 fd fd 6c fd fd fd 62 fd fd fd 36 6d f6 6d fd f5 fd fd fd 58 5b fd 3d 76 7f fd 3b 33 fd fd 53 1d 2e 5e 3e 3f fd fd fd fd fd 5c fd 7c 6e 19 fd 67 fd 6a fd 5a 21 fd 5f 3e 33 fd fd fd fd fd 20 fd 25 fd 20 05 fd 61 0a fd fd 04 25 fd fd 73 38 fd 41 2a 2c 2d fd 73 17 4e fd fd fd 78 50 fd 7e 52 fd 7e 04 fd fd 71 fd fd fd 7a 77 fd 5a 55 fd 05 fd fd fd fd 5b 5b fd fd 3b 37 27 fd ab 6d 7e fd fd fd fd 51 fd 73 6e 2e 7c 7d fd 3b fd 5c fd bb 33 2a 58 fd 76 39 12 fd fd 19 24 2f 5f fd fd 6e fd 2d 67 48 fd fd 3a fd fa 4d 6b fd 29 fd	PNGIHDRaIDATxQ_2SUIbmmX[=v;3.^>?|ngjZ!_>3 % a%sA*,-sNP~R~qzwZU[;7'mQsn.};\3*Xv9$/_n-gH:Mk)	success or wait	1	405E46	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Begravedes\Viewer\Rammedes\view-wrapped-symbolic.symbolic.png	0	208	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd fd 0d fd 20 0c 45 5f 3c fd fd fd 55 64 40 fd 4c 27 2f 4e 20 6b fd 24 04 fd fd fd 27 3f fd fd 7d 6d fd fd 5a 60 01 1c 70 45 3e 01 2b 39 fd fd fd fd fd 1b fd fd fd fd 21 66 fd 49 54 fd 2e fd fd fd 16 15 6e fd 7d fd 1a 69 13 fd fd 6f fd fd 00 3a 60 0f fd 07 30 fd 00 42 fd 5a fd 03 00 fd 62 55 39 40 fd fd 5f 28 06 38 39 fd 57 fd 45 5f fd 22 fd 02 fd 2b 5d 0d fd fd 0d 34 fd 3e 28 fd fd 15 fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8E_<Ud@'/Nk$'?}mZ`pE>+9!fIT.n}io:`0BZbU9@_(89WE_"+]4>(IENDB`	success or wait	1	405E46	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq995B.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 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 15 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 29 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELoZ.!)	success or wait	1	405E46	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dlawt.exe	unknown	512	success or wait	393	405E17	ReadFile
C:\Users\user\Desktop\dlawt.exe	unknown	4	success or wait	2	405E17	ReadFile
C:\Users\user\Desktop\dlawt.exe	unknown	4	success or wait	51	405E17	ReadFile

Disassembly

No disassembly