ID: 798398
Sample Name: DPR602859651100125001V1100125154830E3-2-2023#U00b7pdf.exe
Cookbook: default.jbs
Time: 03:44:08
Date: 04/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

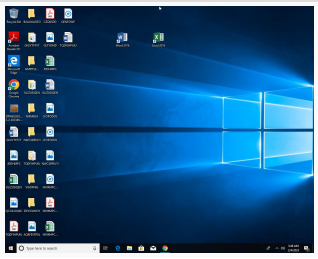
Windows Analysis Report

DPR6028596511001250O1V1100125154830E 3-2-2023#U00b7pdf.exe

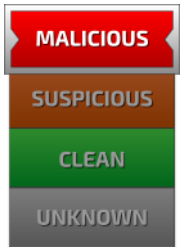
Overview

General Information

Sample Name:	DPR6028596511001250 01V1100125154830E 3-2-2023#U00b7pdf.exe
Analysis ID:	798398
MD5:	91c0c4710db0…
SHA1:	63880c602b96…
SHA256:	a4d4961d124e…
Tags:	exe
Infos:	



Detection

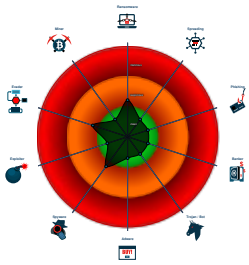


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- Contains functionality to dynamicall…
- Abnormal high CPU Usage
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- DPR6028596511001250O1V1100125154830E 3-2-2023#U00b7pdf.exe (PID: 5032 cmdline: C:\Users\user\Desktop\DPR6028596511001250O1V1100125154830E 3-2-2023#U00b7pdf.exe MD5: 91C0C4710DB096A4689D40E2CEB3814D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

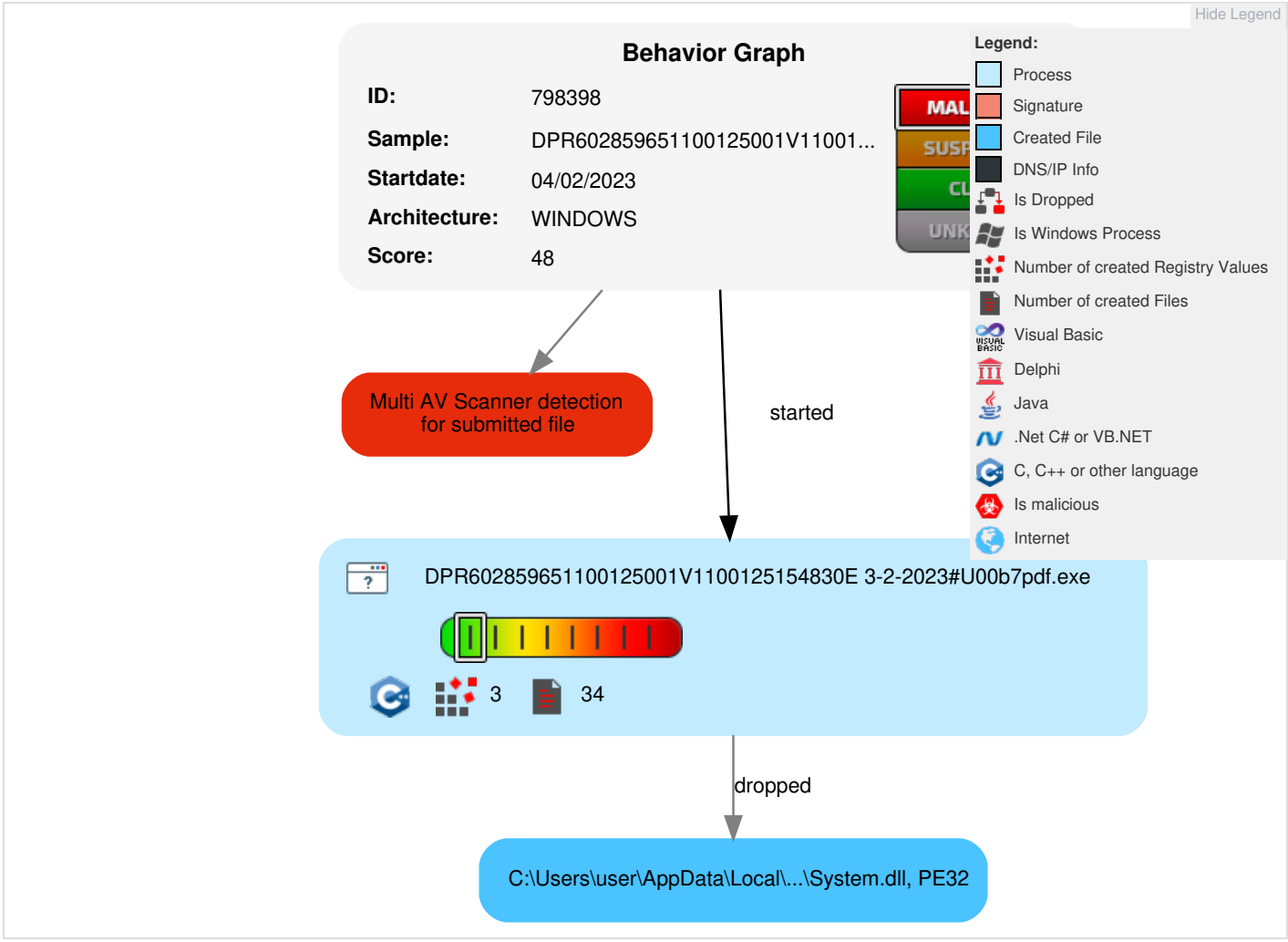
AV Detection

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 1 Masquerading	OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Access Token Manipulation	LSASS Memory	3 System Information 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	Query Registry	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

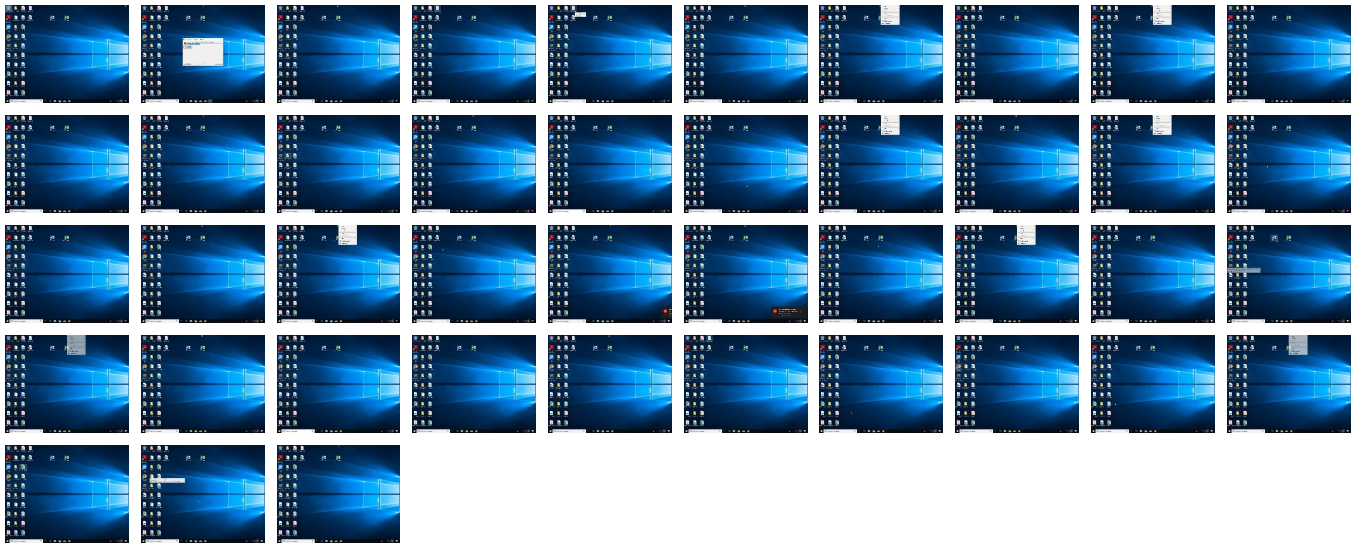
Behavior Graph



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
DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	47%	ReversingLabs	Win32.Trojan.Nsisx	
DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	46%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nshED41.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nshED41.tmp\System.dll	1%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	798398
Start date and time:	2023-02-04 03:44:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Detection:	MAL
Classification:	mal48.winEXE@1/7@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.5%) • Quality average: 87.7% • 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, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

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\Deskriptiv155\Hjertere\Hynde.Una

Process:	C:\Users\user\Desktop\DPR6028596511001250O1V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	ASCII text, with very long lines (34794), with no line terminators
Category:	dropped
Size (bytes):	34794
Entropy (8bit):	3.9997795398371228
Encrypted:	false
SSDEEP:	768:ccaHQHD7RgNO/PDcbf/CBrmE4Hi1r1scfUos2cX7nhL/djYY2v:iQHDyO4mrei7sqc7BdsYG
MD5:	DD18A90498456DFCAE95A46AFC33C475
SHA1:	65AB8F8342AF9C08FE39E7664E3DF9C9646DF211
SHA-256:	856D7590AB2EFC8C760BC37D652D5AE8A5DE982891ADB7A678E43A91D268DDE9
SHA-512:	BC6F1AED9B60D3C383E0A65C19E2FF031252DC9B193AE6AD3B5B6F3767EC2F7E6E6E4B3F65D2A3CBD501ED38C838C89A9648D255EAF1110BD7C5A0142F0A6A10
Malicious:	false
Reputation:	low
Preview:	6A34F0604AEE6DB314B378246D35FE80BFC162A6BA9C27C8E16DA2C9AE4B52DFB6BB4D14CCFA23C4B675E918121507BB7243C36C59FB457F64D397E98034F58490327D6C90C000BCD403F4272BEC91D0A33E5A0129628A58358949F71B9E468413A9F921ED449BFDFDFD8B52A2D79EC29D74E20791961A6CBC321812874EFFDA002DA4B6728BAC6F6A19E8DAA48014568DAC10440B68FF4911CE9C39E654E7BD5108097717BE2EF95C1A30EEFB3987C46DF521EAF29935CD47E5E692C36B39093D4C54B8F75D591A0FBE8521B1B811C1D5DE94F2446E4C6E3A52F9AF8CE6352838F7BFA2A9F2E978B6C63E24B131DB84C3D58F2272E6196F60D39BC78BC16F84DBD6729C7BE4C34C92F59F36A74676FEDD70E5E836CF8087A82BD101F899808FB96B6190BA47B820A5BABE361E59EC9FCCD938CFB68F2B3E0A7B59E68314002BFA8EE8E502796C53CD4716076F9F492DF2833BD6AD60228D25C9991C11A6CB28FAA225570F38AE4FC0F98A17CA0400AD9C6D66D92018971C0D79A5062B675A80F3A3E62E9196691C5DC24E022A718CA4F8012CAFE8F14181671A95F9D9650843B5EDCB80A8B14070975B13838161A8EFC0EB2E3233CE381BB0D822E3EA392FBE123D51467413E23E06FFF39AE85E5BAC5549DB7B405C6BEAC058711C90F3D73941BE2013BCBB2FC5FD5660B746D980317AD92DA8

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Rouleredes.coe

Process:	C:\Users\user\Desktop\DPR6028596511001250O1V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	data

Category:	dropped
Size (bytes):	223928
Entropy (8bit):	7.720384553629306
Encrypted:	false
SSDEEP:	3072:c5Nv/wHlbfgXh62+XKffH2i5A3Mz3xDD1TiBonOxOo0TUhBj4g2RgYyv:c5NvAbfgsrX6qMFdTiBQhooSBj4g2d4
MD5:	B32FFE1EC6ECA11009C35A0829450CB1
SHA1:	146529AFE038064ED79CAE0C62B108A14276D459
SHA-256:	151A299FCA8F459B7670EA4922931161D6E8024B19F1C723130F6576ACBDBC83
SHA-512:	CC32C0713B6E3C83D00682A73F2DB20FEAB0EBCD39A2CD768728FA9AD437CE0C24A6EBA7367DEC162447C14533064B93A2EB8422C843186AADADD6BEB99D7E4C
Malicious:	false
Reputation:	low
Preview:	..wh..8..ArM.0).LL....-G..t..N..."V.M.\og..Q].N...i.4...%.VV1.hK.'/..&.*$.U<....@.n..@..H.(.6.....C.i....z\uy.R.1.f...u.-..S..f....[5A...:b.....p...'..K..g.2O..A.....MGO....j.....I.N^.. .7W..$.6..D.q.....P&~.b4.Y8.@..n.....p..$.V.;.8\|k.\69+.P..Fr1.*.M$.Y.c..?.T...n.....0.....%.m%.#J._....<&-...%..v..4P..=..lz.YR.j.2.).j.*t..E.V.....U...7.R...G.+..ux.Fmg.n..D.. ..jz7...|...&.]K....A.....`oy..FM...(d:wx.._V....Y.bs..f.^$...Q.MZ.O.0.....x.a.t.nk.d....h3n.J8..R.$7..D2..g..f ...)..c..=8C.. N.....B.a"...z..&...e.....'B%-2.Z.*.....&.B.....q5/..A .xG.R3B..@.\|.V.ss.*Y.P..iM.1.F0>....S..{gSc.^.<.kT..A.....%..w..A.....3..{.3id..?....-trml..O.....TH.qU.A.....].a.H.Q4.R.&.Dh.?....8e.....0Sf..r.....,_..S....~..<.i...*0.d.. .+.^..Ou(.6&.>...,*^.w....-:0..=."......l.....H....T.B.F.(..J.3#...f...8...-1.e...j.....{4....!....AG^%.....L./.$.....Qz.T.H.....1.r..?D8*'.n..b>(fo.w.....,...&.....}/6.(..#UJ0.lWB....

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\checkbox_checked.png

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	PNG image data, 32 x 32, 2-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.579261213353732
Encrypted:	false
SSDEEP:	3:yionv//thPl3MrpxyPuReVl/nRwPd/ggZcFmz3iVVyjXrC5RlH1p:6v/lhP6TwOeVV6Pd/MmgEK5RlVp
MD5:	0CA13C84736F193C4DDC36408B63EB79
SHA1:	DAF222B1B08D7F2645FDC2E25E63BE2AA50E9B79
SHA-256:	9B7DA86B40E8FE9DA37BA2A4337C9BCE14B07153A9722DD3DE7772C1C5933DED
SHA-512:	1F95694E920B1BE5A7D9A4C4F7EABCCDE8326965D8B1E3211085C67E84229F76300AED6AE29E2D79E817857CFE7608919233057FAD6FDA3BF515C59F3604099
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .g....PLTE.....f.0....tRNS..v..8...7IDATx.c.....(."..@.& .....R;X...D8.....a^.....N'\..+....IEND.B`.

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\multimedia-volume-control-symbolic.svg

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	651
Entropy (8bit):	5.228667299529662
Encrypted:	false
SSDEEP:	12:t4Cp9xXnlWjoprGDWXYmfM26oprGhyGuC1hz4AeWrGdKdK:t4CpPlWsrGDoY32/rGYG/4AeWrGMQ
MD5:	367D90E6DF90CE72BAD009701DC3D941
SHA1:	C2070B79640687DBB8A64BFAC953CFA7625F7FFF
SHA-256:	2F11A00CC5DD755C1E5054AEF16CE293716532140B3DDB0F0623ABD460F99571
SHA-512:	F6DA3687D0676C11CD4B3D3F4C71797059DD62B05F09DC981684155671EB7924E6096B084DF43664D09B1A13BFADFE61C1FB678B3323ED7E9984EB8D7A2D19EC
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M2 5h2.484l2.97-3H8v12h-.475l-3.04-3H2z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M14 8c0-2.166-.739-4.02-2-5h-1v2c.607.789 1 1.76 1 3 0 1.241-.393 2.22-1 3v2h1c1.223-.995 2-2.873 2-5z" style="marker:none" color="#000" overflow="visible"/><path d="M11 8c0-1.257-.312-2.216-1-3H9v6h1c.672-.837 1-1.742 1-3z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible"/></g></svg>

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\phone-symbolic.svg

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	629
Entropy (8bit):	4.45278069770929
Encrypted:	false

SSDEEP:	12:TMHdPnnl/nu3tln5CfYUtLLgpvAjmAKWlzmOA/e7/lsEbWlM:2dPnnxu3tlQfjngEmAKvOA/U/lsEbN
MD5:	DA3858070B89AA5D3B4D5FC724BED12F
SHA1:	A923CDD523E0519E96147A05DE6D0024135127E4
SHA-256:	3CC19ADDFE48119EB91D48E7FE510920394DC96F3006C384FFD4F63B92A73480
SHA-512:	FF7BE5CC591CD146E56DD22BCB9FD82A21272592EA7E807B57F8D33E77DA7FB2C632CA12980B0B8CDA4028C5802EA803BC75A642714B80AAC244538E4819E502
Malicious:	false
Reputation:	moderate, very likely benign file
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 6 0 c -1.644531 0 -3 1.355469 -3 3 v 10 c 0 1.644531 1.355469 3 3 3 h 4 c 1.644531 0 3 -1.355469 3 -3 v -10 c 0 -1.644531 -1.355469 -3 -3 -3 z m 0 2 h 4 c 0.570312 0 1 0.429688 1 1 v 10 c 0 0.570312 -0.429688 1 -1 1 h -4 c -0.570312 0 -1 -0.429688 -1 -1 v -10 c 0 -0.570312 0.429688 -1 1 -1 z m 0 0"/>. <path d="m 7 1 h 2 c 0.550781 0 1 0.449219 1 1 s -0.449219 1 -1 1 h -2 c -0.550781 0 -1 -0.449219 -1 -1 s 0.449219 -1 1 -1 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\nshED40.tmp

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	296163
Entropy (8bit):	7.470506584929792
Encrypted:	false
SSDEEP:	6144:X5NvAbfgsrX6qMFdTiBQhooSBj4g2dgQ20cP7m:JjvTiapwjGdf20cP7m
MD5:	E0FD6297CF0E89D773C0AE44ED514229
SHA1:	EE4E3DEC2FFAD8B11887DD600B3A5D75982F0170
SHA-256:	5511DCF0AEFA2FDE583BEB5703774277C3ECB68B48AFA8B5D7F89F641B1F87F3
SHA-512:	5911A30953430870D7468C7BD48B57435FD6898800FC81EFA42FD340222E938D1C0889432C413163BC777044B412EF92A72740489FA620FE7220143D0A5A1C56
Malicious:	false
Reputation:	low
Preview:	.^.....,.....W...x?.....]....I^..... .....G...X.....j.....a..... ....

C:\Users\user\AppData\Local\Temp\nshED41.tmp\System.dll

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8Qll975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....MX.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.836361315282437

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:	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File size:	348136
MD5:	91c0c4710db096a4689d40e2ceb3814d
SHA1:	63880c602b960c5f91e55cbe4d5d18c7b8f1d63a
SHA256:	a4d4961d124ea4276512c1584f1ebd30951cd469659b3a623594d6361772fae7
SHA512:	b5fc41a609efb2946ddce21f383b5ae8e70d93b0fd0dec8e48b27f7660569ccdbafe806bf56fc0cd7c4e43826b79f065d57cd66da3c27e865cdced3ca865eb2a
SSDEEP:	6144:twq3NpWyFr7S0HFwnNHF6pmK2DIuua9ma+T4cX+tTMZP3qtTaPwkYn5inpT4:tzayFfDwNg4RE864c4MZ/c2UinS
TLSH:	C6741208B548D9A7C9630932ED628AF67ABDDE613BB1A70733006F7C7D312618F45365
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L...8.MX.....b...*.....J4.....@

File Icon

Icon Hash:	00c4c4dcdcd4d410

Static PE Info

General

Entrypoint:	0x40344a
Entrypoint Section:	.text
Digitally signed:	false
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:	0x584DCA38 [Sun Dec 11 21:50:48 2016 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:	4ea4df5d94204fc550be1874e1b77ea7

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007F0E40A5E5A3h
push ebx
call 00007F0E40A616FCh

Instruction
cmp eax, ebx
je 00007F0E40A5E599h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007F0E40A61676h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F0E40A5E57Ch
push ebp
push 00000009h
call 00007F0E40A616CEh
push 00000007h
call 00007F0E40A616C7h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007F0E40A612B0h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007F0E40A6129Eh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x68000	0x19ef0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b4	.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	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x3d000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x68000	0x19ef0	0x1a000	False	0.8527644230769231	data	7.543225711963014	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x683a0	0xbdfc	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x741a0	0x743a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x7b5e0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x7db88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x7ec30	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x7fad8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x80380	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x809e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x80f50	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x813b8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x816a0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x817c8	0x100	data	English	United States
RT_DIALOG	0x818c8	0x11c	data	English	United States
RT_DIALOG	0x819e8	0xc4	data	English	United States
RT_DIALOG	0x81ab0	0x60	data	English	United States
RT_GROUP_ICON	0x81b10	0xa0	data	English	United States
RT_MANIFEST	0x81bb0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetCurrentDirectoryW, GetFileAttributesW, GetFullPathNameW, Sleep, GetTickCount, CreateFileW, GetFileSize, MoveFileW, SetFileAttributesW, GetModuleFileNameW, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, WaitForSingleObject, GetCurrentProcess, CompareFileTime, GlobalUnlock, GlobalLock, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, WriteFile, lstrcpyA, lstrcpyW, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GlobalFree, GlobalAlloc, GetShortPathNameW, SearchPathW, lstrcmpiW, SetFileTime, CloseHandle, ExpandEnvironmentStringsW, lstrcmpW, GetDiskFreeSpaceW, lstrlenW, lstrcpynW, GetExitCodeProcess, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, MulDiv, MultiByteToWideChar, lstrlenA, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW

DLL	Import
USER32.dll	GetSystemMenu, SetClassLongW, IsWindowEnabled, EnableMenuItem, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, wsprintfW, ScreenToClient, GetWindowRect, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, LoadImageW, SetTimer, SetWindowTextW, PostQuitMessage, ShowWindow, GetDlgItem, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, DrawTextW, EndPaint, CreateDialogParamW, SendMessageTimeoutW, SetForegroundWindow
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW
ADVAPI32.dll	RegDeleteKeyW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, AdjustTokenPrivileges, RegOpenKeyExW, RegEnumValueW, RegDeleteValueW, RegCloseKey, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe PID: 5032, Parent PID: 3528

General

Target ID:	0
Start time:	03:44:57
Start date:	04/02/2023
Path:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Imagebase:	0x400000
File size:	348136 bytes
MD5 hash:	91C0C4710DB096A4689D40E2CEB3814D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshED3F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nshED40.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nshED41.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	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	4058C9	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	4058C9	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	4058C9	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	4058C9	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	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshED41.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	405889	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshED41.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nshED41.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1572	405E13	CreateFileW
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	2	4058C9	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	2	4058C9	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	2	4058C9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Deskriptiv155	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Rouleredes.coe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\checkbox_checked.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Deskriptiv155	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Hynde.Una	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\multimedia-volume-control-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\phone-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nshED41.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	405E13	CreateFileW
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	294	4058C9	CreateDirectoryW
C:\Users\Public	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	294	4058C9	CreateDirectoryW
C:\Users\Public\Music	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	294	4058C9	CreateDirectoryW
C:\Users\Public\Music\Klatres191	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\Public\Music\Klatres191	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	293	4058C9	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshED3F.tmp	success or wait	1	4036D7	DeleteFileW
C:\Users\user\AppData\Local\Temp\nshED41.tmp	success or wait	1	405A32	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshED40.tmp	0	32768	fd 5e 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 57 01 00 00 78 3f 00 00 00 00 00 00 fd 5d 00 00 01 00 00 00 6c 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	^,Wx?]l^	success or wait	14	405EB3	WriteFile
C:\Users\user\AppData\Local\Temp\nshED41.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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 1a fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELMX!	success or wait	1	405EB3	WriteFile
unknown	unknown	124			invalid handle	4	10002965	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Rouleredes.coe	0	16384	fd 5d 77 68 fd fd 38 fd fd 41 72 4d fd 30 29 fd 4c 4c fd 18 87 fd 2d 47 02 79 74 12 fd 4e fd 08 fd 22 56 fd 4d fd 5c 6f 67 fd fd 51 5d fd 4e fd fd fd 69 fd 34 fd fd 0e 25 0a 56 56 31 fd 68 4b fd 27 2f 06 fd 26 fd 2a 24 fd 55 3c 2e 19 fd fd 40 fd 6e b6 fd 40 fd fd 48 0e 28 fd 36 08 04 fd fd 00 00 43 fd 69 0b fd 96 fd 7a 5c 75 79 fd 52 e2 31 fd 66 08 fd fd 75 fd 2d fd fd 53 fd fd 66 fd fd fd fd 5b 35 41 fd fd 3a 62 fd 16 fd 17 fd 70 fd 81 fd 27 fd fd 4b fd fd 67 13 32 4f fd fd 41 fd 04 fd fd 18 fd fd 53 4d 47 4f 15 fd 03 18 6a fd fd 7f 3f fd fd fd 6c fd 4e 5e 11 fd fd 37 57 fd fd 24 11 36 fd 09 44 02 71 fd fd fd fd c2 50 26 7e fd 62 34 fd 59 38 fd 40 fd fd 6e fd fd 11 fd fd 1f fd 70 fd 05 24 fd 56 b9 3b	wh8ArM0)LL-GtN"VM\ogQ]Ni4%VV1hK'/&*$U<.@n@H(6Ciz\uyR1fu-Sf[5 A:bp'Kg2OAMGOjlN^7W $6DqP&~b4Y8@np$V;	success or wait	14	405EB3	WriteFile
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\checkbox_checked.png	0	147	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 20 00 00 00 20 02 03 00 00 00 0e 14 fd 67 00 00 00 09 50 4c 54 45 fd fd fd fd fd fd 00 fd 0c 66 fd 30 00 00 00 02 74 52 4e 53 00 00 76 fd fd 38 00 00 00 37 49 44 41 54 78 01 63 fd 04 fd fd fd fd fd fd 0d 98 fd fd fd 00 28 0c 22 fd 1a 40 0c 26 20 03 fd 14 fd 01 52 3b 58 18 fd 2e 44 38 1e fd 1d fd 07 61 5e fd 12 18 00 fd fd 4e 27 5c fd fd 2b 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDR gPLTEf0tRNSv87IDATxc("@& R;X.D8a^N"\+IENDB`	success or wait	1	405EB3	WriteFile
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Hynde.Una	0	16384	36 41 33 34 46 30 36 30 34 41 45 45 36 44 42 33 31 34 42 33 37 38 32 34 36 44 33 35 46 45 38 30 42 46 43 31 36 32 41 36 42 41 39 43 32 37 43 38 45 31 36 44 41 32 43 39 41 45 34 42 35 32 44 46 42 36 42 42 34 44 31 34 43 43 46 41 32 33 43 34 42 36 37 35 45 39 31 38 31 32 31 35 30 37 42 42 37 32 34 33 43 33 36 43 35 39 46 42 34 35 37 46 36 34 44 33 39 37 45 39 38 30 33 34 46 35 38 34 39 30 33 32 37 44 36 43 39 30 43 30 30 30 42 43 44 34 30 33 46 34 32 37 32 42 45 43 39 31 44 30 41 33 33 45 35 41 30 31 32 39 36 32 38 41 35 38 33 35 38 39 34 39 46 37 31 42 39 45 34 36 38 34 31 33 41 39 46 39 32 31 45 44 34 34 39 42 46 44 46 44 46 44 38 42 35 32 41 32 44 37 39 45 43 32 39 44 37 34 45 32 30 37 39 31 39 36 31 41 36 43 42 43 33 32 31 38 31 32 38 37 34 45 46 46 44	6A34F0604AEE6DB314B378246D35FE 80BFC162A6BA9C27C8E16DA2C9AE4B 52DFB6BB4D14CCFA23C4B675E91812 1507BB7243C36C59FB457F64D397E9 8034F58490327D6C90C000BCD403F4 272BEC91D0A33E5A0129628A583589 49F71B9E468413A9F921ED449BFDFD FD8B52A2D79EC29D74E20791961A6C BC321812874EFFD	success or wait	3	405EB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\multimedia-volume-control-symbolic.svg	0	651	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 32 20 35 68 32 2e 34 38 34 6c 32 2e 39 37 2d 33 48 38 76 31 32 68 2d 2e 34 37 35 6c 2d 33 2e 30 34 2d 33 48 32 7a 22 20 73 74 79 6c 65 3d 22 6d 61 72 6b 65 72 3a 6e 6f 6e 65 22 20 63 6f 6c 6f 72 3d 22 23 62 65 62 65 62 65 22 20 6f 76 65 72 66 6c 6f 77 3d 22 76 69 73 69 62 6c 65 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 31 34 20 38 63 30 2d 32 2e 31 36 36 2d 2e 37 33 39 2d 34 2e 30 32 2d 32 2d 35 68 2d 31 76 32 63 2e 36 30 37 2e 37 38 39 20 31 20 31 2e 37 36 20 31 20 33 20 30 20 31 2e 32 34	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M2 5h2.484l2.97-3H8v12h-.475l-3.04-3H2z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M14 8c0-2.166-.739-4.02-2-5h-1v2c.607.789 1 1.76 1 3 0 1.24	success or wait	1	405EB3	WriteFile
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\phone-symbolic.svg	0	629	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 20 3c 70 61 74 68 20 64 3d 22 6d 20 36 20 30 20 63 20 2d 31 2e 36 34 34 35 33 31 20 30 20 2d 33 20 31 2e 33 35 35 34 36 39 20 2d 33 20 33 20 76 20 31 30 20 63 20 30 20 31 2e 36 34 34 35 33 31 20 31 2e 33 35 35 34 36 39 20 33 20 33 20 33 20 68 20 34 20 63 20 31 2e 36 34 34 35 33 31 20 30 20 33	<?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 6 0 c -1.644531 0 -3 1.355469 -3 3 v 10 c 0 1.644531 1.355469 3 3 3 h 4 c 1.644531 0 3	success or wait	1	405EB3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	unknown	512	success or wait	281	405E84	ReadFile
C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	unknown	16384	success or wait	13	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nshED40.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nshED40.tmp	unknown	24196	success or wait	1	403269	ReadFile
C:\Users\user\AppData\Local\Temp\nshED40.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nshED40.tmp	unknown	4	success or wait	10	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nshED40.tmp	unknown	4	success or wait	5	405E84	ReadFile
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Hynde.Una	unknown	2	success or wait	1023	4026D2	ReadFile
C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Rouleredes.coe	unknown	98226176	success or wait	1	10002965	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sansebeskrivelsers	success or wait	1	40242E	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sansebeskrivelsers\Vandsamling197	success or wait	1	40242E	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sansebeskrivelsers\Vandsamling197\Hybridnettets	success or wait	1	40242E	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sansebeskrivelsers\Vandsamling197\Hybridnettets\Energimaengde52	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\carboxylsyren	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\carboxylsyren\Fluer172	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\carboxylsyren\Fluer172\Amortisationerne	success or wait	1	40242E	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\WOW6432Node\weighers	success or wait	1	40242E	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sansebeskrivelsers\Vandsamling197\Hybridnettets\Energimaengde52	Orientalises	binary	23 CD 59	success or wait	1	40248E	RegSetValueExW
HKEY_CURRENT_USER\Software\carboxylsyren\Fluer172\Amortisationerne	Sociometr	binary	11 45 F3	success or wait	1	40248E	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\weighers	Lunefuldest	unicode	Alphyls	success or wait	1	40248E	RegSetValueExW

Disassembly

No disassembly