ID: 634445
Sample Name: PO64747835 PDF.exe
Cookbook: default.jbs
Time: 06:00:09
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report PO64747835 PDF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 4
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 9
Private 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_ITA.chm 10
C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll 11
C:\Users\user\AppData\Local\Temp\RACOYIAN.hav 11
C:\Users\user\AppData\Local\Temp\foromtalers.Fid 11
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe 12
C:\Users\user\AppData\Local\Temp\libLerc.dll 12
C:\Users\user\AppData\Local\Temp\libenchant-2.dll 12
C:\Users\user\AppData\Local\Temp\msvcr100.dll 13
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll 13
C:\Users\user\AppData\Local\Temp\system-shutdown.png 13
C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg 14
Static File Info 14
General 14
File Icon 14
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 16
Data Directories 16
Sections 16
Resources 16
Imports 17
Version Infos 17
Possible Origin 17
Network Behavior 18
Statistics 18
System Behavior 18

Analysis Process: PO64747835 PDF.exePID: 6248, Parent PID: 5196 18
General 18
File Activities 18
File Created 18
File Deleted 30
File Written 30
File Read 35
Registry Activities 35
Key Created 35
Key Value Created 35
Disassembly 36

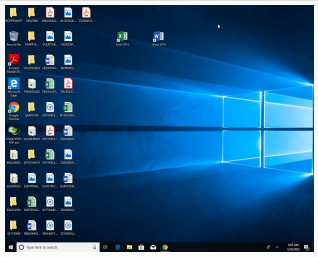
Windows Analysis Report

PO64747835 PDF.exe

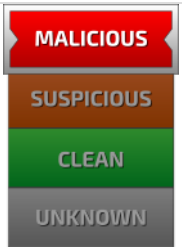
Overview

General Information

Sample Name:	PO64747835 PDF.exe
Analysis ID:	634445
MD5:	9a548d0455360a.
SHA1:	2d96b448e8a704.
SHA256:	9af1b3d7b095b1..
Tags:	exe
Infos:	



Detection



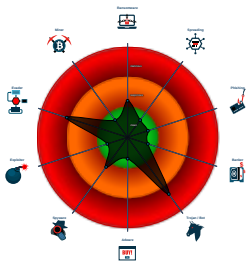
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- PO64747835 PDF.exe (PID: 6248 cmdline: "C:\Users\user\Desktop\PO64747835 PDF.exe" MD5: 9A548D0455360A501EA392C85ECDB905)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://donaldtrumpverse.com/kOrg_stUoodKu54.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.769947048.0000000002920000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

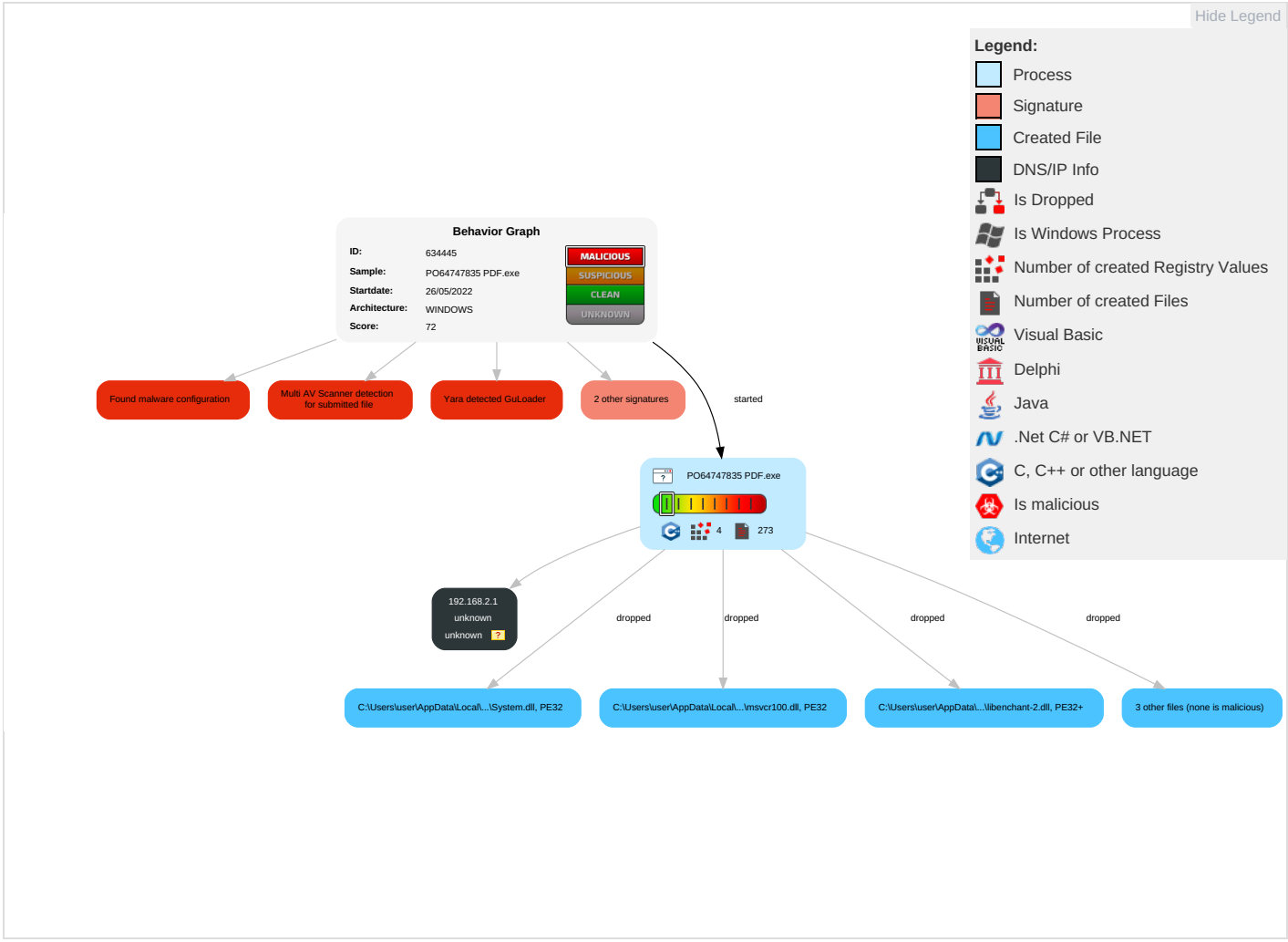
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Windows Service	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	1 Windows Service	2 1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	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 Software Packing	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Timestomp	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

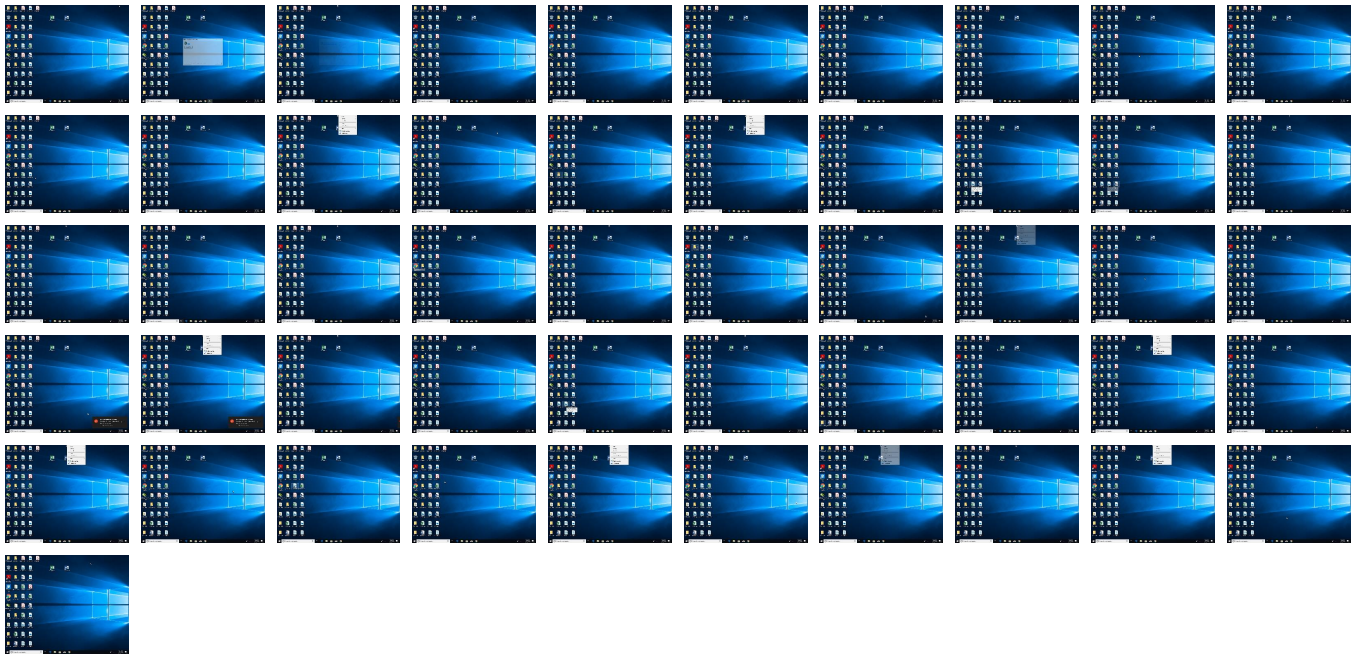
Behavior Graph



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
PO64747835 PDF.exe	15%	ReversingLabs	Win32.Trojan.InjectorX	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libLerc.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libenchant-2.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libenchant-2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\msvcr100.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\msvcr100.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://us1.api.ws-hp.com/clienttelemetry	0%	Avira URL Cloud	safe	
http://https://stage-us1.api.ws-hp.com/clienttelemetry	0%	Avira URL Cloud	safe	
http://https://pie-us1.api.ws-hp.com/clienttelemetry	0%	Avira URL Cloud	safe	
http://donaldtrumpverse.com/kOrg_stUoodKu54.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://donaldtrumpverse.com/kOrg_stUoodKu54.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://schemaregistry.analysis.ext.hp.com/cdm/id/sw/sysInfoBase.schema.json	CDMDataEventHandler.dll.0.dr	false		high
http://https://us1.api.ws-hp.com/clienttelemetry	CDMDataEventHandler.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://stage-us1.api.ws-hp.com/clienttelemetry	CDMDataEventHandler.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	PO64747835 PDF.exe	false		high
http://https://schemaregistry.analysis.ext.hp.com/cdm/id/sw/originatorDetail.schema.json	CDMDataEventHandler.dll.0.dr	false		high
http://https://pie-us1.api.ws-hp.com/clienttelemetry	CDMDataEventHandler.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://schemaregistry.analysis.ext.hp.com/cdm/gun/com.hp.cdm.platform.software.domain.eventing.reso	CDMDataEventHandler.dll.0.dr	false		high

World Map of Contacted IPs

Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private
IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634445
Start date and time: 26/05/202206:00:09	2022-05-26 06:00:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO64747835 PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
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:	mal72.troj.evad.winEXE@1/11@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.3% • 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 • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.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
- 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\Temp\Bluetooth Suite help_ITA.chm

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	43566
Entropy (8bit):	7.382704049850724
Encrypted:	false
SSDEEP:	768:7gyaYEUz32Q+MLPybLI1GPlnL7ZsruV+P/34RE+OUuiozjd/6W4:7gvFUz32ftIsMuV+PYSU9o3d/94

MD5:	27729CF331D3767DF077F52B262D88F3
SHA1:	EF4B6F74A0608B5A4DC6E3CA465A96137C1CAD74
SHA-256:	CA601E57DD2C1E6E92145A8A19083599261B626A4D26B04D8C3FD5BDDDB2CB0D
SHA-512:	AC7B8D61462538011D20BEC2D2BEAE62AB7DAA16866FC9B1CDBBDCEDF47796D93507E2E706CA9DECF0C26D0F1031285B9268A747755ABCB1E4A161B9D9CF 8F2
Malicious:	false
Reputation:	low
Preview:	ITSF....`..................|.{......."......|.{......."..`...............x.......T......................................ITSP....T..j..].!......."..T...............PMGL................/..../#IDXHDR.. .M.../#ITBITS..../#STRINGS...2.]./#SYSTEM..f.T./#TOPICS...M.@./#URLSTR...}.5./#URLTBL.....p./#WINDOWS...M.L./$FIftiMain......G./$OBJINST...G.?./$WWAss ociativeLinks/..../$WWAssociativeLinks/Property...C../$WWKeywordLinks/..../$WWKeywordLinks/BTree.....L./$WWKeywordLinks/Data...e4./$WWKeywordLinks/Map ....../$WWKeywordLinks/Property...# ./Advanced_Phone_Operations.htm....../Audio_Services.htm....../Authorization_Options.htm.....$/Bluetooth Win7 Vista Suite he lp.hhc...Z.k$/Bluetooth Win7 Vista Suite help.hhk...E.../Bluetooth_Devices.htm..0..z./Bluetooth_Devices_files/...//Bluetooth_Devices_files/colorschememapping.xml...\.:%/B luetooth_Devices_files/filelist.xml...a.['/Bluetooth_Devices_files/themedata.thmx...<. ./Bluetooth_Settings.htm...*..[./Bluetooth_

C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	101480
Entropy (8bit):	5.754479856662274
Encrypted:	false
SSDEEP:	1536:HMrDKbA8xl6y9Oj2FqnawHzDYwVY4quXoYbggnC:HM6dMy9MHBVY4qAolOC
MD5:	25F3ECFD195030F6B1BAD60E5EF97163
SHA1:	749B7E267CDBBC83783DFA4C7BF45134556C13D7
SHA-256:	FCD740746D2B3E01945E6A099AB4CDD06ECE05818E25D08C5DDAFBD333B0DC84
SHA-512:	D91803A022DD9A6EF0E77CB231A5FB5DD1BC275F4CC38D886FD365B7EEAD094712ADC4FA3AAFFB8354DC193BAC3B8697F685631AE3B4D23924387706DB3C0 DD9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....?!..........." ..0..h.............. ....`...................................O.......|............r..h..............T........................................... ............... ..H............text....g... ...h................. ..`.rsrc...|............j.............@..@.reloc........ ....p.............@..B......................H........u..(....*.0..S........ r...pr3..p..(....(1...........o2.....r...pr...pr3..p. (....... r...pr3..p."(....*..........'..... ..0..K........ r...pr3..p.'(....(1...o4.....r...pr...pr3..p..(....... r...pr3..p.0(....*.................0..L........ r@..pr3..p.6(..........(......r...pr@..pr3..p.=(....... r@..pr3..p.?(....*......... ....0..u........ r...pr3..p.C(.....(...+..(...+.(....%.o....(.....o....(....o....o.

C:\Users\user\AppData\Local\Temp\RACOYIAN.hav

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	85684
Entropy (8bit):	6.433546139636705
Encrypted:	false
SSDEEP:	1536:dTTvb32heICeH0brTb9rndDhW7ZMTi2A4l+HIhFkUYN:dTTvbzWH0bdthKZvd4QHIhFkxN
MD5:	E17F742A3B79DF2D21AC403EAFB27574
SHA1:	5A53F28B12C228F77FAF580A54F1E12AC6B93427
SHA-256:	D8A19805B48F85692AB8E6D8090A5151041DC73DD5C07B98171F7AE242250E41
SHA-512:	2CD3EB09F986F838A1C38479035C3B0FB5112A89CC81D24CF60C53C70707A04221196249ABC9C37FD65676A22728817285FC7EE8EFC6585F130A12E44478D1FF
Malicious:	false
Reputation:	low
Preview:	...d..o..a......)..Fu..f.h.f.c....4E.G..f..........f....1.A..u....2.L.n77777777777777777777 7777777777777777777777777.......~........f.k.....i,]]]]]]]]]]]]]]]]]]]]]]]]].f..........2E.k...f...f.v..88.q8&&&&&&&&&&&&&&&&&&&&&&&&&&&&& &&&&&&&&&&&&&&&&&&&&&&&&..z.#f.........f...f.....l4.............................q.xf...f......6..ccAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA. ....w.....j../.&._...f.u.....u.....7..7$hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh.....t.f.i....-..N\\.f... .....f.b..+.>`...[.i.r.......t..-A. ;...s."......!.p.b............................ .f...f.........f.v..5l.C..............................

C:\Users\user\AppData\Local\Temp\foromtalers.Fid

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	37208
Entropy (8bit):	3.9995207312720225
Encrypted:	false

SSDEEP:	768:Y9RVFQbsrxeETZvAuCk4H9TTMIjf5Ni/0QQSg2hT/ma6d:YTVF47Ep7Ck89EWeM7JZd
MD5:	EEDF996AEE7BE718D4ED650F72298AC4
SHA1:	BC860286D87BA1D7C66A9E3351C14A8C1C230461
SHA-256:	8ACC66E278720D3C67A2295079BB8C9A595C9732A85F361E01B22349246E333E
SHA-512:	DECB271E8E54929DDD94D1EE60B9538E640B200D3B0F27BBA0E4080996E3817033B38AA54A3C2562AB45CD91E05D99209FBE126F572F9EF1B074CEDF0760C3A B
Malicious:	false
Reputation:	low
Preview:	2AF8FA142F900CA287F3E22503957E71C7D5972707E801D8BA54A11B857A8578CF2F56B2B8CADE6E0BEAFFCEDA706DA46F9320EECA970AC91E6B6797 0921BC7E56F9434099AC7713864E2DBB49EA6A572EF5524AE4013074E0BA83B87F67687AEF99EB5FCC33A78C7A650CF9C306ADAECF2079601B3F7EAC 6C7954041DF3C4802423503C75FCCDA44DE53CC7E1D533510CD12101C669304D903F40755F664B1172B4311D5225F7241D178286C458988474BE1DFB 9697EBD6F82137D5AE9B0C22E9BDAE39AE002BD9CE2F185654638A97743FCD8C0CC9D8125FA8A058B4525E54F787AF6787E90C9654E18BAF3BABABCD 7EBD60C105B2767ABA4AC67BA6B46EBBCA5A972CF44490BE185A1A366D7788BBE9698838F1EBBE6E2474CE0129F76B69A6FB46BBB4885F2E4439B56E 9025C8E061A32745281A43A3C1C2AE41654E8985AAAE3CB0540583B33E54DFB9062AFCFC2CB7C866EA7D42C371452273AE7B83B084D3DECE3EF2DEBA 760BE5854A10FDE5F776F2BBCA19ECA406F2765CEE4BCA0B7E8D24048F6814832C5F866F08FC26B824E94AB3DF1C93AAD642FA07B81A39C3A0EB05FC B24087F7ECB24C45845FAAC3708F30DF8DE1B18034F7749B1B4EC9598C6EDAE5D71F8967CFEB2596F3799AA4ECD37FE7B688252A798F3FDB75C8278C B8F27F4AA3E4020AD0E11BFA1CEDBD9FB9168B27

C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	22479
Entropy (8bit):	5.08095074751023
Encrypted:	false
SSDEEP:	384:PxozhVwKBMySMIKoE/pJf2OG3mcJ7t/CWP9At/H:P6Vf2yS0r/pJf6BEWP9At/H
MD5:	8154B723020AEE70829FFC138C9D1C4C
SHA1:	6F7AF3827B37845F071625458DF1DB8BA9056FD6
SHA-256:	902F9D2A239CCAEBA677DB5838654FB6CE7CF3D21243B8EF122E9D970714B0D3
SHA-512:	D3F59F778AA72D26896AA2C81972F144DAB716DFA8E45E7B3C59F528B2752FE9E8971C86CF927C62E7501D9910E9D1212EFA1A58C29796A92E2D433116E76931
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....N..E.....&....%. ...J.....@..... .....>....`... .....P..@.....@..(.....\.....text...X..... .....`..`.data.....0.....$..... .....@....rdata.....@.....&.....@..@.pdata..@....P.....2.....@..@.xdata.....`.....6.....@..@.bss.....p.....idata.....8.....@. ...CRT....`.....B.....@....tls.....D.....@....rsrc.....F.....@....reloc.....L.....@..B..... .....

C:\Users\user\AppData\Local\Temp\libLerc.dll

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	602739
Entropy (8bit):	6.344393812734055
Encrypted:	false
SSDEEP:	12288:PCaPBchMCFjXEbIaM43VV1oSIG5BY5IikQH/oNguISjFovd:KaaMCeVV1oSIG5BY3/oNuSjFovd
MD5:	58BFEB91921D4882F7EDABAB9C0C1C17
SHA1:	596DB0512A25089EF7CDE48CA3393E4F6878FF90
SHA-256:	5C9DB6D64BAF0250735368825CEC3032EC39999F266125D132157ECC0403EE12
SHA-512:	A86C5F00109267532531366DF07A0187D2FBB80E1628A6E30508AA74098CAB4CDF5CAD54468929604F89CAA656BDBEF6B2F25C462AA1B72898B66F3B8D227AA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&..V.....&"...%....."....P.....Y..... .....P|....`... .....`.....p.,.....L.....@...(.....$r.....text.....`..`.data..... .....@....rdata.....@..@.pdata..L.....@..@.xdata...#... ...$.....@..@.bss.....P.....edata.....`.....@..@.idata.. ,....p.....@....CRT....X..... .....@....tls.....".....@....reloc.....$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\libenchant-2.dll

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows

Category:	dropped
Size (bytes):	49851
Entropy (8bit):	5.71925712297816
Encrypted:	false
SSDEEP:	768:59P9Y+clVaXLNcGRmDRC31lRrox5iJXx/gn9VFuKVcXGJMRv7hb8u+DwbMORdiPF:HPe+lkBcAEC31luGCQKKWJa8atRIPNQa
MD5:	6A9928C42EB4375CCEF3A025F3535795
SHA1:	395703F4970B42F55C2BCB2B8CF3F0D12E192CEB
SHA-256:	CAA457EF4BD84476790D215FFFF048DEB162CABC14DB3FF679795CCEA8972411
SHA-512:	27F1E2E3DDF052A05D9F0C48E0936E0D4A7E850E4E835EAED96495E6241167915FCDAD371EA206C5B741846D70FF3AFCBA83269B01ED90B22B3F7F42572F03DB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....~.....&"...%.h.....P.....V.....P .....O...`... .....\....0..8.....@..l.....@...(.....text...hf.....h.....`..`.data.....l..... .....@....rdata..P.....n.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata.....@..@.idata.. \.....@....CRT....X.....@....tls..... .....@....rsrc...8....0.....@....reloc..l....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\msvcr100.dll

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	773968
Entropy (8bit):	6.901559811406837
Encrypted:	false
SSDEEP:	12288:nMmCy3nAgPAxN9ueqix/HEmxsvGrif8ZSy+rdQw2QRAtd74/vmYK6H3BVoe3z:MmCy3KxW3ixPEmxsvGrm8Z6r+JQPzV7z
MD5:	0E37FBFA79D349D672456923EC5FBBE3
SHA1:	4E880FC7625CCF8D9CA799D5B94CE2B1E7597335
SHA-256:	8793353461826FBD48F25EA8B835BE204B758CE7510DB2AF631B28850355BD18
SHA-512:	2BEA9BD528513A3C6A54BEAC25096EE200A4E6CCFC2A308AE9CFD1AD8738E2E2DEFD477D59DB527A048E5E9A4FE1FC1D771701DE14EF82B4DBCDC90DF0387630
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:.y.~...~...~...w...}...~.....eD.....eD..+...eD..J...eD.....eD.....eD.....Rich~.....PE..L.....M.....!.....0.....x.....@.....H.....d...(.....P.....$L...!..8.....h E..@.....text...!..... ..`.data....Z...0...N.....@....rsrc.....f.....@..@.reloc..$L.....N...j.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
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.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... .....

C:\Users\user\AppData\Local\Temp\system-shutdown.png

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	429
Entropy (8bit):	7.2660585571428715
Encrypted:	false
SSDEEP:	12:6v/723xn6PprukRVpsTWuFTEmRpnJGoQ6:9n6P7RvsTWuFTXpnNQ6
MD5:	84D033B14C06568FA57352CCF18D8D35
SHA1:	1D75B42F61842E8B0FA8D811DAC72B313CDDCA74
SHA-256:	3989B93626DC3ED6EF03430AD0B1FF5C6E358DAC76E34ED7C8086579B68E660F
SHA-512:	EAFE07814DF75D019EB39D999325818CE8F2D164A621E713709EE5E1F3D260EB6BCAA726A17588D034F6A6E7733B71A5141CE5B4CFCE267CBFA22B82D622778 3
Malicious:	false
Preview:	.PNG.....IHDR.....a...tIDATx..S.n.P.-.6w7..8;...#.E.].8.....wh.O."....`....^o{...4.R .....4..F{....h..}o.X..d...4M..V.ELH.aA.-.%D<..g.Tj.....x....[E(..J.z..n7...R..X..\..D... !..h5.....3.w/... ....K.;c....MO.O.`.....h4..d.....`~T9::"..I...0p.R..\.....&.....;.F..X.a....;.._%....P.\.B.D..t.D..Y....B.Z..1...5U.U...1...Z..D"R.T..w@:...%.....\...\..-.B.....E{....h.. ;w....p..+....IEND.B`.

C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg

Process:	C:\Users\user\Desktop\PO64747835 PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	335
Entropy (8bit):	4.737555359684875
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slZRI2rjFvRbWHFHUHFvCpifW1IUHFBLJZtSKlNK+:TMHdPnnl/nu3i2FZ484sIBLjdlj
MD5:	C05C42CB3D95BF3BC7F49CCD8DCCA510
SHA1:	20442E344E95508586B1B2A7B4C6272C3F5C86F8
SHA-256:	695554CE5F23A275D3C25C27410D0CFBF8A83156807DAA3A601635E4E5D8AED0
SHA-512:	0EC19BBA7B5032670524965A8C55D8C6401F833000880DE1C0F74A5EAA4E302B0CE3E60218F3DDB95CB3E1EA7374A197CB71682526DFF910D9A6CF35FF971BE 6
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 4 1 c -1.660156 0 - 3 1.339844 -3 3 v 8 c 0 1.660156 1.339844 3 3 3 h 8 c 1.660156 0 3 -1.339844 3 -3 v -8 c 0 -1.660156 -1.339844 -3 -3 -3 z m 0 6 h 8 v 2 h -8 z m 0 0" fill="#2e3436"/>.</ svg>.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.76537086611817
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:	PO64747835 PDF.exe
File size:	1004686
MD5:	9a548d0455360a501ea392c85ecdb905
SHA1:	2d96b448e8a70468c24aa1e9848c350e9fab1696
SHA256:	9af1b3d7b095b178c588d19e2d7a9418d5c638b4ac7b94ba3dc9d9223f14a52c
SHA512:	0160e41e5bb62af676f965e9b958fd552273abb4a5bdf09b90d13507b474519b9dbb252e2b0d57485fb2cd1bb7b406f1a2b27d28a8cff80ab0e63bb5f56db40c
SSDEEP:	24576:bbHwJU6HPz7KU7lXzd2+glsofFiXKU74yNCj:fHx47NxlMo9i6j
TLSH:	BD2513216614F817F3900972C9E6F77E56B4FA382EA1CA03A6687F2D363D75C5828316
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...Z.Oa.....j.....

File Icon

Icon Hash:	7cbc7e6e78b0e010

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F8FC0AE458Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx

Instruction
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F8FC0AE455Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6c000	0x28498	.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	
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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x36000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x28498	0x28600	False	0.447235390867	data	5.43623310188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6c358	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7cb80	0x94a8	data	English	United States
RT_ICON	0x86028	0x5488	data	English	United States
RT_ICON	0x8b4b0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 65279, next used block 4294967040	English	United States
RT_ICON	0x8f6d8	0x25a8	data	English	United States
RT_ICON	0x91c80	0x10a8	data	English	United States
RT_ICON	0x92d28	0x988	data	English	United States
RT_ICON	0x936b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x93b18	0x100	data	English	United States
RT_DIALOG	0x93c18	0x11c	data	English	United States
RT_DIALOG	0x93d38	0xc4	data	English	United States
RT_DIALOG	0x93e00	0x60	data	English	United States
RT_GROUP_ICON	0x93e60	0x76	data	English	United States
RT_VERSION	0x93ed8	0x27c	data	English	United States
RT_MANIFEST	0x94158	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Version Infos

Description	Data
LegalCopyright	Euthanasiachromo202
FileVersion	24.24.17
CompanyName	Conciliato
LegalTrademarks	LASHINGPREEXPOU
Comments	Subconceptflovse2
ProductName	Ritha
FileDescription	andenk
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

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: PO64747835 PDF.exe PID: 6248, Parent PID: 5196

General

Target ID:	0
Start time:	06:01:09
Start date:	26/05/2022
Path:	C:\Users\user\Desktop\PO64747835 PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO64747835 PDF.exe"
Imagebase:	0x400000
File size:	1004686 bytes
MD5 hash:	9A548D0455360A501EA392C85ECDB905
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: 00000000.00000002.769947048.0000000002920000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsjD8DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	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	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nseD9AB.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	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	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	1	405AF7	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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\RACOYIAN.hav	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_ITA.chm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\foromtalers.Fid	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\libLerc.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\libenchant-2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\msvcr100.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\system-shutdown.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsiE370.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE371.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE372.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE373.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE374.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE375.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE376.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE377.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE378.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE379.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE37A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE37B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE37C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiE37D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3AE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsdE3B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3B9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE3BA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3F9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3FB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3FC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3FD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE3FF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnE400.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4BD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4C0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE4C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE502.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE503.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsdE504.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE505.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE506.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE507.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE508.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE509.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE50A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE50B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE50C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE50D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE50E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE50F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE510.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE511.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE512.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE513.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE514.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE515.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE516.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE517.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE518.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdE548.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE549.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE54A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE54B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsyE54C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE54D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE54E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE54F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE550.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsyE551.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE552.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE553.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE554.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE555.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE556.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE557.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE558.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE559.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyE55A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE58A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE58B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE58C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE58D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE58E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE58F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE590.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE591.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE592.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstE593.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE594.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE595.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE596.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE597.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE598.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE599.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE59A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE59B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE59C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE59D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE59E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE59F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE5A0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE5A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE5A2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE5A3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5D9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5DA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsoE5DB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5DC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5DD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE5DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE60E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE60F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE610.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE611.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE612.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE613.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE614.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE615.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE616.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE617.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE618.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE619.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE61A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE61B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE61C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE61D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE61E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE61F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE620.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE65F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE660.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstE661.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE662.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE663.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE664.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE665.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE666.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE667.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE668.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE669.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE66A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE66B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE66C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstE66D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE69D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE69E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE69F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsoE6A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6AE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE6E7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6E9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6EA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6EB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6ED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6EE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE6F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseE720.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE721.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE722.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE723.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE724.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE725.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE726.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE727.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE728.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE729.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE72A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE72B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE72C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE72D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE72E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE72F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE730.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE731.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE732.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE733.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE734.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE735.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE736.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE737.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE738.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseE739.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseE73A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE76A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE76B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE76C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE76D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE76E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE76F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE770.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE771.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE772.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE773.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE774.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE775.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE776.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE777.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE778.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE779.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE77A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE77B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE77C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE77D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE77E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE77F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszE780.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nszE781.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjD8DF.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseD9AB.tmp\System.dll	0	12288	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 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\RACOYIAN.hav	0	27744	fd fd 0f 64 fd 0f 6f fd 0f 61 fd fd fd fd fd fd 29 fd fd 46 75 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 66 0f 68 50 66 0f 63 fd fd fd fd 34 45 a5 47 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 66 fd fd 00 0f fd fd fd 1b fd fd 66 0f fd fd fd 31 fd 41 fd 1c fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 fd fd fd fd 0f fd fd 0f 75 fd fd fd fd 32 fd 4c fd 6e 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37	doa)Fufhfc4EGff1Au2Ln777777777777777777777777777777777777777777	success or wait	4	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_ITA.chm	0	23662	49 54 53 46 03 00 00 00 60 00 00 00 01 00 00 00 fd fd fd fd 09 04 00 00 10 fd 01 7c fd 7b fd 11 fd 0c 00 fd fd 22 fd fd 11 fd 01 7c fd 7b fd 11 fd 0c 00 fd fd 22 fd fd 60 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 78 00 00 00 00 00 00 00 54 10 00 00 00 00 00 00 fd 10 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 2e fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 54 53 50 01 00 00 00 54 00 00 00 0a 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 01 00 00 00 09 04 00 00 6a fd 02 5d 2e 21 fd 11 fd fd 00 fd fd 22 fd fd 54 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 50 4d 47 4c fd 07 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 01 2f 00 00 00 08 2f 23 49 44 58 48 44 52 01 fd fd 4d fd 00 08 2f 23 49 54 42 49 54 53 00 00	ITSF`|{"| {"`xT.ITSPTj].!"TPMGL //#IDXHDRM/#ITBITS	success or wait	3	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\foromtalers.Fid	0	28286	32 41 46 38 46 41 31 34 32 46 39 30 30 43 41 32 38 37 46 33 45 32 32 35 30 33 39 35 37 45 37 31 43 37 44 35 39 37 32 37 30 37 45 38 30 31 44 38 42 41 35 34 41 31 31 42 38 35 37 41 38 35 37 38 43 46 32 46 35 36 42 32 42 38 43 41 44 45 36 45 30 42 45 41 46 46 43 45 44 41 37 30 36 44 41 34 36 46 39 33 32 30 45 45 43 41 39 37 30 41 43 39 31 45 36 42 36 37 39 37 30 39 32 31 42 43 37 45 35 36 46 39 34 33 34 30 39 39 41 43 37 37 31 33 38 36 34 45 32 44 42 42 34 39 45 41 36 41 35 37 32 45 46 35 35 32 34 41 45 34 30 31 33 30 37 34 45 30 42 41 38 33 42 38 37 46 36 37 36 38 37 41 45 46 39 39 45 42 35 46 43 43 33 33 41 37 38 43 37 41 36 35 30 43 46 39 43 33 30 36 41 44 41 45 43 46 32 30 37 39 36 30 31 42 33 46 37 45 41 43 36 43 37 39 35 34 30 34 31 44 46 33 43 34 38	2AF8FA142F900CA287F3E22503957E 71C7D5972707E801D8BA54A11B857A 8578CF2F56B2B8CADE6E0BEAFFCEDA 706DA46F9320EECA970AC91E6B6797 0921BC7E56F9434099AC7713864E2D BB49EA6A572EF5524AE4013074E0BA 83B87F67687AEF99EB5FCC33A78C7A 650CF9C306ADAECF2079601B3F7EAC 6C7954041DF3C48	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 02 3f 21 fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 68 01 00 00 08 00 00 00 00 00 00 0a fd 01 00 00 20 00 00 00 fd 01 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 1e fd 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?!" 0h `	success or wait	5	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe	0	22479	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 4e 00 00 45 00 00 00 fd 00 26 02 0b 02 02 25 00 20 00 00 00 4a 00 00 00 02 00 00 fd 14 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 00 00 00 04 00 00 3e fd 00 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdNE&% J@>`	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\libLerc.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 26 09 00 56 00 00 00 fd 00 26 22 0b 02 02 25 00 fd 08 00 00 22 09 00 00 02 00 00 50 13 00 00 00 10 00 00 00 00 fd 59 03 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 09 00 00 04 00 00 50 7c 09 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd&V&"%"PYP|`	success or wait	26	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\libenchant-2.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0c 00 00 00 00 00 00 fd 00 00 7e 00 00 00 fd 00 26 22 0b 02 02 25 00 68 00 00 00 fd 00 00 00 04 00 00 50 13 00 00 00 10 00 00 00 00 10 56 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 50 01 00 00 04 00 00 fd 4f 01 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd~&"%hPVPO`	success or wait	3	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msvcr100.dll	0	30923	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 3a fd 79 fd 7e fd 17 fd 7e fd 17 fd 7e fd 17 fd 77 fd fd fd 7d fd 17 fd 7e fd 16 fd fd fd 17 fd 65 44 fd d4 fd 17 fd 65 44 fd fd 2b fd 17 fd 65 44 fd fd 4a fd 17 fd 65 44 fd fd fd fd 17 fd 65 44 fd fd 7f fd 17 fd 65 44 fd fd 7f fd 17 fd 65 44 fd fd 7f fd 17 fd 52 69 63 68 7e fd 17 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 1e fd fd 4d 00 00 00	MZ@!L!This program cannot be run in DOS mode.$:y~~~w}~eDeD+eDJeDeDeDeDRich~PELM	success or wait	33	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\system-shutdown.png	0	429	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 74 49 44 41 54 78 01 fd 53 05 6e 02 50 0c 2d fd 36 77 37 1c b2 38 3b 06 fd fd 23 fd 45 fd 5d fd 38 fd 0e fd fd 04 77 68 fd 4f fd 22 fd fd fd 0f fd fd 60 fd fd fd 7c 5e 6f 7b fd 05 2e 34 fd 52 20 10 fd fd fd fd 34 1b fd 46 7b fd 00 17 1a 68 fd fd 7d 6f fd 58 fd fd 64 fd fd fd 34 4d 0a a1 56 fd 45 4c 48 fd 61 41 03 2d fd 25 44 3c 1e fd 67 fd 54 6a 17 0a fd fd 0b 78 fd 0b fd fd 5b 45 28 14 fd 4a fd 7a fd fd 6e 37 19 0c 06 52 fd fd 58 fd fd 5c fd fd 44 17 fd cd 21 03 fd 68 35 1a fd fd fd fd 05 11 16 fd fd 01 1b 33 10 77 2f 02 fd 00 20 fd fd fd fd 4b fd 3b 63 fd fd fd fd 4d 4f fd 4f fd 60 02 fd fd 0e fd fd 0f fd 68 34 fd fd 64 fd fd 1d	PNGIHDRatIDATxSnP-6w78;#E]8whO"`^o{.4R4F{h}oXd4MVELHaA-%D<gTjx[E(Jzn7RX\D!h53w/K;cMOO`h4d	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg	0	335	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 34 20 31 20 63 20 2d 31 2e 36 36 30 31 35 36 20 30 20 2d 33 20 31 2e 33 33 39 38 34 34 20 2d 33 20 33 20 76 20 38 20 63 20 30 20 31 2e 36 36 30 31 35 36 20 31 2e 33 33 39 38 34 34 20 33 20 33 20 33 20 68 20 38 20 63 20 31 2e 36 36 30 31 35 36 20 30 20 20 33 20 2d 31 2e 33 33 39 38 34 34 20 33 20 2d 33 20 76 20 2d 38 20 63 20 30 20 2d 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"> <path d="m 4 1 c -1.660156 0 -3 1.339844 -3 3 v 8 c 0 1.660156 1.339844 3 3 3 h 8 c 1.660156 0 3 -1.339844 3 -3 v -8 c 0 -1.	success or wait	1	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO64747835 PDF.exe	unknown	512	success or wait	419	4060CA	ReadFile
C:\Users\user\Desktop\PO64747835 PDF.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\PO64747835 PDF.exe	unknown	4	success or wait	68	4060CA	ReadFile
C:\Users\user\Desktop\PO64747835 PDF.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\PO64747835 PDF.exe	unknown	4	success or wait	494	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\foromtalers.Fid	unknown	2	success or wait	1023	40275E	ReadFile
C:\Users\user\AppData\Local\Temp\RACOYIAN.hav	unknown	1048576	success or wait	1	734B2C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\HAAND	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\HAAND\Benfisken85	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\PARANTHRACENE	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Valeward72	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Valeward72\esc	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\DOMMERASPIRANTER	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\DOMMERASPIRANTER\ETHERIIDAE	success or wait	1	406407	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\HAAND\Benfisken85	detaljeprojektets	unicode	anginaerne	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\PARANTHRACENE	INTERPELLATION	dword	1	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Valeward72\esc	Transfixation98	binary	15 13 3C	success or wait	1	40251B	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\DOM MERASPIRANTER\ETHERIIDAE	internalising	binary	FF 8B CF 9F	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly