ID: 830399
Sample Name: rFACTURA_FAC_2023_1-1000733.PDF.exe
Cookbook: default.jbs
Time: 10:47:06
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

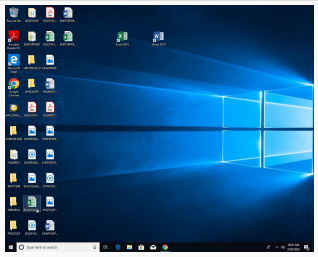
Windows Analysis Report

rFACTURA_FAC_2023_1-1000733.PDF.exe

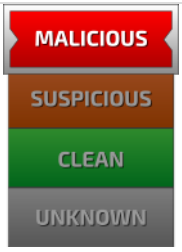
Overview

General Information

Sample Name:	rFACTURA_FAC_2023_1-1000733.PDF.exe
Analysis ID:	830399
MD5:	a6ef5ed777ba7..
SHA1:	f707bc0343f41…
SHA256:	878d710875b0…
Tags:	exe
Infos:	



Detection



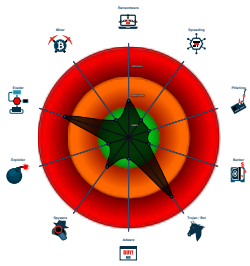
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Tries to detect virtualization through…
- Uses an obfuscated file name to hid…
- Uses 32bit PE files
- PE file does not import any functions
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Binary contains a suspicious time s…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- rFACTURA_FAC_2023_1-1000733.PDF.exe (PID: 5732 cmdline: C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe MD5: A6EF5ED777BA7369C2BB28E46B198BA6)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	**http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.782485165.0000000004480000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000000.00000002.782485165.00000000059F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

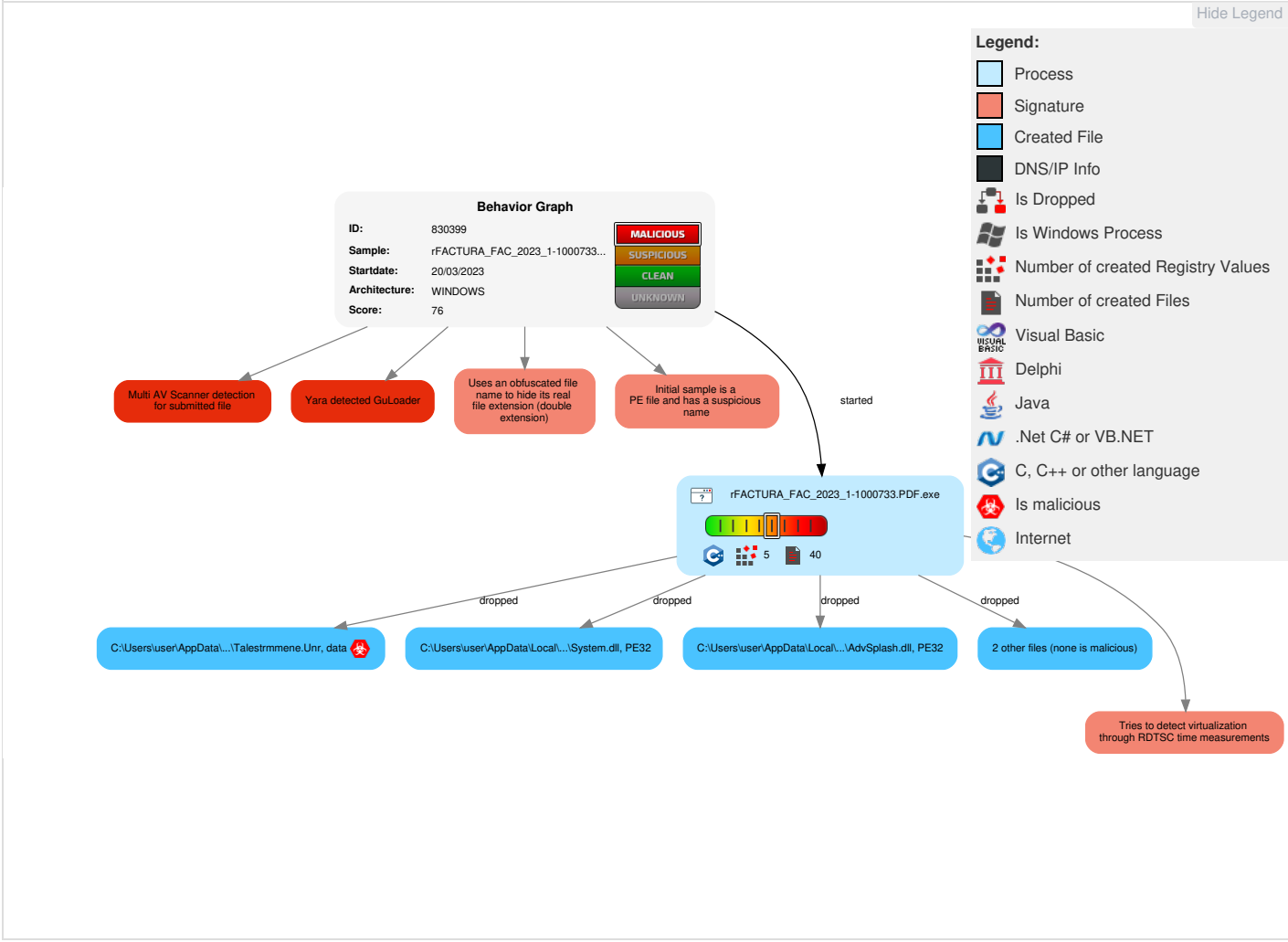
Malware Analysis System Evasion

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 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Windows Service	1 Access Token Manipulation	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
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

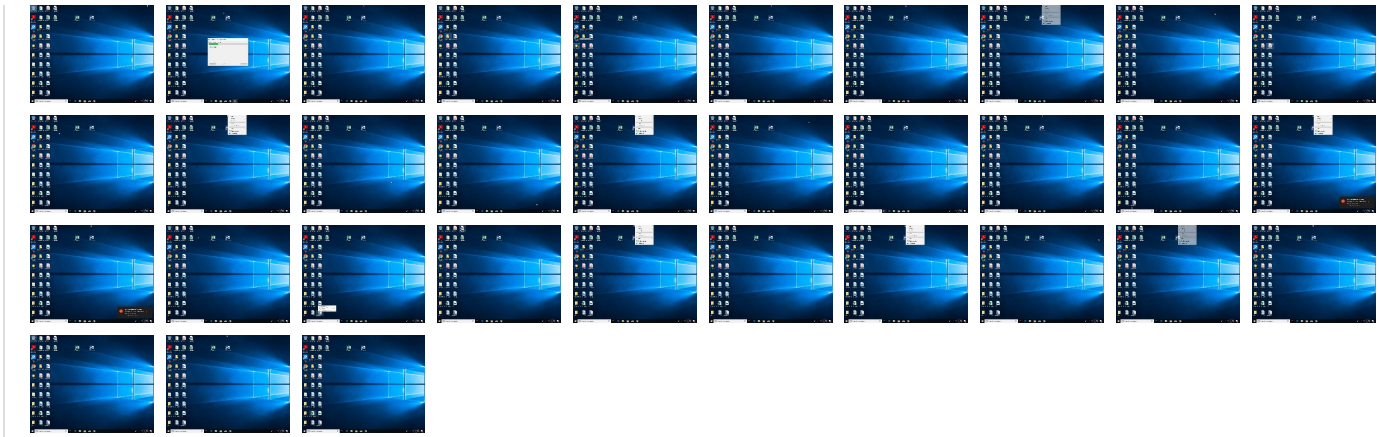
Behavior Graph



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
rFACTURA_FAC_2023_1-1000733.PDF.exe	20%	Virustotal		Browse
rFACTURA_FAC_2023_1-1000733.PDF.exe	5%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\System.Reflection.TypeExtensions.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\System.Reflection.Primitives.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#DerivativeWorks	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://crl.certum.pl/ctsca2021.crl0o	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://creativecommons.org/licenses/by-sa/4.0/	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Distribution	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://repository.certum.pl/ctnca.cer09	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://crl.certum.pl/ctnca.crl0k	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://subca.ocsp-certum.com05	rFACTURA_FAC_2023_1-1000733.PDF.exe	false	• URL Reputation: safe	unknown
http://creativecommons.org/ns#Attribution	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://subca.ocsp-certum.com02	rFACTURA_FAC_2023_1-1000733.PDF.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	rFACTURA_FAC_2023_1-1000733.PDF.exe	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://repository.certum.pl/ctnca2.cer09	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://creativecommons.org/ns#ShareAlike	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://https://github.com/dotnet/runtimeBSJB	rFACTURA_FAC_2023_1-1000733.PDF.exe, 00000000.00000002.780766390.000000000078900 0.00000004.00000001.01000000.00000003.sdmp, System.Reflection.TypeExtensions.dll.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://creativecommons.org/ns#Notice	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Reproduction	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://www.certum.pl/CPS0	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://creativecommons.org/ns#	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://https://github.com/dotnet/runtime	rFACTURA_FAC_2023_1-1000733.PDF.exe, 00000000.00000002.780766390.000000000078900 0.00000004.00000001.01000000.00000003.sdmp, System.Reflection.Primitives.dll.0.dr, System.Reflection.TypeExtensions.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830399
Start date and time:	2023-03-20 10:47:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	rFACTURA_FAC_2023_1-1000733.PDF.exe
Detection:	MAL
Classification:	mal76.troj.evad.winEXE@1/14@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.6% (good quality ratio 61%) • Quality average: 88.1% • Quality standard deviation: 22.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.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\Musicalises34\Coleman\Biarcuated\Nikotins61.sto

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	ASCII text, with very long lines (22842), with no line terminators
Category:	dropped
Size (bytes):	22842
Entropy (8bit):	2.691165226704503
Encrypted:	false
SSDEEP:	384:WHfXmxNkvIy6aQ+y57fZOKip2EuiP7Ecw8b:WHfWxNkvIy6axy57fAK82EuiP7Ecw8b
MD5:	27DC252D9E7B26BA6BF2C6D437997658
SHA1:	F81398F1F6FC24692BA8DF740CA2BF2AB73B27D6
SHA-256:	530F4F75B62CB7E1B585671E4F184AC9C667FC4335CDA4120D27136E6F4F0100
SHA-512:	473F5FED1BA3F62088A6ABE0D383EE9220DAABCB8524EFE8AC502B7503F4ACBA3DDAC69BBF1E046B5235C51129F2BF55F54C1D75285D7C5EE824C6DCA88D323D
Malicious:	false
Reputation:	low
Preview:	0008000000000000000F3008800000000000000D9D900D3000000BA000000444444003D000065000000666600003200A600F200007C7C0000FDFDFDFD00AE0000989898980000000A200000000B60000000000000001000000066007A00AEAE00393939393939000000C3C300000000000A9005F00002100FAFAFAFA003636007C00007000000053000000BCBC00AD000900000000000000D3000081810015151500000000D7D7D7D70000BABA0000D600001D1D00EDEDED000099990003 00ED008E000000000000000000B6B6000000E3E300000000010000A5A50000D10000D70000868600DFDFDFDF000007000000AD00D40000EDEDEDED00 000013000000C600C60000000007070000000069696900150090002121210000000004F4F4F0022000000B4B4006B6B000E000078000000003737007000000D300F2F2F2F200B5B5B50021000000BA00990042001C1C002E000000003E0000BC000000000000000000002828000000D4D4000B00EB0000CE001D1D00F200000009090900140000003F3F3F00000000009E9E0000000A0A00DEDEDEDEDE00000000A6A6001E0000007D0000000000D2000001000000505000080D70000969696000000A3A30000B9B900000F000050505000000000360020200000000000000000000D9D9D90075757500D9D9D900999900080000000D6D6D600747474

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\System.Reflection.TypeExtensions.dll

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32368
Entropy (8bit):	6.393948275188786
Encrypted:	false
SSDEEP:	384:yWweWqlXnYcLpSfX0lawccfNXLWrdzy+A2jc2EPLNtAf/uPHRN7AJ/AlGseC62c:EqlXYcgEAwcc17Wc+bj+PLHuMU/xjx2c
MD5:	F2A123183E106BB1CF19376A8079D171
SHA1:	2B96296BE92D5F2EF7C59A70858AF4CAABC99A9D
SHA-256:	896D4ED138C35ECF19AE432380096562872EAB103F7E352C15D214FD875B337A
SHA-512:	FCA6A89EFB16780A06CD25A55638882970F03E1535180A0E463AF9794184B04EB345CF29B12D4F261094E04A584E9225A7AD36A62631227451059F64A77B3C67
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....[....." .....P..... ..`...@.....@..... .....<.....Z..p$...p.....T.....H.....text....N.....P..... ..`.data.....`.....R..... .....@....reloc.....p.....X.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F. i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...Z.!...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.e.f.l.e.c.t.i.o.n...T.y.p.e.E.x.t.e.n.s.i.o.n.s.....L... ..C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j.!...F.i.l.e.D.e.s.c.r.i.p.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\System.Reflection.Primitives.dll

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14952
Entropy (8bit):	6.599053939997928
Encrypted:	false
SSDEEP:	192:mrlnC6xxk2R5Ws+Wql73WOL8/pCuPHnhWgN7aoWTF6lI+XqnajlkEv:6nbW2R5Ws+Wql7//uPHRN7SIImlqW
MD5:	EDA04E04EBC0EBF7F8BBF30C4DAE6DE3
SHA1:	7BC4D50E6EEC7F04A9272BFEE4E4DB6F278DBE63
SHA-256:	F3E55CB3ADFA93F563B09114D93062E680AB0864C220491458FBE151798B862F
SHA-512:	7027DA3404675596B71394B660E600DA12C0750895F624776362167869760555EE9990699FFC9E4407301FC9437B2F638E2734B8BDEF3C7054990FD5A9C86550
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."!..0.....^+... .....@.. ....`.....+..K....@.....h$...`.....T*..8..... ....H.....text...d.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....@+.....H..... .....P .....H>.s..X.\...3V...?G../..3q..l.L.....qKy6b..u"HO...JmYQ.....J...*S..".R..=1RY. ....\?.&dM.....@'J.j.:.'.A.../.....I.BSJB.....v4.0.30319.....`.....#~.....#Strings.....#GUID.....#Blob.....3.....3.....@..... .Y.....`.....g...?.g.....g...y.g.....g.....g.....g...`.g...m.g.....

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	224632
Entropy (8bit):	7.3469254146259635
Encrypted:	false
SSDEEP:	3072:WQyWMNv4aM4lqtUHXAxcNxBrQeb8hlosuRUVGiyKrFyPlWUUVkUiXPQW/NhrsPPR:lWEbtUAixGhlo2l+hyEUJXVFm0XQ
MD5:	D2BE5DE19D44424CCB3F89510938FB53
SHA1:	B98E5FD30E1DE7437187787AFE48AD516223E01F
SHA-256:	0796783FC019D2AD4F01FF7AF14C24A9D3CFBAAB2BB9B44945231A46B6774D2B
SHA-512:	6E54E8C97F5A10921DAD011AAD9FBBA1D4D622CF78F4C977A366EF6C7C49B35552A6100BFAFCC4464B34B351CC200AD9EE12406DDE37FC96C2614BD24A5D053
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr, Author: Joe Security
Preview:	...>.....).....OOOO.....###.GG.....BB.....T.....#....=.....{{.....++.....V.....)._.@.....@@@@...```.....*.....+..... ....f.....7.....9.....".iii....?..88.F.....P.....).....Z.....$.....,.....BBB...{{.UU....Q.....@@.....'''''.....ttt.....qq.....vv.....,..... .....?..00....W.BB...r.....55.....8.9...--.....{{.....E.....qqqqq..___.....H.....tt.....0.....WW.....X.55..y.....mm.....~.D.....(.@@....{{{{{{{{{.. .....oo.....SSS..V...]]....33333....7..>.d.????.....@@.....j.8.TTTT..9.....BB.....C.....II...).....@@.....@@@..&&.....z.....ppp.....4.z.....|.....++...\ \\....".....).....v.....2.I.hh.....I.....9.....hhhh

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\battery-level-90-charging-symbolic.svg

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	6689
Entropy (8bit):	5.135211840989561
Encrypted:	false
SSDEEP:	192:VkjcMIy2+X2l2F2C2G2fH7y8cQaVB2nnuy1FQOcQaVv2q22L2k2s:mjcM7u8xaV8nnL1FQOxaVu6
MD5:	C96D0DD361AFC6B812BDDD390B765A26
SHA1:	71081F096719CAA70B9BAEF86FE642635D8E2765
SHA-256:	6690799E5FA3FB0DD6CCE4BAC5AA1607C8A6BB16507854A87520C7DE53052E1B
SHA-512:	7C73BC880A9401C64AB0571957B414180C1B94137C7BC870BA602979E7A990640A37991CB87A40BC7E5942A37FDA25EFC58C759C00F4344BA3D88B9AA64182D
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>.<svg. xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:cc="http://creativecommons.org/ns#". xmlns :rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#". xmlns:svg="http://www.w3.org/2000/svg". xmlns="http://www.w3.org/2000/svg". width="16". version="1.1". style ="enable-background:new". id="svg7384". height="16.000036">. <metadata. id="metadata90">. <rdf:RDF>. <cc:Work. rdf:about="">. <dc:format>i mage/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <c c:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/li censes/by-sa/4.0/">. <cc:permits. rdf:resource="http://creativecommons.org/ns#Reproduction" />. <cc:permits. rdf:resource="htt

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\colorimeter-colorhug-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	227
Entropy (8bit):	6.604776901672149
Encrypted:	false
SSDEEP:	6:6v/lhPysE9Xj1F/bkqdXujFErL4MlmATQZu22F+p:6v/7kR7/bjd8Kgm2Q/2y
MD5:	7843C38CC42C6786B3373F166AF10172
SHA1:	BA0163109D9B641B1312230B3F62E1E10A61AA5E
SHA-256:	E3AF1293F8E8AB5C81300196AF55A7C15D5608291D46A2B86D4255910A7D0E59
SHA-512:	B1D3DF6A0A8CACD729CD9A2FD5AB0F74ED611270FA172CDBEB13D46FA71DD5CC5540A2FBFDB6C3004E652D317C8FAD4EC3AE437DF1C082B629870A33CC6D34F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1..P.....#.bae....^.^K/fek+.....X.....gfw....\.D/..b...a.4..$.....H#....o8...}..6.K.....Xc.$ ..'.1.2..vu.../O..>V.....CD....< ....w.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\media-playlist-consecutive-symbolic.svg

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1329
Entropy (8bit):	4.950241534342892
Encrypted:	false
SSDEEP:	24:t4Cp/YHyKbRAecFxVrGDT/Gfd8hTdyKbRAecFxVrGDT/bNxNxZrGQ:9YHNtAecFmDT/s8hdNtAecFmDT/j3YQ
MD5:	021A9F00A28C9D496E490AE951E8EF12
SHA1:	F8A6392065D07BAC72E138B0E47A24FFDCCEE74B
SHA-256:	B420561770B77FCB47F69B6198B34B11155535F8A2E907BC4A0998CE74AFD340
SHA-512:	7F4F2D904EA968BF68E35E0D7F1EAE9718234757D1989879996BFB49D9C447F67544CB0E1C441FD6539D58B5F2C6ACA7E9E0208738C235D9AF0C093511760212
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M1.018 7v2H14V7z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" color="#bebebe" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M11.99 4.99a1 1 0 00-.697 1.717L12.586 8l-1.293 1.293a1 1 0 101.414 1.414L15.414 8l-2.707-2.707a1 1 0 00-.717-.303z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decorati

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-offline-symbolic.svg

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1155
Entropy (8bit):	5.154592341044034
Encrypted:	false
SSDEEP:	24:t4CpQyhEXQDWu4AeWrGMyRQJaPahrGDfJcghSvOqIIQX6e4AeWrGMyp:vhjDWu4Ae3M5wSgDDontqe4Ae3MO
MD5:	EFB3C780BC44B346B50B1F0DC6CF6D0F
SHA1:	472B0EDD1C4C3092BC7C4DF934ABE126885B1780
SHA-256:	990859D3B2C830E23EC276BF1D38A38EE1BA3D89BF04CB138107E4CDE31167B5
SHA-512:	5B9C96F146C6A065C89172D02BDE8020876DC9C78859AD2B8B9529C615215F88BA85C2789544F5C5A247C148BB52FE4B5FCA325E7EAC4826D31A0365A0B8BCBE
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M5 7c-.31 0-.615.09-.812.281L.594 11l3.656 3.719c.198.19.44.281.75.281h1v-1c0-.257-.13-.529-.312-.719L4.406 12H9s1 0 1-1c0 0 0-1-1-1H4.375l1.219-1.281C5.776 8.529 6 8.257 6 8V7z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible" opacity=".35"/><path d="M11 11h1.375l1.125 1.094L14.594 11H16v1.469l-1.094 1.062L16 14.594V16h-1.438L13.5 14.937 12.437 16H11v-1.406l1.063-1.063L11 12.47z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M11 9c.31 0 .615-.09.813-.281L15.406 5 11.75 1.281C11.552 1.091 11.31 1 11 1h-1v1c0 .257.13.529.313.719L11.593 4H7c-.528-.007-1 .472-1 1s.472 1.007 1 1h4.625l-1.219 1.281c-.182.19-.406.462-.406.719v1z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:star

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-wireless.png	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	891
Entropy (8bit):	7.745720384539504
Encrypted:	false
SSDEEP:	24:d4qWCHdkXfUZEcO5Mkli416cOQSkye9V+:d4qnHd8Mkli4Dpb6
MD5:	5AF147D26AD399F83825377F04FD56A1
SHA1:	B378A498B0DB8114C794E21D533E80CEBE5DDE04
SHA-256:	6147A091847FCC9D9EDB22E655C4FC9DE6632C76D4252350400FA286F9791109
SHA-512:	EEC16DE49A4698FE4F03F841FBCF045FBBDC9D634EB73ED35DB544B6DB4BC0135CD8E1DF102FD1E8BDE9FC75380948B4C0459685EE2C21858D645B7973759 A6
Malicious:	false
Preview:	.PNG.....IHDR.....a...BIDATx.m.S.%9...$U.Fkl.y].m.6.m.F..5*g;k}.....P.....~u.....M.....M.q.....\|OM>....:?>.X7.U..j.v..?...e....>.Jk.&.{.[=.....t.d.....4.D... V....b..s.L.....Jg,..=V..@.n.....Rqv...._....B.h.;l....A....r.ap....N...1./.O.2.u7#..../....o..*..O...[..X,<. .....@v.....t...H..Rf..C?q..8.HB.!{K..N.....t..5..1d.+.....).....pL.5.R..=....jC". ...t6.BA.)....xZ..d..^W~yU...ya.....U/...VA.r.....r.U....["D.).8..iO<..[.....t.e9S...K8!....K..&p..Y2l.....".P8:..v..0....zd.."....O?+^.. =..b....t..K../.....?.?5...c.[.f.nP.P.o....7..k..t.?P(..O >.H~...n..jh.'..]..SC.5M.....'.}.n..'...t..9..c*...Ki...t..1z..N.q...w.w..y..W...K7x.^..p....j...%..3.\|.....x...G.\|~..a.o.N.<.....wK...]..u.....`...(z.B!.?q.b..u..$(.#1..N...b.u...@h...|.w..g.. ..}i....?~.....1~...l..]h.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\preferences-desktop-font-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	225
Entropy (8bit):	6.596645802250635
Encrypted:	false
SSDEEP:	6:6v/lhPysi5NuhsPwRngRfPq/3+phjSfVsup:6v/7thstJACSNsc
MD5:	F894266AB6A933B2FDA751E6490C319A
SHA1:	2D2D3635198FEEFCB64D1D6B3CDCCDC4EA3DF4B0
SHA-256:	95F533585B4C61936C369557B3B7E397E56545A4C9DB9A5BDDD0E9ABB7A7F7E7
SHA-512:	977ED04753C3CB2B883D03A2A55001F6FCC8617DC3060B6C25AB7E5C691C3F76049E7DEADC7F6567AB7E8DC8492DE2874E8E632CF3EAD7B39ABC8CC98D331 42
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1..@.E...".u.`..#.v.,r.[..1$..]B.@6.,,.e.....fwg...._)9.....y..[n...t.$g..:...P....@k.q.....W.. .PY.$z..x....t..(-~!.0$:P.t.....`..... .Ba..Y.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\task-due-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	263
Entropy (8bit):	6.731374842054556
Encrypted:	false
SSDEEP:	6:6v/lhPysw9TXm0RZC/8xhbPgfdSwj4vw29OjuAO4+ZvYNVp:6v/7QVXm0a/8xhbPgfdSBvNYn2ZvYd
MD5:	003B524806C1CA654CAC6ED2EB883E1B
SHA1:	F6F6ACA125DC4DB3B33378404017B5EE7D21D334
SHA-256:	2899E53769FA741E2C0675A2C69D2C246A8F34601BEE58DD66B16261005962A9
SHA-512:	AA905997F9CE39F039E33C4CCA167C0137775D91B4929D918528BA00B92737C448EC46D91A4221644CCC00D1FCAA403AFF83F07276BAB6FD80D4B9E88E652F8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...K..1.D.....g.e=.x.....[]....Y$J'..`.@.S)R.4.q.D.K....x..%..0>~.;}..^.X....Lt.f!..K.....D.&,.7,..BM..t@..}N..o.?.....Hv.J...(..r.. ..)L... .&..dT<..1y...X..X.....q...p..p.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\window-close.png	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	337
Entropy (8bit):	7.143668471552015

Encrypted:	false
SSDEEP:	6:6v/lhPWFmX9Ckymx8BZhCjO5QO6MsHqd+K/eBDQeU2oG9xqgjp:6v/7K0omx8yOqVtHH1U2oGR
MD5:	7FBFE5B0A7AD2A67AACFD8481F8DCA01
SHA1:	21BABB6B7EC4746835DB43DC6A69A4AF0EFECA2D
SHA-256:	0B4CD789E087F712F131FACCD754DC461774498DF3CA19B346D461D18A0AE622
SHA-512:	3A8F0D9653301F789A0588E848C40FFC92394461BF70A3421ABC85647F2C115948134FE9E161D055A11D200536356A15677D9C0E645346D27E122001F67FE22B
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx..S.r.P..=7.cw.....W.m...=.....V....I...K.?#@D.0G.....R.rF..^$....p..b..f.<.T.z..... +..3#.v.K...$....pT.j.....[.....r..p....O.2.Y.T.,.....==...9{/.. .T./....Qa...3%....5...xmkI.7.1..P,g.%y..J..#^.e..I(.%jzI..#../..49...*..?#..I. =~..E.,MN@.....`...../...=.-...1....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsa150D.tmp\AdvSplash.dll

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.496995234059773
Encrypted:	false
SSDEEP:	96:1IUNaXnnXyEIPtXvZhr5RwiULuxDtJ1+wolpE:1lx3XyEwXvZh1RwnLUDtf+I
MD5:	E8B67A37FB41D54A7EDA453309D45D97
SHA1:	96BE9BF7A988D9CEA06150D57CD1DE19F1FEC19E
SHA-256:	2AD232BCCF4CA06CF13475AF87B510C5788AA790785FD50509BE483AFC0E0BCF
SHA-512:	20EFFAE18EEBB2DF90D3186A281FA9233A97998F226F7ADEAD0784FBC787FEEE419973962F8369D8822C1BBCDFB6E7948D9CA6086C9CF90190C8AB3EC97F4C 38
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....`$..E.... ..d.....@..$..... ..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsa150D.tmp\System.dll

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8QII972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.02530526585537
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:	rFACTURA_FAC_2023_1-1000733.PDF.exe

File size:	431872
MD5:	a6ef5ed777ba7369c2bb28e46b198ba6
SHA1:	f707bc0343f41d95f57e776a9f85f6a2c5791aa7
SHA256:	878d710875b07ec61bef0b198ba67bf81ad0730a3a483d5762cd18e13fb4b525
SHA512:	3b0bbbf4199dfc669a75a8fb62cfa55423e2331358f43057219ee2a4099cc9c2b007d85b2cb1b6cd9c64d8d8421575690bed95556ca788cf13d6a53c96b3a2eb
SSDEEP:	6144:B6bAcJvkzKmPPzS58G93IuZCBabjYBNwmlJ8kUEe/oqBaH0NxsvLg/nkrIak7r8m:a7ubCHICiwkBySs/vBGwxs0vh7rXN
TLSH:	B194F161BFDBE857D02278B4A09ADE1E5E74EF14A249E307F3B139ACE5752513C1B202
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....uY.....d....:....

File Icon

Icon Hash:	20c4f8f8e8f0f24c

Static PE Info

General

Entrypoint:	0x403350
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759518 [Mon Jul 24 06:35:04 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Giordano@Agencies.ano, OU="Desidiose Haarvkstens ", O=Percussion, L=Mccomb, S=Mississippi, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 1/8/2023 6:53:11 PM 1/7/2026 6:53:11 PM
Subject Chain	• E=Giordano@Agencies.ano, OU="Desidiose Haarvkstens ", O=Percussion, L=Mccomb, S=Mississippi, C=US
Version:	3
Thumbprint MD5:	B7600E9E947B9005922C17012BBF815F
Thumbprint SHA-1:	F61732487D62043541218B18386BFA3513D9C7CF
Thumbprint SHA-256:	C6510EBAF8763805CB5E0AAB32A94AEEFD9E39180B9A6D5F85E0272807031574
Serial:	1B9B07C3A599FD0DBF3CF80F5B8149857D2F3BA7

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h

Instruction
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax
je 00007F0591104523h
push ebx
call 00007F05911077B9h
cmp eax, ebx
je 00007F0591104519h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F0591107733h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F05911044FCh
push 0000000Ah
call 00007F059110778Ch
push 00000008h
call 00007F0591107785h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007F0591107779h
cmp eax, ebx
je 00007F0591104521h
push 0000001Eh
call eax
test eax, eax
je 00007F0591104519h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

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

Data Directories			
Name	**Virtual Address**	**Virtual Size**	**Is in Section**
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84fc	0xa0	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d0000	0x28268	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x67500	0x2200	.data
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	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a9000	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3d0000	0x28268	0x28400	False	0.3355129076086957	data	4.767250735975199	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d0310	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x3e0b38	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x3e9fe0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x3ef468	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x3f3690	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x3f5c38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x3f6ce0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x3f7668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x3f7ad0	0x100	data	English	United States
RT_DIALOG	0x3f7bd0	0xf8	data	English	United States
RT_DIALOG	0x3f7cc8	0xa0	data	English	United States
RT_DIALOG	0x3f7d68	0x60	data	English	United States
RT_GROUP_ICON	0x3f7dc8	0x76	data	English	United States
RT_MANIFEST	0x3f7e40	0x423	XML 1.0 document, ASCII text, with very long lines (1059), with no line terminators	English	United States

Imports

DLL	Import

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

Possible Origin

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

Network Behavior

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

Statistics

No statistics

System Behavior

Analysis Process: rFACTURA_FAC_2023_1-1000733.PDF.exe PID: **5732**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:48:04
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
Imagebase:	0x400000
File size:	431872 bytes

MD5 hash:	A6EF5ED777BA7369C2BB28E46B198BA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000000.00000002.782485165.0000000004480000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.782485165.00000000059F0000.00000040.00001000.00020000.00000000.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	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsk1412.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DBF	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsa150D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DBF	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	40581B	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	40581B	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	40581B	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	40581B	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	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsa150D.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	4057DB	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\AdvSplash.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	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	3	40581B	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	3	40581B	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	3	40581B	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	3	40581B	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	3	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\System.Reflection.Primitives.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nikotins61.sto	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\System.Reflection.TypeExtensions.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\battery-level-90-charging-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\colorimeter-colorhug-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\media-playlist-consecutive-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-offline-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-wireless.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\preferences-desktop-font-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\task-due-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\window-close.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405D7D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsk1412.tmp	success or wait	1	403601	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsa150D.tmp	success or wait	1	40599C	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\AdvSplash.dll	0	6144	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 2b fd 59 16 6f fd 37 45 6f fd 37 45 6f fd 37 45 6f fd 36 45 46 fd 37 45 fd fd 6a 45 66 fd 37 45 3b fd 07 45 6d fd 37 45 fd fd 33 45 6e fd 37 45 52 69 63 68 6f fd 37 45 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 08 fd 75 59 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 0a 00 00 00 0a 00 00 00 00 00 00 60 11 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$+Yo7Eo7Eo7Eo6E F7EjEf7E;Em7E3En7ERicho7EPELuY!`	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr	0	32768	00 fd 00 3e 00 00 00 14 00 1b 00 00 29 00 fd 00 fd 00 fd 00 4f 4f 4f 4f 00 19 19 19 00 fd fd 00 00 fd 00 00 fd 00 00 23 23 23 00 47 47 00 02 02 00 00 00 42 42 00 00 00 fd 00 00 00 fd 00 00 54 00 12 00 fd 00 00 00 23 00 00 00 00 3d 00 00 00 00 fd 00 00 00 00 00 00 7b 7b 00 09 09 09 09 00 00 2b 2b 00 00 00 00 00 fd 00 00 00 00 56 00 00 fd fd fd fd 00 00 29 00 5f 00 40 00 fd 00 00 00 fd fd fd fd 00 00 00 00 fd 00 40 40 40 40 00 00 00 60 60 60 00 00 fd fd fd 00 00 00 2a 00 fd fd 00 0b 0b 00 00 00 00 00 fd 00 00 00 00 0a 0a 0a 0a 00 00 00 00 00 00 fd fd 00 00 04 00 00 00 fd fd fd 00 fd fd fd fd fd fd 00 fd 00 00 fd 00 fd 00 00 00 fd 00 2b 00 00 fd fd fd 00 fd fd 00 00 66 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 fd 00 1b 1b 00 01 01 00 37 00 fd fd fd	>)OOOO###GGBBT#={{++V)_@@@@@```*+f7	success or wait	7	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\System.Reflection.Primitives.dll	0	14952	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 50 45 00 00 4c 01 03 00 fd fd 0a fd 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 30 00 00 0c 00 00 00 08 00 00 00 00 00 00 5e 2b 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd fd 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL"!0^+ @ `	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nikotins61.sto	0	22842	30 30 30 38 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 46 33 30 30 38 38 30 30 30 30 30 30 30 30 30 30 30 30 30 30 44 39 44 39 30 30 44 33 30 30 30 30 30 30 42 41 30 30 30 30 30 30 34 34 34 34 34 34 30 30 33 44 30 30 30 30 36 35 30 30 30 30 30 30 36 36 36 36 30 30 30 30 33 32 30 30 41 36 30 30 46 32 30 30 30 30 37 43 37 43 30 30 30 30 46 44 46 44 46 44 46 44 30 30 41 45 30 30 30 30 39 38 39 38 39 38 39 38 30 30 30 30 30 30 30 30 41 32 30 30 30 30 30 30 30 30 42 36 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31 30 30 30 30 30 30 30 36 36 30 30 37 41 30 30 41 45 41 45 30 30 33 39 33 39 33 39 33 39 33 39 33 39 30 30 30 30 30 30 43 33 43 33 30 30 30 30 30 30 30 30 30 30 41 39 30 30 35 46 30 30 30 30 32 31 30 30 46 41 46 41 46 41 46 41 30 30 33 36 33 36 30	00080000000000000000F300880000 0000000000D9D900D3000000BA0000 00444444003D000065000000666600 003200A600F200007C7C0000FDFDFD FD00AE00009898989800000000A200 000000B60000000000000010000000 66007A00AEAE003939393939390000 00C3C30000000000A9005F00002100 FAFAFAFA0036360	success or wait	1	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\System.Reflection.TypeExtensions.dll	0	32368	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 50 45 00 00 64 fd 03 00 fd 5b fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 50 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd fd 00 00 03 00 60 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd[" P`@@	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\battery-level-90-charging-symbolic.svg	0	6689	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0a 3c 73 76 67 0a 20 20 20 78 6d 6c 6e 73 3a 64 63 3d 22 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 65 6c 65 6d 65 6e 74 73 2f 31 2e 31 2f 22 0a 20 20 20 78 6d 6c 6e 73 3a 63 63 3d 22 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6e 73 23 22 0a 20 20 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 0a 20 20 20 78 6d 6c 6e 73 3a 73 76 67 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 0a 20 20	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cc="http://creativecommons.org/ns#" xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:svg="http://www.w3.org/2000/svg"	success or wait	1	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\colorimeter-colorhug-symbolic.symbolic.png	0	227	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 31 0a fd 50 10 04 17 fd fd fd 23 08 62 61 65 fd 01 fd 16 5e fd 5e 4b 2f 66 65 6b 2b fd fd 07 fd fd fd 13 fd 58 fd fd 18 fd 03 fd fd 81 0f fd 7f 67 66 77 fd fd 10 1b 5c fd 44 2f fd fd 62 fd 09 98 61 fd 34 fd fd 24 fd 0c 17 fd 0a fd 0c 03 48 23 01 09 fd fd 6f 38 fd 0c 01 7d fd fd 36 fd 4b fd fd fd 0e fd 58 63 fd 24 20 fd 02 27 fd 31 fd 32 f1 fd 76 75 fd fd 02 2f 4f fd fd 3e 56 fd 0a fd fd fd fd 43 44 13 fd fd 11 3c 00 fd 1e 1b 77 1e fd 0a fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT81 P#bae^^K/f ek+Xgfw\D/ba4$H#o8}6K Xc$ '12vu /O>VCD<wIENDB`	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\media-playlist-consecutive-symbolic.svg	0	1329	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 2e 30 31 38 20 37 76 32 48 31 34 56 37 7a 22 20 73 74 79 6c 65 3d 22 6c 69 6e 65 2d 68 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 6c 69 67 61 74 75 72 65 73 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 70 6f 73 69 74 69 6f 6e 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 63 61 70 73 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 6e 75 6d 65 72 69 63 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M1.018 7v2H14V7z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-vari	success or wait	1	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-offline-symbolic.svg	0	1155	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 35 20 37 63 2d 2e 33 31 20 30 2d 2e 36 31 35 2e 30 39 2d 2e 38 31 32 2e 32 38 31 4c 2e 35 39 34 20 31 31 6c 33 2e 36 35 36 20 33 2e 37 31 39 63 2e 31 39 38 2e 31 39 2e 34 34 2e 32 38 31 2e 37 35 2e 32 38 31 68 31 76 2d 31 63 30 2d 2e 32 35 37 2d 2e 31 33 2d 2e 35 32 39 2d 2e 33 31 32 2d 2e 37 31 39 4c 34 2e 34 30 36 20 31 32 48 39 73 31 20 30 20 31 2d 31 63 30 20 30 20 30 20 30 2d 31 2d 31 2d 31 48 34 2e 33 37 35 6c 31 2e 32 31 39 2d 31 2e 32 38 31 43 35 2e 37 37 36 20 38 2e 35 32 39 20 36 20	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M5 7c-.31 0-.615.09-.812.281L.594 11l3.656 3.719c.198.19.44.281.75.281h1v-1c0-.257-.13-.529-.312-.719L4.406 12H9s1 0 1-1c0 0 0-1-1-1H4.375l1.219-1.281C5.776 8.529 6	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-wireless.png	0	891	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 03 42 49 44 41 54 78 01 6d fd 53 fd 25 39 14 fd fd 24 55 fd 46 6b 6c de 79 5d f6 6d fd 36 b6 6d fd 46 fd fd 35 2a 67 3b 6b 7d fd 04 11 fd fd fd fd 1d 50 fd fd fd 1f 0f fd 7e 75 fd fd fd fd fd 03 fd 1c fd fd 37 0e fd fd f5 fd 4d 03 fd a3 fd 1b fd 4d fd 71 fd fd fd fd 49 fd 7c 4f 4d 3e fd fd 49 fd 3a 3f 3e fd 58 37 15 55 fd fd 6a fd 76 fd fd 3f fd fd fd 65 fd 1f fd fd 3e fd 4a 6b fd 26 92 7b fd 5b 3d 9c fd 13 fd fd fd 74 fd 64 fd fd fd fd fd 34 fd 44 fd fd fd 56 fd 07 40 fd 62 fd fd 73 fd 4c fd fd fd fd fd 4a 67 2c fd 02 3d 56 fd fd 40 fd 6e fd 05 fd 58 fd fd 52 71 76 fd fd fd	PNGIHDRaBIDATxmS%9$UFkly]m6mF5*g;k}P~uMMq|OM>:?>X7Ujv?e>Jk&{[=td4DVbsLJg,=V@nRqv	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\preferences-desktop-font-symbolic.symbolic.png	0	225	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd 31 0a fd 40 10 45 fd fd fd 22 fd 75 2e 60 fd fd 23 fd 76 11 2c 72 03 5b 0f fd 31 24 fd fd 5d 42 fd 40 36 fd 2c 2c 1f 65 fd fd fd 0f 1f 66 77 67 fd fd fd fd 5f 29 39 fd 03 fd fd fd fd fd 79 04 2e 5b 6e fd fd fd 74 fd 24 67 05 fd 3a fd fd 13 50 03 fd 16 15 40 6b 09 71 fd 02 fd fd 0a fd 57 12 03 20 fd 50 59 fd 24 7a fd 0c 78 fd fd fd fd 74 fd 00 28 2d 7e 21 1f 30 24 3a 50 fd 74 fd 13 fd 01 fd 04 60 06 1a 00 1d fd 0b 45 42 61 fd 1c 59 fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT81@E"u.`#v,r[1$]B@6,,efwg_)9y.[nt$g:P@kqW PY$zxt(-~!0$:Pt`BaYIENDB`	success or wait	1	405E1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\task-due-symbolic.symbolic.png	0	263	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 4b 0a 02 31 10 44 fd fd 08 11 15 04 67 fd 65 3d fd 78 0d fd fd 11 fd fd 5b 5d fd 11 19 fd 59 24 4a 27 fd fd 60 fd 40 fd 53 29 52 fd 34 fd 71 05 44 fd 4b fd fd fd 01 78 02 af 25 fd 16 30 3e 7e 00 3b 7d fd 05 5e fd 58 13 10 fd 05 4c 74 fd 66 21 fd 19 4b fd fd fd 00 fd 44 fd 26 2c fd 37 2c 0a fd 42 4d fd 08 74 40 03 fd 7d 4e fd fd 6f 11 3f 16 ac fd 10 fd 48 76 fd 4a 02 16 fd 28 fd cf 72 7f fd 20 fd fd 29 4c 11 16 fd fd 26 fd 0b 64 54 3c 03 fd 31 79 fd fd 1e 58 03 fd 58 fd fd fd fd fd 4f fd fd 1e cd fd fd fd 1e 71 00 fd fd 70 48 fd 70 fd 00 00 00 00	PNGIHDRasBIT|dIDAT8 K1Dge=x[]Y$ J'`@S)R4qDKx%0>~;}^X Ltf!KD&,7,BMt@}No? HvJ(r)L&dT<1yXXqpp	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\window-close.png	0	337	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 18 49 44 41 54 78 01 fd 53 03 72 fd 50 18 fd 3d 37 fd 63 77 0e fd 1b fd fd 57 fd 6d 1b 17 fd 3d 0c fd fd fd fd fd 56 fd fd fd fd 49 fd 10 fd 4b fd 3f 23 40 44 0d 30 47 fd fd fd fd 17 11 52 fd 72 46 18 fd 5e 24 00 fd fd fd 70 fd 2d 62 fd fd 66 fd 3c fd 54 4b 7a 2e fd 1f fd 12 fd 12 fd fd 20 2b fd fd 33 23 fd 76 fd 4b fd 1b fd 24 2e 1b fd fd 70 54 fd 6a 07 fd fd fd fd 5b fd fd fd 08 fd fd fd 72 fd 1b 70 fd fd fd 7f 4f fd 32 fd 59 fd 54 fd 2c 00 fd fd fd fd fd 3d 3d fd fd 05 39 7b 2f fd fd fd 54 1b 2f fd 8a fd fd 51 61 fd fd 18 33 25 fd 2e 02 fd 35 fd 0b fd 78 6d 6b 49 fd 37 05 31 39 fd 50 2c 67 fd 25 79 fd 1f 4a fd 1c 23 5e	PNGIHDRaIDATxSrP=7c wWm=VIK?#@D 0GRrF^$pbf<Tz. +3#vK$.pTj[rpO2 YT,==9{/T/Qa3%.5xmkI7 1P,g%yJ#^	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\nsa150D.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELuY!	success or wait	1	405E1D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe	unknown	512	success or wait	396	405DEE	ReadFile
C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe	unknown	4	success or wait	2	405DEE	ReadFile
C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe	unknown	4	success or wait	37	405DEE	ReadFile
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nikotins61.sto	unknown	2	success or wait	1023	4026B6	ReadFile
C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe	unknown	4	success or wait	2	405DEE	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\InstallDir32	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Micos	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Micos\Irises	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Micos\Irises\Kandissens	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Micos\Irises\Kandissens\Raceblanding	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hermeneutics	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hermeneutics\Ophjedes	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hermeneutics\Ophjedes\Amtsraadsmedlemmet	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Replyingly	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Replyingly\Avnbgen	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Replyingly\Avnbgen\Spisekamrenes	success or wait	1	406129	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\Fetichry	success or wait	1	406129	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\InstallDir32	Path	unicode	256	success or wait	1	40246F	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Micos\Irises\Kandissens\Raceblanding	Sulphammonium164	dword	0	success or wait	1	40246F	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hermeneutics\Ophjedes\Amtsraadsmedlemmet	Printerproblemernes	unicode	Inexpressively	success or wait	1	40246F	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Replyingly\Avnbgen\Spisekamrenes	Rumfartscenterets	dword	1	success or wait	1	40246F	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Fetichry	Isobase	unicode	Uncuticulate	success or wait	1	40246F	RegSetValueExW

Disassembly

No disassembly