ID: 736949
Sample Name: CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Cookbook: default.jbs
Time: 12:21:13
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

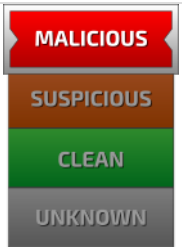
CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe

Overview

General Information

Sample Name:	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Analysis ID:	736949
MD5:	045f22ce9be3d3..
SHA1:	91b74e75d55c33..
SHA256:	e05ec32c2edc10..
Infos:	

Detection



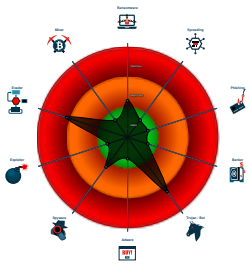
GuLoader

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Tries to detect virtualization through…
- Executable has a suspicious name …
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Contains functionality to dynamicall…
- Abnormal high CPU Usage
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe (PID: 2800 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 045F22CE9BE3D33B07A00780EE66FCFD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.835753026.0000000002A70000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

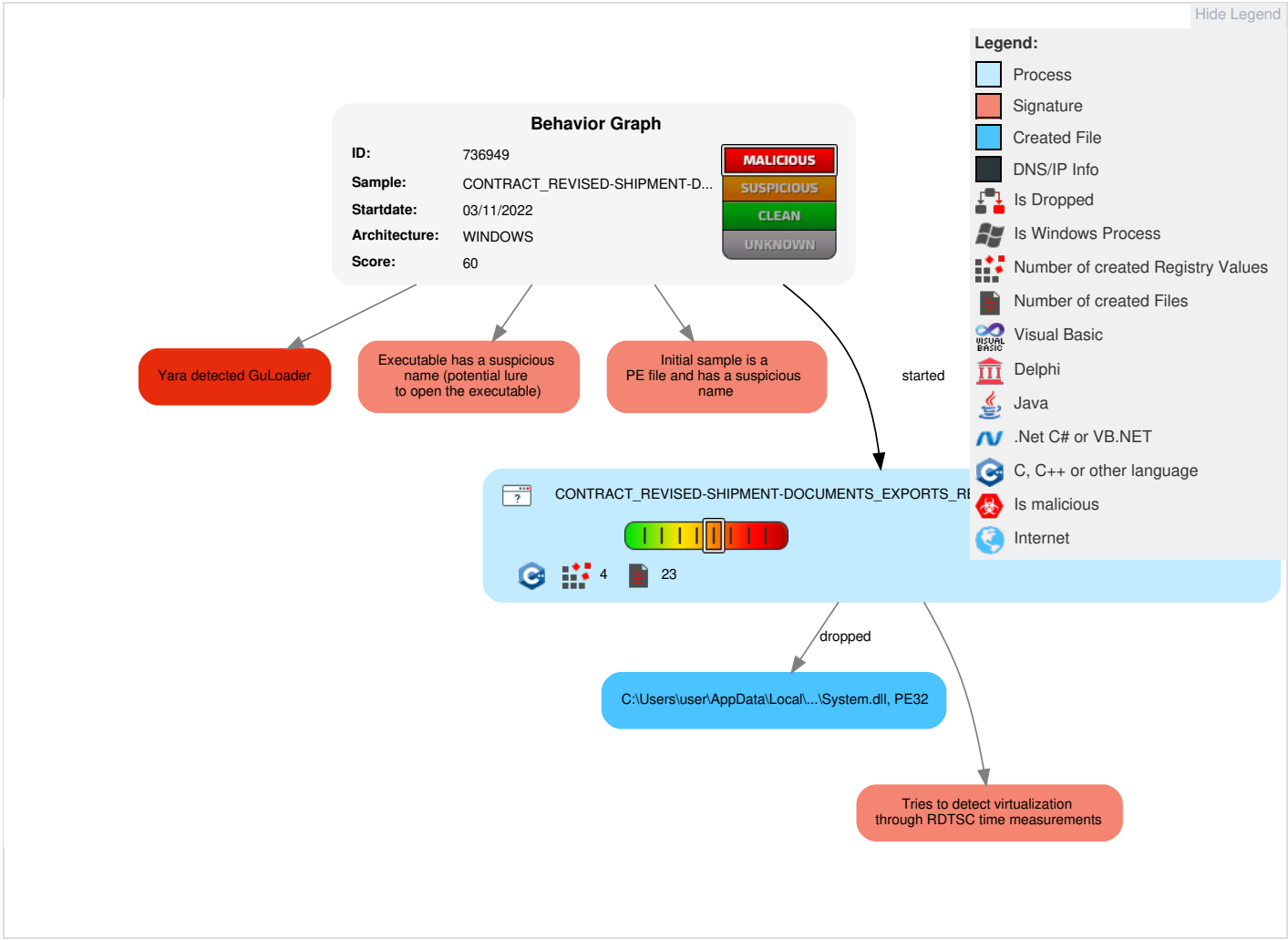
Malware Analysis System Evasion

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 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	3 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

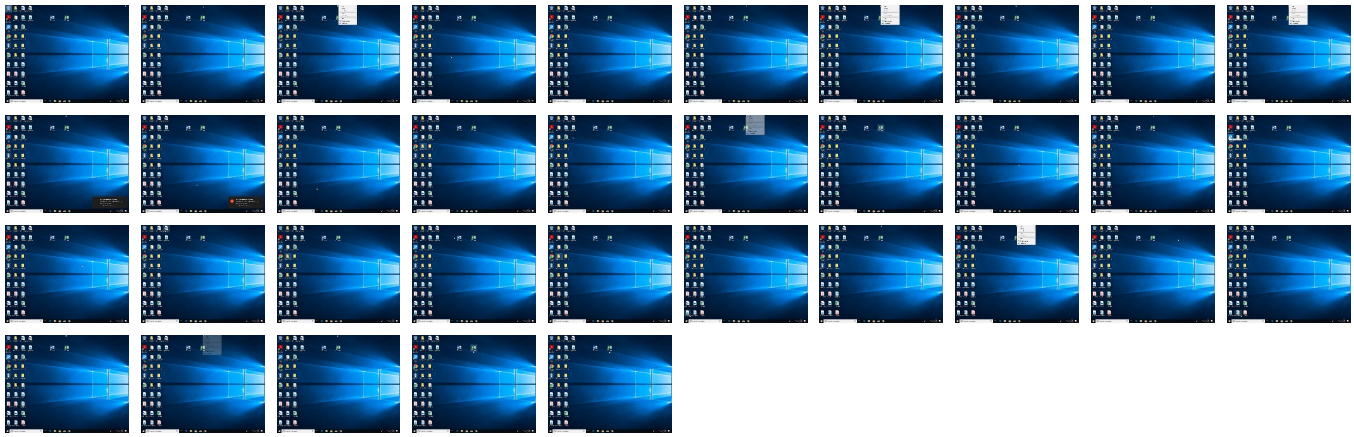
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900 299348.exe	10%	ReversingLabs	Win32.Downloader.Minix	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll	4%	Metadefender		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736949
Start date and time:	2022-11-03 12:21:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.troj.evad.winEXE@1/3@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.3% (good quality ratio 83.8%) • Quality average: 86.9% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
12:22:10	API Interceptor	1x Sleep call for process: CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe modified

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\nso5721.tmp\System.dll

Process:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.737556724687435
Encrypted:	false
SSDEEP:	192:MenY0qWTlt70lAj/lQ0sEWc/wtYbBH2aDybC7y+XBaIwL:M8+Qlt70Fj/lQRY/9VjjgL
MD5:	6E55A6E7C3FDBD244042EB15CB1EC739
SHA1:	070EA80E2192ABC42F358D47B276990B5FA285A9
SHA-256:	ACF90AB6F4EDC687E94AAF604D05E16E6CFB5E35873783B50C66F307A35C6506
SHA-512:	2D504B74DA38EDC967E3859733A2A9CACD885DB82F0CA69BFB66872E882707314C54238344D45945DC98BAE85772ACEEF71A741787922D640627D3C8AE8F1C3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 4%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L...X..`.....!....."....)....@.....p.....@.....B.....@..P.....`.....@..X.....text...O ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Roaming\Shoved\Factorist\dialog-warning-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	286
Entropy (8bit):	6.880810677512409
Encrypted:	false
SSDEEP:	6:6v/lhPysDQqinrW8/97kGwr/F+Elz3hsKrnLluYK/SwtNVp:6v/7ZiK817kG3Mz3ZliSoN7
MD5:	03DEC13C99CA8B2766C9B4468E0E781B
SHA1:	DA2202AF040D5494D7281FAB003C748457255CEE
SHA-256:	DEBC1949821086D01AE4A60BFFF1A73CFF47E7AB100E9028556496C254C05655
SHA-512:	566533ABC453A817570660154026D2206866073AB28CA6243C15AFF6A57C4A8B686EB7F23B4161EF4AE2A2C5C71F3DD6FD7271F4667A8C2E606D7CA19CC71FE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...?J.A.....A...../.%.2....<.....6...H..i..-.'Eva.qw_.`.|.3.0.s.....O_2..Y=....p..N..].J.....t.Q6..y... ..u.....|.u....1.D..b...2|..H.. .....HS]=...~.M..$.>q.....|..wq.~vZ.|a..f..Tg.x._I....IEND.B`.

C:\Users\user\AppData\Roaming\Shoved\skrupforelskede.bin

Process:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File Type:	data
Category:	dropped
Size (bytes):	106887
Entropy (8bit):	7.75553468119485
Encrypted:	false
SSDEEP:	1536:bYpDSzihO1IsnBzEfH5ZR0fha22stcSuYZtL+8VdfWuZTJrBWmlRsMM:mDcgO1IeQfH5ZRXstcgKodfhrBBDM
MD5:	73A6739AA8670352F00CA22E28B2E5E3
SHA1:	14B5E6BB7FA6A534D9CCB20C19F57D82C8C8D634
SHA-256:	1E182B58911811ED9709B682EFE83DD96093AC013DA58698D2687E526E4D3B96
SHA-512:	46D0E7F0B7EC4042B66B0CF98076D9E59157B3A011A9EB2E1238D4B5B579B9B9194F257F3B6DB9191F66F135232B0D9DA85360CBC8F87B612847FAE471083971
Malicious:	false
Reputation:	low
Preview:	Tw8... .....x.q.f..a.!..P.....r...D..L.i.:....D...|..$d.....u.....<..g..b..`.....3...<....;.....^.....#.....;<._.....W<V....s.w.....5XU....F...5G*6.<Q..%-L...<...,-...C ....y5.....<`.....[1.....`@.....@..m<s@.....@<L..K=L...u..W.....l.....`]h.Q..&.-.X[?S..;.c..vh..^.!....o.....ue.@....C&<..}....G/.E....N.b.Sx.k..*.0..-.V..F.....gCV....a$r".q.. <2)..@^$.i ...5./.Y...z'...5)jJI..:.J.[S.....`e.D_(.yp.[?....A..6uD7+.....WHf..Vp....\g.8.;....k.9....Z.W....8D.+..+..+..+..+..+..+..+..+..+..+..~..{.q...p...9..t...G.X.e.X.\..D.V...8 H.+..+..+..+..+..+..+..+..+..+..+..+..+..~p....W...qr..?...|.]q,..t.2.....!0I.V....q.C..I..A-.'R..*.....pf...'..q.%.....V.!>...4.....,;c.....5\%\q/.]..Y.....W..p.a...%.?. &...`.u/E..R.]h.h.b....~ p...5P..|V....m.W.~....n.`.....&.I5v..E.a.q..E..?.....U.....Uz...~p.e...~p..U.i..(.c..`.....5...a.|V.....@|N.....|.X..V..h.a... &

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.688048037898308
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:	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File size:	236896
MD5:	045f22ce9be3d33b07a00780ee66fcfd
SHA1:	91b74e75d55c33d8d82b10bed51ca7d3ad80147c
SHA256:	e05ec32c2edc10b6917a3cbcac9d823cb37db908cc51f3ec459800992e2b8b37
SHA512:	c363c64fe3b52d615601810b577168be5b3339ba6bde011ae0c76bbee76718782f8b737b0c9f6d82d34197045ce1c35389cba26622349bb2c0c77f62ed29d063
SSDEEP:	6144:vT4DtMeWIPR0PVPCespE0s67yIMYxrzWJougaEzEk:vTpeZ00SI18ogC
TLSH:	2134014177B5C463ED564A30C813A7F2A9B97C11D9E89F4707423E8EBC76382DA1A32D
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...P..`.....h.....

File Icon

Icon Hash:	879b931b3bb3b393

Static PE Info

General

Entrypoint:	0x4034c5
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:	0x60FC9250 [Sat Jul 24 22:21:04 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:	6e7f9a29f2c85394521a08b9f31f6275

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	OU="Squatterism Autodialing ", E=Wirestitched@Longobardian.No, O=driftier, L=West Tarbert, S=Scotland, C=GB
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	• 7/17/2022 6:44:12 PM 7/16/2025 6:44:12 PM
Subject Chain	• OU="Squatterism Autodialing ", E=Wirestitched@Longobardian.No, O=driftier, L=West Tarbert, S=Scotland, C=GB
Version:	3
Thumbprint MD5:	CE0B0A248006454637FB21369D393B35
Thumbprint SHA-1:	FDB8159D5CAE5E96B90D0300979493249FE76435
Thumbprint SHA-256:	67AA1334C6C443A496FCD527B5F1A30A2CA661AC20D33E7BCCADEF6982D2575C
Serial:	33616A6CE5467077

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080CCh]
call dword ptr [004080D0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [00434F0Ch], eax
je 00007F4CDCBD8053h
push ebx
call 00007F4CDCBDB341h
cmp eax, ebx
je 00007F4CDCBD8049h
push 00000C00h
call eax
mov esi, 004082B0h

Instruction
push esi
call 00007F4CDCBDB2BBh
push esi
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F4CDCBD802Ch
push 0000000Bh
call 00007F4CDCBDB314h
push 00000009h
call 00007F4CDCBDB30Dh
push 00000007h
mov dword ptr [00434F04h], eax
call 00007F4CDCBDB301h
cmp eax, ebx
je 00007F4CDCBD8051h
push 0000001Eh
call eax
test eax, eax
je 00007F4CDCBD8049h
or byte ptr [00434F0Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408298h]
mov dword ptr [00434FD8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0042B228h
call dword ptr [0040818Ch]
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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x147e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x37ca8	0x20b8	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6793	0x6800	False	0.6720628004807693	data	6.495258513279076	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a4	0x1600	False	0.4385653409090909	data	5.01371465125838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.5240885416666666	data	4.155579717739458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x36000	0x48000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x7e000	0x147e8	0x14800	False	0.8290658346036586	data	7.314494987254223	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x7e4f0	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x7e858	0x820b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x86a68	0x39ac	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0x8a418	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x8c9c0	0x14fa	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0x8dec0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x8ef68	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x8fe10	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x906b8	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x90d20	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x91288	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x916f0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x919d8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x91b00	0x144	data	English	United States
RT_DIALOG	0x91c48	0x13c	data	English	United States
RT_DIALOG	0x91d88	0x100	data	English	United States
RT_DIALOG	0x91e88	0x11c	data	English	United States
RT_DIALOG	0x91fa8	0xc4	data	English	United States
RT_DIALOG	0x92070	0xb6	data	English	United States
RT_DIALOG	0x92128	0x60	data	English	United States
RT_GROUP_ICON	0x92188	0xae	data	English	United States
RT_VERSION	0x92238	0x270	data	English	United States
RT_MANIFEST	0x924a8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), 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

DLL	Import
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, GetWindowLongW, GetSysColor, SetWindowPos, 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, GetVersion, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, ExitProcess, CopyFileW, 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

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe

PID: **2800**, Parent PID: **3528**

General

Target ID:	0
Start time:	12:22:10
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x400000
File size:	236896 bytes
MD5 hash:	045F22CE9BE3D33B07A00780EE66FCFD
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: 00000000.00000002.835753026.0000000002A70000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsc73B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F75	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	2	4059D1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4059D1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Shoved	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Shoved\skrupforelskede.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\AppData\Roaming\Shoved	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Shoved\Factorist	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4059D1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Shoved\Factorist\dialog-warning-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nso5721.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F75	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	4059D1	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	4059D1	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	1	4059D1	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	4059D1	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	4059D1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso5721.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	405991	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	405F33	CreateFileW
C:\Users\user\AppData\Local\Temp\nsv99C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F75	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	405F33	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc73B.tmp	success or wait	1	403774	DeleteFileW
C:\Users\user\AppData\Local\Temp\nso5721.tmp	success or wait	1	405B52	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Shoved\skrupforelskede.bin	0	18253	54 77 38 fd fd fd 20 04 fd fd fd fd fd 78 fd 71 fd 66 7e fd 61 fd 21 fd 01 50 fd fd fd fd 73 02 fd fd fd e2 72 fd fd 1d 44 fd 08 4c fd 69 fd 3a fd 0a fd 0c 44 fd fd 07 7c fd 56 24 64 fd fd 5c a7 fd 75 fd fd fd fd 16 fd 11 fd 14 fd fd fd 19 fd fd fd fd fd fd 2e fd fd 3c 00 fd 67 fd fd 62 fd fd 60 fd fd fd fd fd 10 fd fd 1c fd 33 fd fd fd 3c fd fd fd fd 3b fd 00 fd 04 fd fd 5e fd fd 11 fd fd fd fd fd fd 23 fd fd 1e fd fd fd fd 00 00 00 fd fd 3b 3c fd 5f fd fd fd fd fd 18 57 3c 56 fd fd fd fd 73 fd 77 fd fd fd fd fd 15 35 58 55 05 fd fd fd 46 fd fd 12 35 47 2a 36 fd 3c 51 fd fd 25 2d 4c 16 fd fd 3c 09 fd fd 2c 2d fd fd fd 43 fd fd 40 fd 79 35 fd fd fd 80 fd 40 fd fd 3c 60 fd fd fd fd fd fd fd	Tw8 xqfa!PrDLi:D|$du.<gb`3<;^#;<_W<Vsw5XUF5G*6<Q%-L<,-Cy5<`	success or wait	6	405FD3	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Roaming\Shoved\Factorist\dialog-warning-symbolic.symbolic.png</td><td>0</td><td>286</td><td>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 3f 4a 03 41 18 fd fd 09 16 41 04 fd fd fd fd 14 2f 10 25 fd 32 fd fd 11 fd 3c fd fd fd 04 fd fd fd 36 fd 80 17 48 fd fd 69 a4 13 2d 14 27 45 76 61 5d 71 77 5f fd 60 fd 7c fd 33 fd 30 fd 73 fd 0f fd fd fd 4f 5f 32 fd 08 59 3d fd fd fd 0a 70 fd 0f 4e fd fd 5d fd 4a fd fd fd fd fd fd 02 74 fd 51 36 fd fd 79 1d fd f2 20 13 e7 75 fd fd b5 c2 fd fd 14 7c fd 75 03 fd 02 fd 31 fd 44 fd fd 62 fd fd fd 32 7c fd fd 48 fd 10 fd fd fd 15 fd fd fd fd 48 53 5d 3d fd fd 19 7e 13 4d 17 18 24 fd 3e 71 fd fd fd fd 65 fd fd fd fd 1e 1e fd fd 7c fd fd 77 71 fd</td><td>PNGIHDRasBIT|dIDAT8? JAA/%2<6Hi- 'Evaqw_`|30sO_2Y=pN]Jt Q6y u|u 1Db2|HHS]=~M$>q|wq</td><td>success or wait</td><td>1</td><td>405FD3</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nso5721.tmp\System.dll</td><td>0</td><td>12288</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 58 fd fd 60 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 fd 29 00 00 00 10 00</td><td>MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E !D2Da0t1DV1n4D3@4DR ich5DPELX`.!")</td><td>success or wait</td><td>1</td><td>405FD3</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	unknown	512	success or wait	238	405FA4	ReadFile
C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	unknown	4	success or wait	2	405FA4	ReadFile
C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	unknown	4	success or wait	9	405FA4	ReadFile
C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	unknown	4	success or wait	2	405FA4	ReadFile
C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	unknown	4	success or wait	8	405FA4	ReadFile
C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	unknown	4	success or wait	2	405FA4	ReadFile
C:\Users\user\AppData\Roaming\Shoved\skrupforelskede.bin	unknown	1048576	success or wait	1	739A2BB9	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Bestyrelsesformanden	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unengrossed	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unengrossed\assistance	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unengrossed\assistance\Irrer36	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unengrossed\assistance\Irrer36\Trasker	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Investigational	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Investigational\Phenomenally	success or wait	1	4062DB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Investigational\Phenomenally\Abortive	success or wait	1	4062DB	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Retssags	success or wait	1	4062DB	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Retssags\Minigolfens	success or wait	1	4062DB	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Retssags\Minigolfens\Cerutterne	success or wait	1	4062DB	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Retssags\Minigolfens\Cerutterne\Pisset	success or wait	1	4062DB	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Bestyrelsesformanden	Knsdiskriminering	dword	0	success or wait	1	402513	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unengrossed\assistance\Irrer36\Trasker	Gloomings	unicode	Sacrifices	success or wait	1	402513	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Investigational\Phenomenally\Abortive	nettoprisens	binary	92 4B F0	success or wait	1	402513	RegSetValueExW
HKEY_CURRENT_USER\Software\Retssags\Minigolfens\Cerutterne\Pisset	Dactylopius	binary	84 EF 51	success or wait	1	402513	RegSetValueExW

Disassembly

No disassembly