ID: 756301
Sample Name: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Cookbook: default.jbs
Time: 00:21:08
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

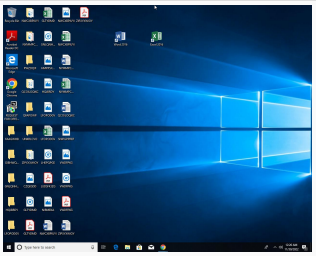
Windows Analysis Report

REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe

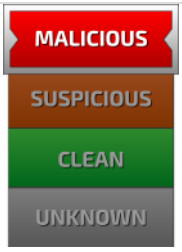
Overview

General Information

Sample Name:	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Analysis ID:	756301
MD5:	b9f70f4146b8461.
SHA1:	97cb5de0e0cc2f…
SHA256:	ff235029990af04..
Tags:	exe Loki
Infos:	



Detection



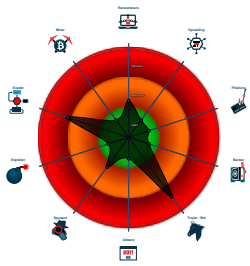
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Tries to detect virtualization through…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Sample file is different than original …
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Contains functionality to dynamicall…
- Found dropped PE file which has no…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe (PID: 1372 cmdline: C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe MD5: B9F70F4146B846179FA182AC868D0C15)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.830075184.0000000000694000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000000.00000002.830514930.00000000030F0000.00000040.00001000.00020000.00000000.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

Machine Learning detection for sample

Data Obfuscation

Yara detected GuLoader

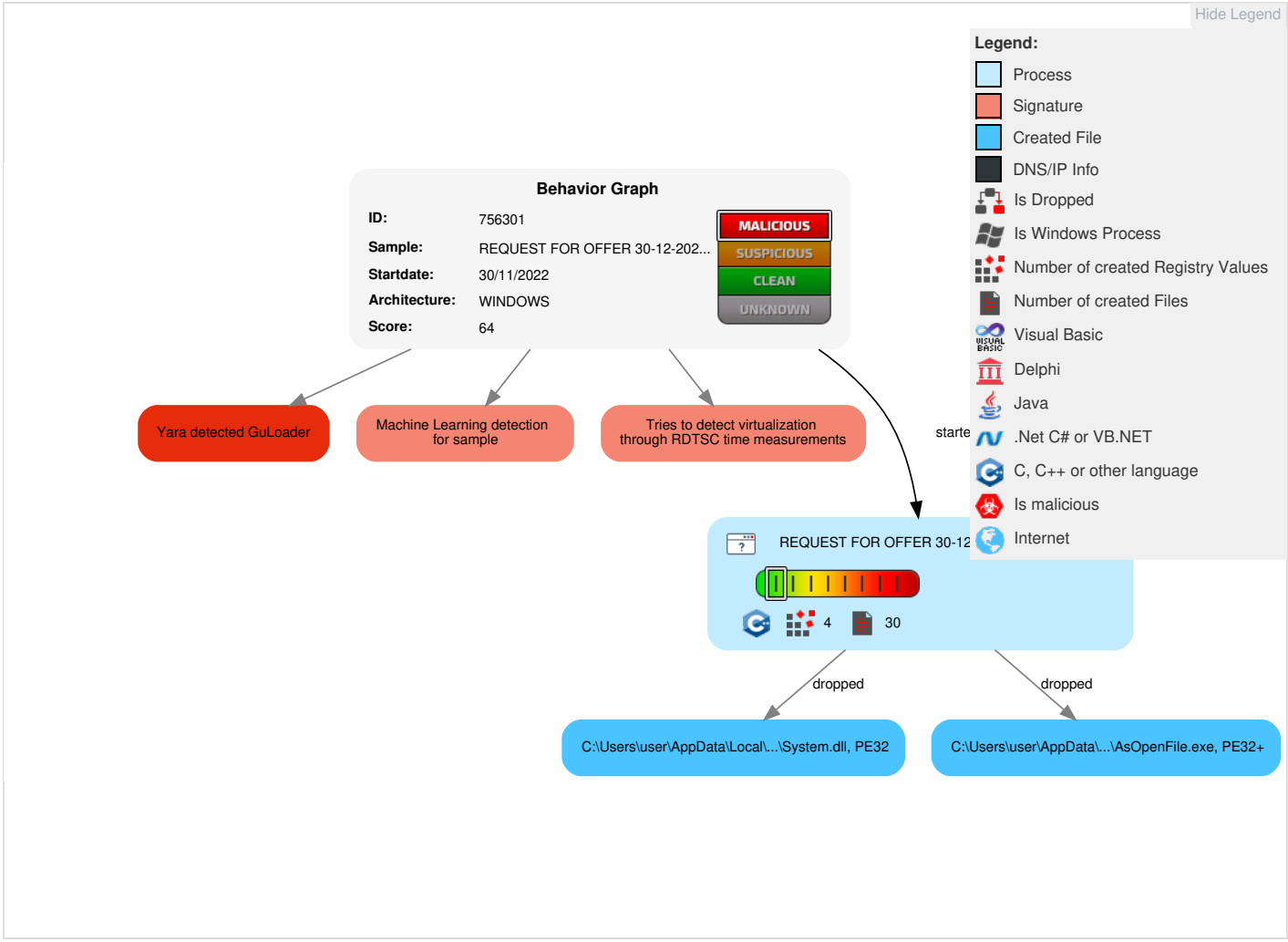
Malware Analysis System Evasion

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

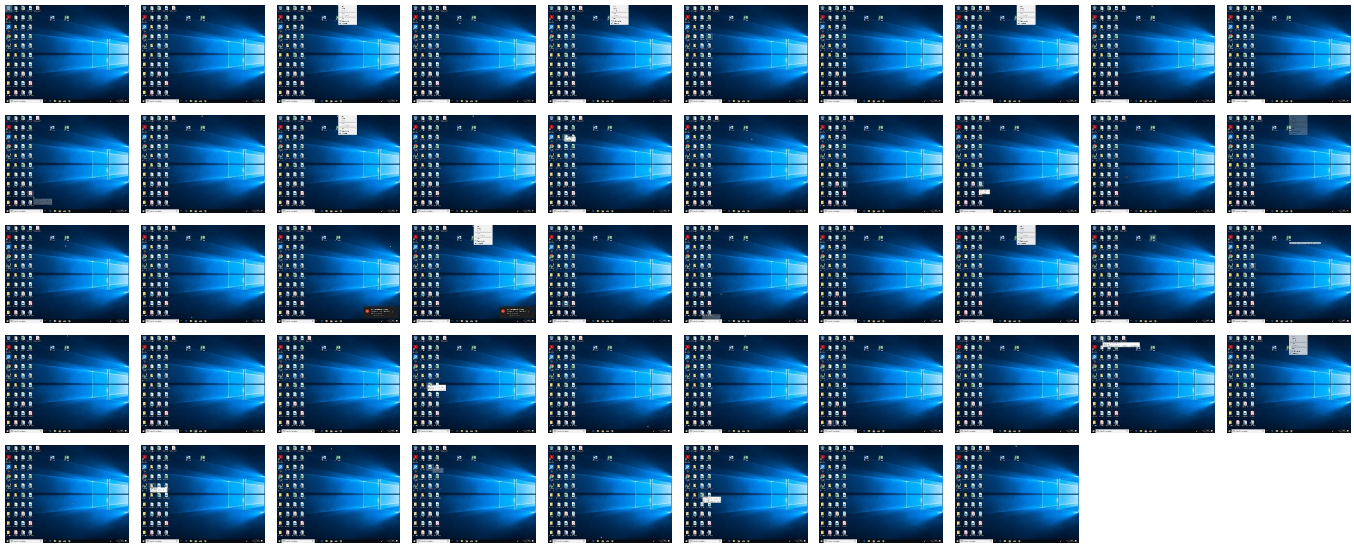
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp\System.dll	2%	ReversingLabs		

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	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756301
Start date and time:	2022-11-30 00:21:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REQUEST FOR OFFER 30-12-2022#U00b7pdf.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:	mal64.troj.evad.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.5%) • Quality average: 87.8% • 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
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe

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\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38632
Entropy (8bit):	5.840976252158136
Encrypted:	false
SSDEEP:	768:tba0g4rhVUkxIlaPrd6cMCP1diTLmz1BeeKH2X98VwhH:HPUkxIlaPrsCPXK6z1Bee3+k
MD5:	ED609F8F09DE8AAA4F8CFF0285E0420A
SHA1:	A7ADE9EB5BD4BAEFAB796C1D6EA92417F1396135
SHA-256:	2488796ACE769813C729198CFD9E3C9D0A512168301D387BE569F2557C683821
SHA-512:	32F080433C121FE1970BBB82911024A389E43B8B6BA059931FF0F3AFA4096BE79660C6DC9C1E027C21692D320F95896B0211C9FA0997AEC30F7A373382443FF2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!..r..r..r..4r..r..s..r..s..r..s..r..s..r..r..r..s..rp.s..rp.Xr..r.0r..rp.s..rRich..r.....PE..d.....a.....#.....^.....@.....Vo.... .....N.....h....p..L....x.....B..p.....@D..(...@C.....0.....text..... ..`.rdata..*....0...0..."....@..@.data.....`.....R.....@....pdata..L....p.....T.....@..@.rsrc...h.....X.....@..@.....

C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\Tusindtallig.Syn

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	29309

<table>
<tr><td>Entropy (8bit):</td><td>7.9930541941014255</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:E49NB/CsjPddY0nfj1fIXSgH0uO7wt1WayrQ0bThetG:nlCsxfVIXHH2wOfKG</td></tr>
<tr><td>MD5:</td><td>849FDC040AA117FC8B8AC03C745C690D</td></tr>
<tr><td>SHA1:</td><td>831EE9C0B27F05069A323940A7C581CA21C9BE68</td></tr>
<tr><td>SHA-256:</td><td>3C6382D1FD4C832B2BBD7CDD2508DDAA80BF40D17732C8B17C31D70CED631A79</td></tr>
<tr><td>SHA-512:</td><td>A5F45B85DAD9FD26B7B111F402467D33B92E01F9C13CD4C2932FA53617746C246393BFEF020DAEE78F4C4515BABA2B50461DA761607CD97A200B3E2206BB08A6</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>...'.A&:}.....Y8.)..rRqi....t.b.&..K1....vy}5j.........=.f.(.....3C....p+,+.`Y[]..'u.1.].].0..?KP..F.v\..M...(.V.M..^D".3.r..t....9\.N...R..6..K..S.....o|.^Z b....C.G$.s(k^...m...r.L70.m.2q' .7.%*t..5u..d.#..T.,....%..5O?..".G._.(._V.......7e.``..r....~u.A..-o.7.{.....9.T<.+.H...u.}P..:..........p..t...^...D......#..0....j.?D.rG..".....C.....QP.......+.A..=...|.X..J.w(..V.....>{8.... .7. 2m...>..;=.-....Qq...cx.=.....3..m.x.#..../...........3.w.@Rd.rVt..Q.v..1LW`]'..Bs.{...........5....J...t..o..1..M.........H,(ugAw.....C.]...J.y...<~(u.....|..Y....B...}....(cn.....Gc..|.6x6w.....HD. ...GV........r....u\......^Po.._|]R.......R...|. LH....Z/}(st..0..F..L...J.G 5|.0t.q.x..m..W..X.k..=..k.+.a..U...r..f..|<O...t.vN.)..>t..J.j....J.'..OR.-.S..cU....?X...........L!......3....I...a..A.[c.,....2....p.~..!%..m.2.....[=.......r.n.6......G...1...IqV..fn..j...E..[........>.CZHT.......w..~7<=.......<8e..I.p..Q...f.....qD..]Xh..LA...J........7.....O..</td></tr>
</table>

C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\prowl.Dgn

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	141909
Entropy (8bit):	7.124693631306355
Encrypted:	false
SSDEEP:	3072:COxlLD2mpgf8pOxNjQzNUflgAG63+OAyam6kxnv:COxlmcg5EzuNG6MyaJSv
MD5:	0A951AA33DE8994CBE161F0E07F169B8
SHA1:	38033C58EEFF600D22A068F1A7F599646BDFDD1E
SHA-256:	4A98204499C5BA9F9518D6A7EF078A5A5F0B82173919E9A5D41179172BD28F60
SHA-512:	F9BE445FDBD89EB0F5CACBB325D89E89755906F1DADE3A7E32593E4ADFCBFF2C8927350226BB8FD0238B4F8F72377F757ADCDAFE20C7FA2FF41C4A14814D8A27
Malicious:	false
Reputation:	low
Preview:	.T.....i.. ..YA..^..;;..3Gn._+.P.a1TG...$;....r..K...8.W..gS..9j.t...j y._........e.....[z......Ae.8/...f........B..).. ....o..-...7.Qf......B..e..f....L..2B...!..a....-.F..ooo ooooooooooooooooooooooooooooooooooooo..c.B......JV.XS...B.....f.r...=..U..f....'.5~.......... ....9x...f....:.e...67..N..!.f...f....9$}17..2/. .LPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPf......

C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp\System.dll

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8QIl975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	moderate, very likely benign file
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......1...u.u.u...s.u.a....r.!..q....t....t.Richu.........................PE..L.....MX.. ....!..... ....'.......0..............................`......................................2.......0..P............................P.........................................................0..X...........................text............ ........ .......... ..`.rdata..S....0.......$.............@..@.data...x....@.......(.............@....reloc..b....P.......*.............@..B... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.875386203366202
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:	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File size:	194987
MD5:	b9f70f4146b846179fa182ac868d0c15
SHA1:	97cb5de0e0cc2f53cd73552f9d5b4381ab5a5907
SHA256:	ff235029990af0449ce8f82c5546dfe37170d5e27ce1a22b0a43965a980344be
SHA512:	2cc45205394074ddf9a5481a81b89582d84d42a34023329e06cf589c455c2fef144905362b5d1001e26026480d490304b6ac96526ab32f5344b1706d98ceff48
SSDEEP:	3072:MRD+3q3NxPTNuY/bQZFler2MUPaSa1y8XKdV06k55ohchNqV3AzlbEnJZGqItyWJ:mwq3NpNSFleCMUPVaidHXMNqwlInJ0q8
TLSH:	A714125533E0C523CAF202702DBB652F9EE9A642E262FF131360AF9D7D56307864C356
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L...8.MX.....b...*.....J4.....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40344a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x584DCA38 [Sun Dec 11 21:50:48 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4ea4df5d94204fc550be1874e1b77ea7

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007FEAF0D9B2A3h

Instruction
push ebx
call 00007FEAF0D9E3FCh
cmp eax, ebx
je 00007FEAF0D9B299h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007FEAF0D9E376h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FEAF0D9B27Ch
push ebp
push 00000009h
call 00007FEAF0D9E3CEh
push 00000007h
call 00007FEAF0D9E3C7h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007FEAF0D9DFB0h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007FEAF0D9DF9Eh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x69000	0xb48	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x3e000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x69000	0xb48	0xc00	False	0.4228515625	data	4.372183800985918	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x691c0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x694a8	0x100	data	English	United States
RT_DIALOG	0x695a8	0x11c	data	English	United States
RT_DIALOG	0x696c8	0xc4	data	English	United States
RT_DIALOG	0x69790	0x60	data	English	United States
RT_GROUP_ICON	0x697f0	0x14	data	English	United States
RT_MANIFEST	0x69808	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

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

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe PID: 1372, Parent PID: 3528

General	
Target ID:	0
Start time:	00:22:02
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Imagebase:	0x400000
File size:	194987 bytes
MD5 hash:	B9F70F4146B846179FA182AC868D0C15
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000000.00000002.830075184.0000000000694000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.830514930.00000000030F0000.00000040.00001000.00020000.00000000.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	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsuC2DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsuC2DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Folkedansens	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Folkedansens\Suffigere	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\prowl.Dgn	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\Tusindtallig.Syn	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nsgC6C8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\ProgramData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	10	4058C9	CreateDirectoryW
C:\ProgramData\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	10	4058C9	CreateDirectoryW
C:\ProgramData\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	10	4058C9	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Templates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	10	4058C9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\Templates\Efterspor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Templates\Efterspor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	9	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405889	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	14	405E13	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsuC2DE.tmp	success or wait	1	4036D7	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsgC6C9.tmp	success or wait	1	405A32	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	405EB3	WriteFile
unknown	42068	21265	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	405EB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\prowl.Dgn	0	16384	fd 54 fd 1b fd 09 fd 69 15 1b 20 fd fd 59 41 fd fd 5e 06 fd 3b 3b fd fd 33 47 6e fd 5f 2b fd 50 fd 61 31 54 47 fd fd fd 24 3b fd fd 1a fd 72 fd 1f 4b fd c3 07 38 fd 57 12 fd 67 53 fd 15 39 6a fd 74 fd fd fd 6a 20 79 fd 5f fd fd fd fd fd fd fd 65 c1 fd fd fd fd 5b 7a fd fd fd fd fd fd 41 65 fd 38 2f fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 66 fd fd 00 fd fd fd fd fd 42 fd 0f 29 2e fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 44 fd fd fd 0f 6f fd fd 2d	Ti YA^;;3Gn_+Pa1TG$;rK8 WgS9jtj y_e[zAe8/fB).o-	success or wait	9	405EB3	WriteFile
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 21 73 fd 72 73 fd 72 73 fd 72 fd fd 34 72 f3 fd 72 fd 66 73 f3 fd 72 fd e3 73 f3 fd 72 fd e4 73 f3 fd 72 fd e2 73 b3 fd 72 73 fd 72 72 fd 72 fd e6 73 33 fd 72 70 ae 73 b3 fd 72 70 fd 58 72 33 fd 72 73 30 72 33 fd 72 70 a5 73 33 fd 72 52 69 63 68 73 fd 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$!rrr4rrsrsrsrs rrrsrpsrpXrr0rrpsrRichr	success or wait	3	405EB3	WriteFile
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\Tusindtallig.Syn	0	16384	0d 1d fd 27 fd 41 26 3a 7d fd fd fd 16 fd 59 38 fd 29 0c fd 72 52 71 69 bd fd fd fd 74 fd 62 fd 26 fd 04 4b 31 fd fd fd 03 76 79 7d 35 6a 0f 7f fd fd fd fd 1b fd fd 3d 0a 66 fd 28 fd fd fd 01 fd 33 43 fd fd 13 fd 70 2b 2c 2b fd 60 59 5b 5d fd fd 27 75 fd 31 fd 5d fd 5d fd 30 fd fd 3f 4b 50 fd fd 46 fd 76 5c fd fd 4d fd 06 fd 28 fd 56 fd 4d fd fd 5e 44 22 fd 33 2d 72 fd 14 74 fd fd fd fd 39 5c fd 4e fd fd fd 52 fd 18 36 fd fd 4b 17 fd 53 fd fd fd 06 fd 6f 7c fd 5e 5a 20 62 fd 2e fd 0a 43 1a 47 24 fd 73 28 6b 5e fd 13 fd 6d fd fd fd 72 fd 4c 37 30 fd 6d fd 32 71 27 17 37 1a 25 2a 74 fd 18 35 75 15 fd 64 17 23 fa fd 54 fd 2c fd fd fd 19 25 fd 12 35 4f 3f 1b fd 22 fd 47 0b 5f fd 28 fd 5f 56 fd fd fd fd fd fd fd 37 65 1b 60 60 fd fd 72 fd fd	'A&:}Y8)rRqitb&K1vy}5j=f (3Cp+,+`Y[]'u1]]0? KPFv\M(VM^D"3rt9\N R6KSo|^Z b.CG$s(k^mrL70m2q'7%* t5ud#T,%5O?"G_(_V7e``r	success or wait	2	405EB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsgC6C9.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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 1a fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELMX!	success or wait	1	405EB3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	unknown	512	success or wait	77	405E84	ReadFile
C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	unknown	16384	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsuC2DF.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsuC2DF.tmp	unknown	23350	success or wait	1	403269	ReadFile
C:\Users\user\AppData\Local\Temp\nsuC2DF.tmp	unknown	4	success or wait	3	405E84	ReadFile
C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	unknown	16384	success or wait	9	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsuC2DF.tmp	unknown	16384	success or wait	14	405E84	ReadFile
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\Tusindtallig.Syn	unknown	2	success or wait	275	4026D2	ReadFile
C:\Users\user\AppData\Local\Temp\nsuC2DF.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\prowl.Dgn	unknown	1052672	success or wait	1	10002965	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Procentuelles232	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Procentuelles232\Frafaldsprocents	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Procentuelles232\Frafaldsprocents\Forarbejdendes	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Procentuelles232\Frafaldsprocents\Forarbejdendes\Inceration	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Sammenlgningens	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Sammenlgningens\Tjurunga	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Sammenlgningens\Tjurunga\Pakkeforsendelserne	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Sammenlgningens\Tjurunga\Pakkeforsendelserne\Thiophthene	success or wait	1	40242E	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\Compoundedness	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Bekvemmeligheder	success or wait	1	40242E	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Procentuelles232\Frafaldsprocents\Forarbejdendes\Inceration	Pythius	unicode	home	success or wait	1	40248E	RegSetValueExW
HKEY_CURRENT_USER\Software\Sammenlgningens\Tjurunga\Pakkeforsendelserne\Thiophthene	Etaper	expand unicode	%Grumpier248%\Sejlklart.Dis	success or wait	1	40248E	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Compoundedness	Caballo	expand unicode	%Polering%\Arbejdsdelingerne159.Bin	success or wait	1	40248E	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Bekvemmeligheder	Hovedbiblioteker ne	dword	0	success or wait	1	40248E	RegSetValueExW

Disassembly

No disassembly