ID: 756266
Sample Name: PO.exe
Cookbook: default.jbs
Time: 22:38:05
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

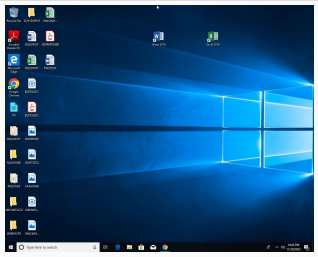
Windows Analysis Report

PO.exe

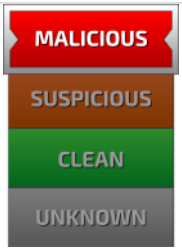
Overview

General Information

Sample Name:	PO.exe
Analysis ID:	756266
MD5:	9297126fd9624f7.
SHA1:	c30b3c8fddd49f7..
SHA256:	edd8e1858bcc70..
Tags:	exe
Infos:	



Detection



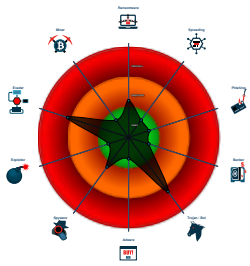
GuLoader

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- PO.exe (PID: 2372 cmdline: C:\Users\user\Desktop\PO.exe MD5: 9297126FD9624F7DC2D4F64F072668A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.766696218.0000000003190000.00000040.00001000.00020000.00000000.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

Data Obfuscation

Yara detected GuLoader

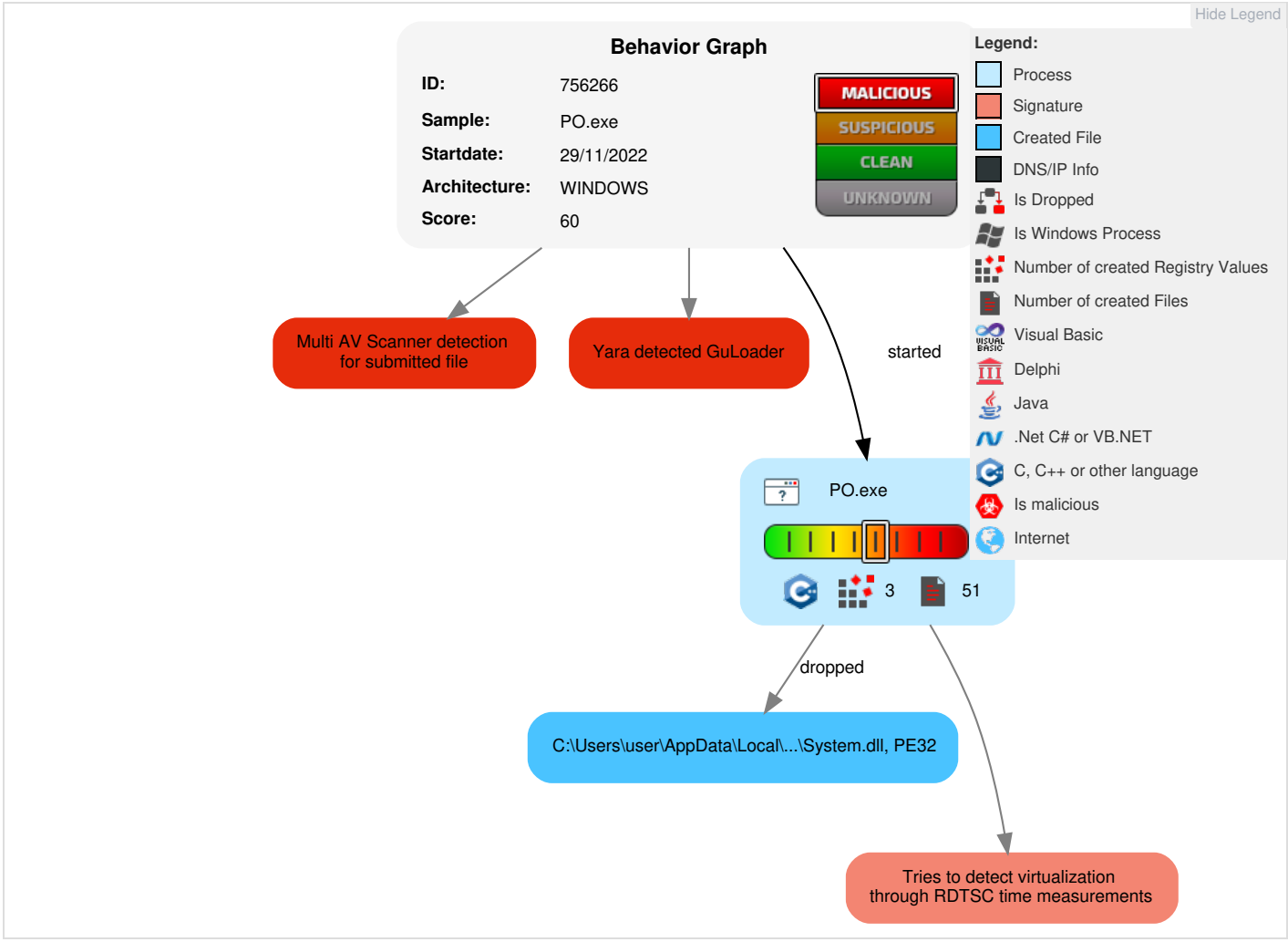
Malware Analysis System Evasion

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	Windows Management Instrumentation	1 Windows Service	1 Access Token Manipulation	1 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

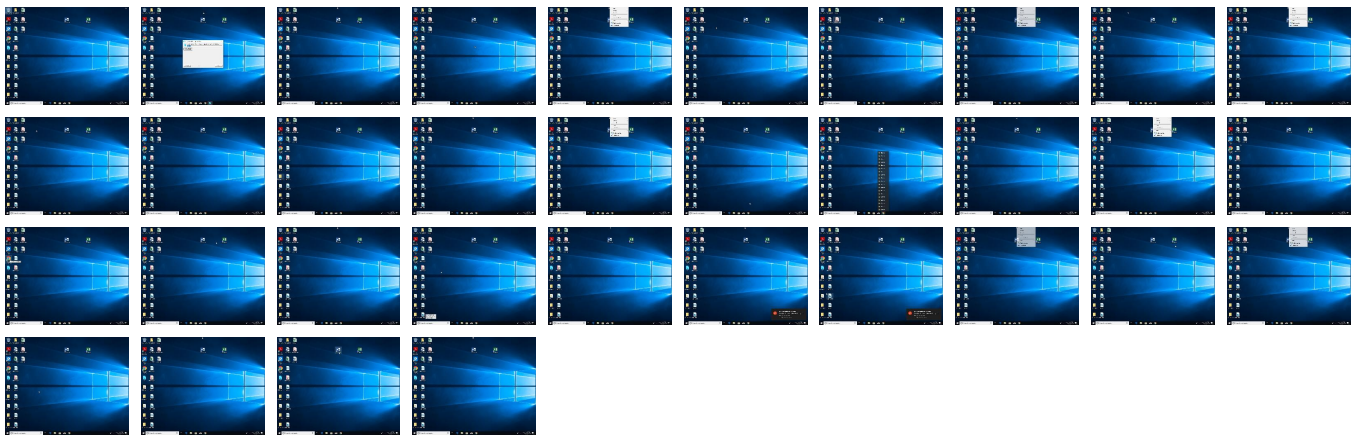
Behavior Graph



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
PO.exe	27%	ReversingLabs	Win32.Downloader.Nemesis	
PO.exe	29%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp\System.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	PO.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756266
Start date and time:	2022-11-29 22:38:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO.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:	11
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@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63% (good quality ratio 61.7%) • Quality average: 88.2% • Quality standard deviation: 21.9%
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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey 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\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically\Omfattede\Iblanding\Heterodoxical.Ufo

Process:	C:\Users\user\Desktop\PO.exe
File Type:	data
Category:	dropped
Size (bytes):	169298
Entropy (8bit):	6.993422708563822
Encrypted:	false
SSDEEP:	3072:3H36doFRBxbYjEigfKAFBx4klY9HcLYO6P7tbLkXlBDPn4rrHIRqkFjOjz:XHRojYfLqkqFZbSjDKrSnpOH
MD5:	E9CD51B8DF0E079A6D84286C4F8FB583
SHA1:	30BB91305F4BAD22563D16D837405BD105982218
SHA-256:	B1DFFFB8EE9D8CB22BF5C8660D793719ACFEC38A08F2A78E90EE8D4067512159
SHA-512:	D33B5DED1B891A2BEB68B0127FFB8E0B30AE3856877F7BEF93D42440D15FFEF6EADC8007137E0BC1B1257CB09777344B22773CEA9F9FDDC81FBDAC3A66DF65AD
Malicious:	false
Reputation:	low
Preview:	.:.V,:.. E....-^,z..3U.g...v.Q.sY..x.....@...m|..I...V.y...@.....S.....G.+...UQg5...@..:..o8.v.j.5.<../..3..0,E.b.v...._...h..b...J.M..._.E/x24.K...\.R.....X.~...._4..%...2\.....:6.5.>E...N &j)yc.F....o....R.tZZ.F.UW....0.....N.,GTMj.....I.....[{..0U..4..3...,I$..}.g.&.u..!.".lstg.5..{..~az..U..J.....j.c[...z.j./...!m.....Cy.U....X.. 9...@..V$...M..*%...O.@..V5.....+".}.4.>.. ...<..e.....;..b9;"D...&E.....A_Q.%..^..t.N&1^....c.....G..h=H.....?.....W.....`.4..,..3.IaaH.B.ZmB....f.J.....a..(p.-X..*...f..W.'.D(O...,..4..cG...../G./..^....6X..x.CD{\g.....{...F:.. 4...tJ>J..=..#K...-.....v...f....J.=7@oM.e.$l..U..m..<..:.O6.,...\.Y|[do.8.w....#]2..f.. ....[...J....g.h`.....Q.f.C_..T...iIR.....A..%t._6fYH.]g.....o.i.c..U.H...h....M...@.n...9.[t.X.....o... ...t.....%PWY.t@..Ce..WG.%.I..b}eF....B.6K.N....Qf.C.P....f....2.>.#...3.5Y.=...d..3.....\f.J..9S.16bQ...}..'.g..M.I.B^e\.8...A.L....v.p..u.....:....Y~t...i...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Referenceliste\holdovers\open-menu-symbolic.svg

Process:	C:\Users\user\Desktop\PO.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	314
Entropy (8bit):	4.555782614723155

Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slLlNkRI7NtAlaRI7SdtAlaRI7UNtAlBC:TMHdPnnl/nu3tln7NWlz7MWlz7UNWlM
MD5:	53C42FCA9E64A93B4C572D5BA805FD4D
SHA1:	1659423CA8F981CFD2EEB6ADD25C03CA5B37FFBD
SHA-256:	DD3F1C117437A6F5124905DE7212A1A320E76F9B33D8411BF70DBDBEFA8E9BAD
SHA-512:	2852EB784E5090F298259F04516C1413734ECF20EA7D143864FE0312A6410E83FFF49E16DCE3CF7F61177238B4DECEBD540FD839E3721965A5141856908392DD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 1 2 h 14 v 2 h -14 z m 0 0"/>. <path d="m 1 7 h 14 v 2 h -14 z m 0 0"/>. <path d="m 1 12 h 14 v 2 h -14 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\TOBEN.lnk

Process:	C:\Users\user\Desktop\PO.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	856
Entropy (8bit):	2.928119175705163
Encrypted:	false
SSDEEP:	12:8gl02sX2lw/tz+7RafgKD7mWH/+CNJkKAb4t2Y+xIBjK:8dTaRMgKhPHAJ7aB
MD5:	B81090D32591EB295A10138D5B0439B3
SHA1:	19285E160280462064A63B6957DA2F3F71DB25F1
SHA-256:	8294B2C9D6BD61D43566B01682100C387EA0D67A72634365D416404EB1377C36
SHA-512:	F7BC33A0A7B7DEF27D495ED9E92C5E2EA4D1A0D5B4B99009CB01F7DBABE79297A8487E2E70A7FBD579EE01E8F27A560EA75B94F5579FE9E451A0F4A294D13DCF
Malicious:	false
Reputation:	low
Preview:	L.....F.....)....P.O. .:i.....+00../C:\.....P.1.....Users.<.....U.s.e.r.s.....Z.1.....user..B.....e.n.g.i.n.e.e.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....\.2.....TOBEN.txt.D.....T.O.B.E.N...t.x.t.....\.T.O.B.E.N...t.x.t.....(.....!^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp\System.dll

Process:	C:\Users\user\Desktop\PO.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.6557532861400945
Encrypted:	false
SSDEEP:	192:eK24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35OlASl:u8Qll975eXqlWBrz7YLOlA
MD5:	0FF2D70CFDC8095EA99CA2DABBEC3CD7
SHA1:	10C51496D37CECD0E8A503A5A9BB2329D9B38116
SHA-256:	982C5FB7ADA7D8C9BC3E419D1C35DA6F05BC5DD845940C179AF3A33D00A36A8B
SHA-512:	CB5FC0B3194F469B833C2C9ABF493FCEC5251E8609881B7F5E095B9BD09ED468168E95DDA0BA415A7D8D6B7F0DEE735467C0ED8E52B223EB5359986891BA6E2E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L....z.W.....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... .....rdata..S....0.....$.....@..@.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):	6.435141913006391

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:	PO.exe
File size:	269537
MD5:	9297126fd9624f7dc2d4f64f072668a2
SHA1:	c30b3c8fddd49f7dfba687026daf6293f6d90b1b
SHA256:	edd8e1858bcc704fdea75837bb448eceda61317e7f8028e82aa2a0e5559c658a
SHA512:	57fd81274b3f16cb8f0056c9afe2c697649db154c12e63a4ed8bad65ccb6b598845adce9883bd2695335e05e8f3c877fc9f2e32a637c01e170d0b671e32c6d0b
SSDEEP:	6144:DB+pqUiH1YF0tV1R5nqyw8TqwiV6lMATl:DgcHyF+Hqyw83iLATl
TLSH:	39448B147A6CE127F11AC6709B52AD1B7E783F040865D203BEC4FB5E353B14299FA26B
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....z.W.....b...*.....3.....@

File Icon

Icon Hash:	b474f4c4c4c4c4d4

Static PE Info

General

Entrypoint:	0x4033b6
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:	0x57017AB0 [Sun Apr 3 20:18:56 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 00007FCDBCE10033h
push ebx
call 00007FCDBCE1318Ch

Instruction
cmp eax, ebx
je 00007FCDBCE10029h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007FCDBCE13106h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FCDBCE1000Ch
push ebp
push 00000009h
call 00007FCDBCE1315Eh
push 00000007h
call 00007FCDBCE13157h
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 00007FCDBCE12D40h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007FCDBCE12D2Eh
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	0x6c000	0x19f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x615d	0x6200	False	0.6616709183673469	data	6.45041359169741	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	0.5026041666666666	data	3.9824009583068882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x41000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6c000	0x19f28	0x1a000	False	0.062424879807692304	data	2.7337265494354486	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6c358	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x6c6c0	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x7cee8	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x81110	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x836b8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x84760	0x9ee	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x85150	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x855b8	0x144	data	English	United States
RT_DIALOG	0x85700	0x13c	data	English	United States
RT_DIALOG	0x85840	0x100	data	English	United States
RT_DIALOG	0x85940	0x11c	data	English	United States
RT_DIALOG	0x85a60	0xc4	data	English	United States
RT_DIALOG	0x85b28	0x60	data	English	United States
RT_GROUP_ICON	0x85b88	0x5a	data	English	United States
RT_MANIFEST	0x85be8	0x340	XML 1.0 document, ASCII text, with very long lines (832), with no line terminators	English	United States

Imports

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

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

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: PO.exe PID: **2372**, Parent PID: **3452**

General

Target ID:	0
Start time:	22:38:56
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO.exe
Imagebase:	0x400000
File size:	269537 bytes
MD5 hash:	9297126FD9624F7DC2D4F64F072668A2
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: 00000000.00000002.766696218.0000000003190000.00000040.00001000.00020000.00000000.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	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaCD4A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DC1	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsaCD4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DC1	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	405835	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	405835	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	405835	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	405835	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	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus\Hagmane	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus\Hagmane\Vestblok	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus\Hagmane\Vestblok\fiji	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DC1	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	405835	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405835	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	405835	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	405835	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	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaCD4C.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	4057F5	CreateDirectoryW
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	405835	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	405835	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	3	405835	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	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\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	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically\Omfattede	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically\Omfattede\Iblanding	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically\Omfattede\Iblanding\Heterodoxical.Ufo	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7F	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Referenceliste	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Referenceliste\holdovers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Referenceliste\holdovers\open-menu-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7F	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7F	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405D7F	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	405835	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	405835	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	3	405835	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	405835	CreateDirectoryW

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	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus\Hagmane	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus\Hagmane\Vestblok	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Fladlus\Hagmane\Vestblok\fiji	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405835	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	405D7F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaCD4A.tmp	success or wait	1	403643	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsaCD4C.tmp	success or wait	1	40599E	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	405E1F	WriteFile
unknown	48617	22716	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	405E1F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ablepticallly\Omfattede\Iblanding\Heterodoxical.Ufo	0	16384	fd 3a fd 56 2c 3a 1d fd 20 45 fd fd 14 fd 2d 5e 2c 7a fd fd 33 55 fd 67 82 fd a0 76 0f 51 12 73 59 fd fd 78 fd a1 fd fd fd 40 fd fd fd 6d 7c 0b fd 49 fd fd fd 56 fd 79 fd fd fd 40 1f 15 fd 13 c7 53 63 fd 0f 28 fd 47 2e 2b fd fd fd 55 51 67 35 61 fd fd 40 08 16 3a fd fd 6f 38 fd 76 fd 6a fd 35 fd 3c fd fd 2f fd fd 33 fd 04 30 2c 45 fd 62 00 76 41 fd fd fd 5f fd fd fd 68 fd fd 62 fd 13 fd 4a 1b 4d fd 0f fd 5f fd 45 2f 78 32 34 fd 4b fd 15 fd 5c fd 52 09 0a fd 1c fd fd 58 fd 7e 36 1b fd fd 5f 34 07 fd 25 fd fd fd 32 5c fd 1c fd fd 03 3a 36 fd 35 fd 3e 45 fd fd fd 4e 26 6a 29 79 63 4b 46 fd fd fd 80 6f fd 01 fd fd 52 fd 74 5a 5a fd 46 fd 55 57 fd fd 11 fd 30 14 fd 1a 1e fd 2e 14 9f d9 4e fd 2c 47 54 4d 6a fd	:V,: E- ^,z3UgvQsYx@m|IVy@SG.+U Qg5@:o8vj5</30,Ebv_hbJM_E/x24K \RX~_4%2\:65>EN&j)ycFoRtZZFUW0.N,GTMj	success or wait	11	405E1F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Referenceliste\holdovers\open-menu-symbolic.svg	0	314	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 31 20 32 20 68 20 31 34 20 76 20 32 20 68 20 2d 31 34 20 7a 20 6d 20 30 20 30 22 2f 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 31 20 37 20 68 20 31 34 20 76 20 32 20 68 20 2d 31 34 20 7a 20 6d 20 30 20 30 22 2f 3e 0a 20 20 20 20 20 20 20 20	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <g fill="#2e3436"> <path d="m 1 2 h 14 v 2 h -14 z m 0 0"/> <path d="m 1 7 h 14 v 2 h -14 z m 0 0"/>	success or wait	1	405E1F	WriteFile
C:\Users\user\AppData\Local\Temp\nsaCD4C.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 00 00 50 45 00 00 4c 01 04 00 fd 7a 01 57 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!qttRichuPELzW!	success or wait	1	405E1F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO.exe	unknown	512	success or wait	278	405DF0	ReadFile
C:\Users\user\Desktop\PO.exe	unknown	16384	success or wait	1	405DF0	ReadFile
C:\Users\user\AppData\Local\Temp\nsaCD4B.tmp	unknown	4	success or wait	1	405DF0	ReadFile
C:\Users\user\AppData\Local\Temp\nsaCD4B.tmp	unknown	31728	success or wait	1	4031D5	ReadFile
C:\Users\user\AppData\Local\Temp\nsaCD4B.tmp	unknown	4	success or wait	2	405DF0	ReadFile
C:\Users\user\Desktop\PO.exe	unknown	16384	success or wait	7	405DF0	ReadFile
C:\Users\user\AppData\Local\Temp\nsaCD4B.tmp	unknown	16384	success or wait	12	405DF0	ReadFile
C:\Users\user\AppData\Local\Temp\nsaCD4B.tmp	unknown	4	success or wait	1	405DF0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically\Omfattede\Iblanding\Heterodoxical.Ufo	unknown	1052672	success or wait	1	10002965	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\One	success or wait	1	4023BF	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Lysogenicity	success or wait	1	4023BF	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Lysogenicity\Afvaskning	success or wait	1	4023BF	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Lysogenicity\Afvaskning\Sphenes	success or wait	1	4023BF	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Ahorntrets	success or wait	1	4023BF	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Ahorntrets\Kanaima	success or wait	1	4023BF	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\One	Guli	dword	145	success or wait	1	40241B	RegSetValueExW
HKEY_CURRENT_USER\Software\Lysogenicity\Afvaskning\Sphenes	Komponenttegninger	expand unicode	%Hyperthermal%\Inrush\Piggen.Sko	success or wait	1	40241B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Ahorntrets\Kanaima	Forstuvningerne	dword	0	success or wait	1	40241B	RegSetValueExW

Disassembly

No disassembly