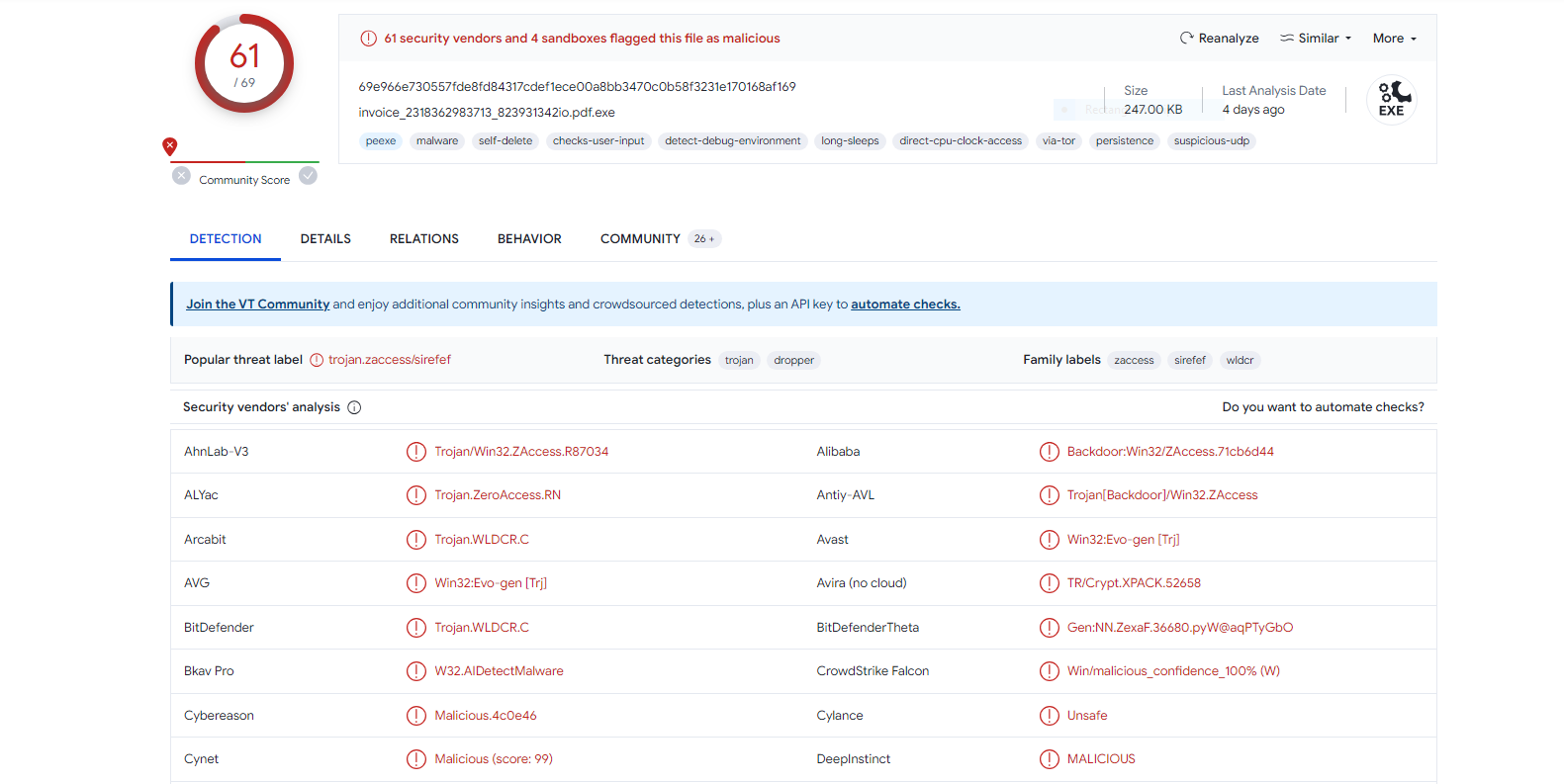
**Zeus Banking Trojan Report**



VirusTotal Report

**Hashes**

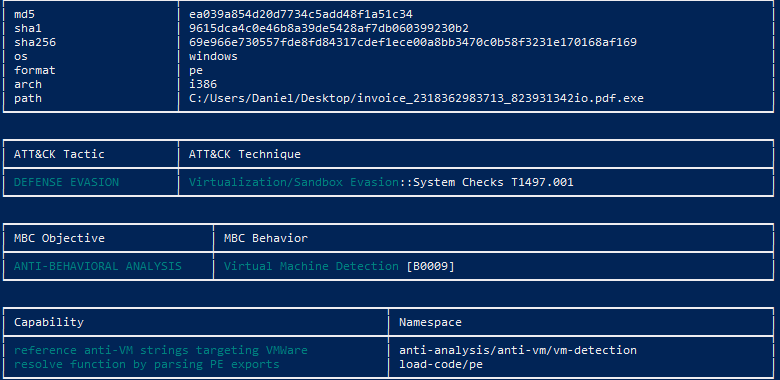
**Md5**: ea039a854d20d7734c5add48f1a51c34

**sha1**: 9615dca4c0e46b8a39de5428af7db060399230b2

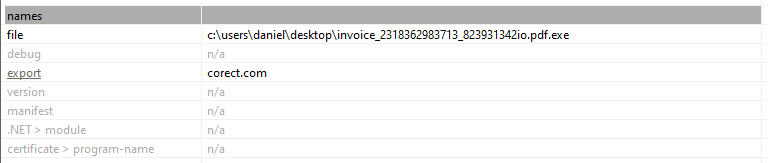
**sha256:** 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

**Filename:** invoice\_2318362983713\_823931342io.pdf.exe

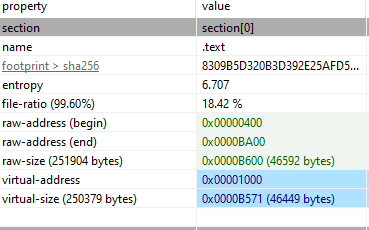
**Capa Output**



**Basic Static Analysis**

****

Research showed this to be a Romanian News Source

****

Doesn’t appear to be compressed, raw address and virtual are similar sizes

**API CALLS:**

ascii,14,section:.itext,-,import,windowing,-,CallWindowProc

ascii,12,section:.itext,-,import,windowing,-,UpdateWindow

ascii,24,section:.itext,x,import,windowing,-,AllowSetForegroundWindow

ascii,10,section:.itext,-,import,windowing,-,GetCapture

ascii,15,section:.itext,-,import,windowing,-,IsWindowEnabled

ascii,19,section:.itext,-,import,windowing,T1010 | Window Discovery,GetWindowTextLength

ascii,21,section:.itext,-,import,synchronization,-,DeleteCriticalSection

ascii,14,section:.itext,-,import,resource,-,SizeofResource

ascii,22,section:.itext,x,import,reconnaissance,-,GetEnvironmentVariable

ascii,16,section:.itext,-,import,reconnaissance,-,GetLogicalDrives

ascii,12,section:.itext,-,import,reconnaissance,T1124 | System Time Discovery,GetTickCount

ascii,12,section:.itext,-,import,reconnaissance,-,GetDriveType

ascii,22,section:.itext,x,import,reconnaissance,-,GetEnvironmentVariable

ascii,11,section:.itext,-,import,memory,-,LocalUnlock

ascii,8,section:.itext,-,import,memory,-,HeapFree

ascii,14,section:.itext,-,import,memory,T1055 | Process Injection,VirtualQueryEx

ascii,10,section:.itext,-,import,memory,-,LocalAlloc

ascii,9,section:.itext,-,import,memory,-,LocalFree

ascii,9,section:.itext,x,import,input-output,-,VkKeyScan

ascii,16,section:.itext,x,import,input-output,T1056 | Input Capture,GetAsyncKeyState

ascii,20,section:.itext,-,import,input-output,-,CopyAcceleratorTable

ascii,15,section:.itext,-,import,input-output,-,SwapMouseButton

ascii,19,section:.itext,x,import,file,-,PathRenameExtension

ascii,15,section:.itext,-,import,file,-,PathQuoteSpaces

ascii,11,section:.itext,-,import,file,-,PathCombine

ascii,9,section:.itext,x,import,file,-,WriteFile

ascii,21,section:.itext,-,import,file,-,GetCompressedFileSize

ascii,17,section:.itext,-,import,file,-,CreateFileMapping

ascii,12,section:.itext,x,import,file,T1083 | File and Directory Discovery,FindNextFile

ascii,16,section:.itext,x,import,execution,-,GetCurrentThread

ascii,20,section:.itext,-,import,execution,-,GetPrivateProfileInt

ascii,7,section:.itext,x,-,execution,T1106 | Execution through API,WinExec

ascii,11,section:.itext,-,import,dynamic-library,-,FreeLibrary

ascii,15,section:.itext,-,import,dynamic-library,-,GetModuleHandle

**Suspected Function Calls**

ascii,57,section:.pdata,-,-,-,-,AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimChaoLyreroeno

ascii,15,section:.pdata,-,-,-,-,KERNEL32.MulDiv

ascii,35,section:.pdata,-,-,-,-,BagsSpicDollBikeAzonPoopHamsPyasmap

ascii,28,section:.pdata,-,-,-,-,KERNEL32.SetCurrentDirectory

ascii,11,section:.pdata,-,-,-,-,BardHolyawe

ascii,20,section:.pdata,-,-,-,-,SHLWAPI.SHFreeShared

ascii,47,section:.pdata,-,-,-,-,BathEftsDawnvilepughThroCymakohloverMitefuzerat

ascii,28,section:.pdata,-,-,-,-,SHLWAPI.PathMakeSystemFolder

ascii,41,section:.pdata,-,-,-,-,BemaCadsPodsWavyCedeRadsbrioOustPerefenom

ascii,21,section:.pdata,-,-,-,-,USER32.SetDlgItemText

ascii,33,section:.pdata,-,-,-,-,BullbonyaweeWaitsnugTierDriblibye

ascii,21,section:.pdata,-,-,-,-,KERNEL32.VirtualQuery

ascii,14,section:.pdata,-,-,-,-,CameValeWauler

ascii,15,section:.pdata,-,-,-,-,USER32.IsIconic

ascii,35,section:.pdata,-,-,-,-,CedeSalsshulLimyThroliraValeDonabox

ascii,18,section:.pdata,-,-,-,-,USER32.CreateCaret

ascii,24,section:.pdata,-,-,-,-,CellrotoCrudUntohighCols

ascii,19,section:.pdata,-,-,-,-,KERNEL32.CreateFile

ascii,25,section:.pdata,-,-,-,-,DenyLubeDunssawsOresvarut

ascii,26,section:.pdata,-,-,-,-,SHLWAPI.PathRemoveFileSpec

ascii,40,section:.pdata,-,-,-,-,DragRoutflusCrowPeatmownNewsyaksSerfmare

ascii,18,section:.pdata,-,-,-,-,USER32.DestroyIcon

ascii,11,section:.pdata,-,-,-,-,Dumpcotsavo

ascii,20,section:.pdata,-,-,-,-,USER32.SetDlgItemInt

ascii,62,section:.pdata,-,-,-,-,DungBadebankBangGelthoboCocaBozotsksWheyVaryShoghoseNipsCadisi

ascii,15,section:.pdata,-,-,-,-,USER32.EndPaint

ascii,58,section:.pdata,-,-,-,-,ExitRollWoodGumsgamaSloerevsWussletssinkYearZitiryesHypout

ascii,19,section:.pdata,-,-,-,-,USER32.GetClassInfo

ascii,15,section:.pdata,-,-,-,-,FociTalcileador

ascii,29,section:.pdata,-,-,-,-,KERNEL32.ConvertDefaultLocale

ascii,10,section:.pdata,-,-,-,-,GeneAilshe

ascii,22,section:.pdata,-,-,-,-,KERNEL32.FindFirstFile

ascii,27,section:.pdata,-,-,-,-,GhisGoodHowlCoonCigscateged

ascii,28,section:.pdata,-,-,-,-,KERNEL32.GetWindowsDirectory

ascii,47,section:.pdata,-,-,-,-,GimpWadsdashHoraYardSeatDeanScanscowRantKeasfib

ascii,20,section:.pdata,-,-,-,-,KERNEL32.LCMapString

ascii,9,section:.pdata,-,-,-,-,Haesourfe

ascii,21,section:.pdata,-,-,-,-,USER32.GetKeyNameText

ascii,35,section:.pdata,-,-,-,-,HoggSoonLasstwaeNapeCeilBawlscopdub

ascii,29,section:.pdata,-,-,-,-,KERNEL32.SystemTimeToFileTime

ascii,13,section:.pdata,-,-,-,-,Icontellnoway

ascii,24,section:.pdata,-,-,-,-,SHLWAPI.PathRemoveBlanks

ascii,32,section:.pdata,-,-,-,-,ImidslatJokyCombdrubChefBilkSale

ascii,21,section:.pdata,-,-,-,-,USER32.GetShellWindow

ascii,56,section:.pdata,-,-,-,-,IzararfsFlamWostAirsconsMouefemelallPoretweeSacsOxidMinx

ascii,24,section:.pdata,-,-,-,-,SHLWAPI.PathAddExtension

ascii,39,section:.pdata,-,-,-,-,JabsNaveFateLariManyLeeksecshiesBawlwoo

ascii,31,section:.pdata,-,-,-,-,KERNEL32.CreateIoCompletionPort

ascii,24,section:.pdata,-,-,-,-,KatsDoreOmerBetsKoraKeef

ascii,25,section:.pdata,-,-,-,-,KERNEL32.GetShortPathName

ascii,12,section:.pdata,-,-,-,-,KineChamLows

ascii,28,section:.pdata,-,-,-,-,KERNEL32.SetCurrentDirectory

ascii,8,section:.pdata,-,-,-,-,LeerMiff

ascii,29,section:.pdata,-,-,-,-,KERNEL32.LeaveCriticalSection

ascii,43,section:.pdata,-,-,-,-,MaarSectFiscNextMattbamsErasnimstoeaBadshon

ascii,19,section:.pdata,-,-,-,-,USER32.GetClassInfo

ascii,31,section:.pdata,-,-,-,-,MarkMokeOsesShwaSkegpornlimemim

ascii,23,section:.pdata,-,-,-,-,KERNEL32.GetStartupInfo

ascii,50,section:.pdata,-,-,-,-,MeanOrrabirogirtWorkGawpSassPirnVinoLotaPledEidefe

ascii,20,section:.pdata,-,-,-,-,SHLWAPI.SHLockShared

ascii,22,section:.pdata,-,-,-,-,NextLoveOralwanySurfhm

ascii,28,section:.pdata,-,-,-,-,KERNEL32.VerSetConditionMask

ascii,47,section:.pdata,-,-,-,-,NisiBoyolineJiaoveryObiaowedblamHaetMaulweensky

ascii,24,section:.pdata,-,-,-,-,SHLWAPI.PathCanonicalize

ascii,32,section:.pdata,-,-,-,-,OastcabskamiKartDumbInksSomsMass

ascii,28,section:.pdata,-,-,-,-,KERNEL32.SetCurrentDirectory

ascii,19,section:.pdata,-,-,-,-,PeckQuinFillrillsaw

ascii,26,section:.pdata,-,-,-,-,KERNEL32.GetThreadPriority

ascii,20,section:.pdata,-,-,-,-,RamilimaputtHastJobs

ascii,21,section:.pdata,-,-,-,-,KERNEL32.FindNextFile

ascii,48,section:.pdata,-,-,-,-,RemsSlaySoreAnoaaxalbuffusesemeuMapsyogaHangLoud

ascii,22,section:.pdata,-,-,-,-,SHLWAPI.PathMakePretty

ascii,23,section:.pdata,-,-,-,-,RidsFineZingMickMomsdue

ascii,21,section:.pdata,-,-,-,-,USER32.GetMonitorInfo

ascii,25,section:.pdata,-,-,-,-,SeminerdsoloseenYaginobox

ascii,25,section:.pdata,-,-,-,-,SHLWAPI.PathIsLFNFileSpec

ascii,34,section:.pdata,-,-,-,-,SiretomsbritGrewIckyNapaLumsBoaren

ascii,24,section:.pdata,-,-,-,-,KERNEL32.OpenFileMapping

ascii,60,section:.pdata,-,-,-,-,SlabKitsSlayseptPfftjiffSabsdeskOafsNowtMemsKirnKepiMiffDunt

ascii,22,section:.pdata,-,-,-,-,KERNEL32.OpenSemaphore

ascii,28,section:.pdata,-,-,-,-,SoldKartAgueiliaRushWauldhal

ascii,17,section:.pdata,-,-,-,-,SHLWAPI.PathIsUNC

ascii,50,section:.pdata,-,-,-,-,SuitplieGunsMaidBaitFeusJiaotodycolyAlbsLuneToyspe

ascii,14,section:.pdata,-,-,-,-,USER32.GetProp

ascii,32,section:.pdata,-,-,-,-,SungActaKopsMaarposyparefuzedeck

ascii,23,section:.pdata,-,-,-,-,SHLWAPI.PathIsDirectory

ascii,43,section:.pdata,-,-,-,-,ToeaTailecusGeesSoliCadeSpueEndsPlaykaphall

ascii,22,section:.pdata,-,-,-,-,SHLWAPI.PathRemoveArgs

ascii,22,section:.pdata,-,-,-,-,Vavsrubepodsjadebrooli

ascii,19,section:.pdata,-,-,-,-,USER32.GetUpdateRgn

ascii,15,section:.pdata,-,-,-,-,VeerCrawFlateel

ascii,29,section:.pdata,-,-,-,-,SHLWAPI.PathParseIconLocation

ascii,27,section:.pdata,-,-,-,-,WainMeekPinyWonkpooflaudsir

ascii,28,section:.pdata,-,-,-,-,KERNEL32.GetWindowsDirectory

ascii,32,section:.pdata,-,-,-,-,WhopTestrangrapsdebsTzarNipaYins

ascii,19,section:.pdata,-,-,-,-,KERNEL32.DeleteFile

ascii,8,section:.pdata,-,-,-,-,YeukMags

ascii,21,section:.pdata,-,-,-,-,KERNEL32.GlobalHandle

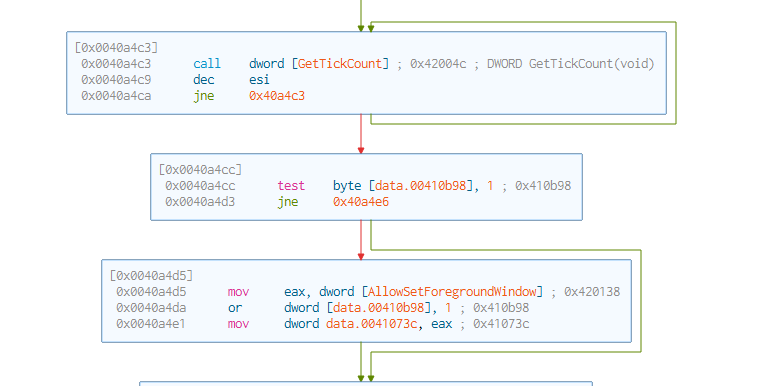
ascii,57,section:.pdata,-,-,-,-,ZetaBeduPirnhipsjailTingSrisTeleAposhuskNameHoerflagemuwo

ascii,15,section:.pdata,-,-,-,-,USER32.LoadIcon

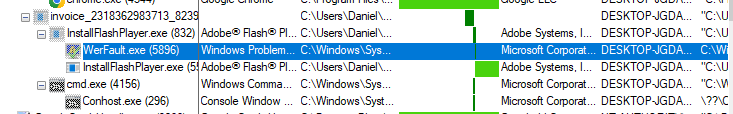
**Libraries**

* SHLAWPI.dll
* KERNEL32.dll
* USER32.dll

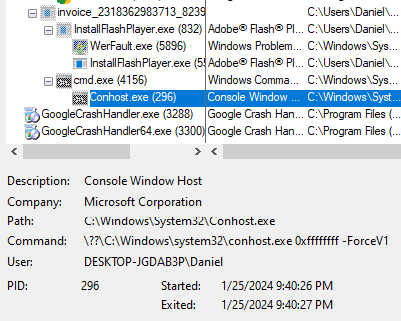
**Advanced Static Code Analysis:**



**Dynamic Code Analysis**



The .exe that the malware used to run



Hidden terminal session behind screen executing