

# Zeus Banking Trojan Report

61  
169

Community Score

61 security vendors and 4 sandboxes flagged this file as malicious

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

invoice\_2318362983713\_823931342io.pdf.exe

Size

247.00 KB

Last Analysis Date

4 days ago

peexe

malware

self-delete

checks-user-input

detect-debug-environment

long-sleeps

direct-cpu-clock-access

via-tor

persistence

suspicious-udp

Reanalyze

Similar

More

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 26

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.zaccess/sirefef

Threat categories

trojan

dropper

Family labels

zaccess

sirefef

wldor

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan.Win32.ZAccess.R87034	Alibaba	Backdoor.Win32.ZAccess.71cb6d44
ALYac	Trojan.ZeroAccess.RN	Antiy-AVL	Trojan[Backdoor]/Win32.ZAccess
Arcabit	Trojan.WLDCR.C	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/Crypt.XPACK.52658
BitDefender	Trojan.WLDCR.C	BitDefender Theta	Gen:NN.Zexaf.36680.pyW@aqPTyGbO
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.4c0e46	Cylance	Unsafe
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS

## VirusTotal Report

## Hashes

**Md5:** ea039a854d20d7734c5add48f1a51c34  
**sha1:** 9615dca4c0e46b8a39de5428af7db060399230b2  
**sha256:** 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

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

## Capa Output

md5	ea039a854d20d7734c5add48f1a51c34
sha1	9615dca4c0e46b8a39de5428af7db060399230b2
sha256	69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
os	windows
format	pe
arch	i386
path	C:/Users/Daniel/Desktop/invoice_2318362983713_823931342io.pdf.exe
ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Virtualization/Sandbox Evasion::System Checks T1497.001
MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Virtual Machine Detection [B0009]
Capability	Namespace
reference anti-VM strings targeting VMWare resolve function by parsing PE exports	anti-analysis/anti-vm/vm-detection load-code/pe

## Basic Static Analysis

names	
file	c:\users\daniel\desktop\invoice_2318362983713_823931342io.pdf.exe
debug	n/a
export	corect.com
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

Research showed this to be a Romanian News Source

property	value
section	section[0]
name	.text
footprint > sha256	8309B5D320B3D392E25AFD5...
entropy	6.707
file-ratio (99.60%)	18.42 %
raw-address (begin)	0x00000400
raw-address (end)	0x0000BA00
raw-size (251904 bytes)	0x0000B600 (46592 bytes)
virtual-address	0x00001000
virtual-size (250379 bytes)	0x0000B571 (46449 bytes)

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,-,-,-,AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimChaoLyroeno  
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

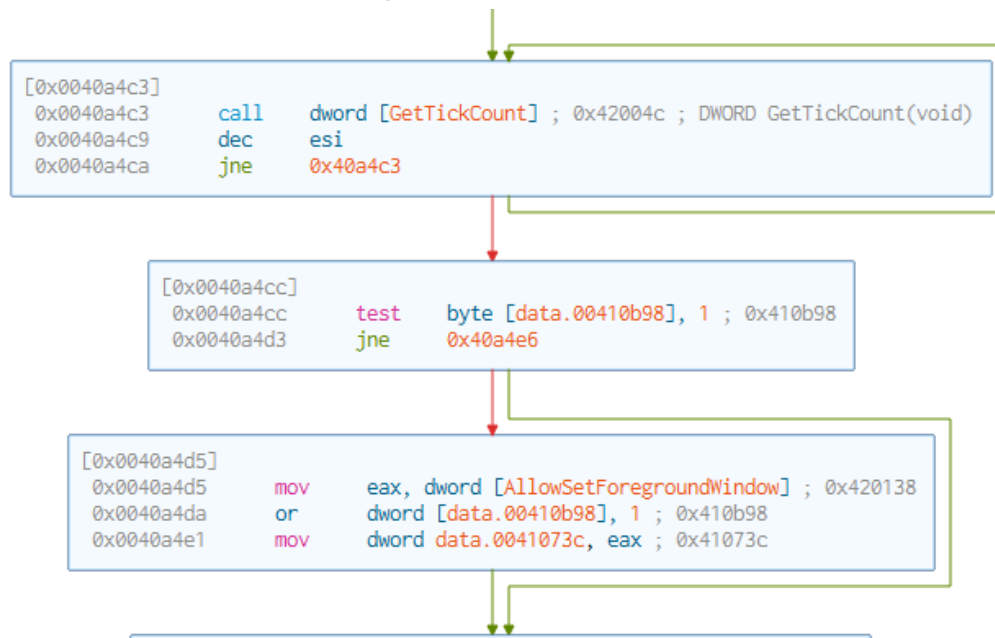
ascii,20,section:.pdata,-,-,-,USER32.SetDlgItemInt  
ascii,62,section:.pdata,-,-,-,DungBadebankBangGelthoboCocaBozotsksWheyVaryShoghoseNi  
psCadisi  
ascii,15,section:.pdata,-,-,-,USER32.EndPaint  
ascii,58,section:.pdata,-,-,-,ExitRollWoodGumsgamaSloerevsWussletssinkYearZitiryesHypout  
ascii,19,section:.pdata,-,-,-,USER32.GetClassInfo  
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,-,-,-,lcontellnoway  
ascii,24,section:.pdata,-,-,-,SHLWAPI.PathRemoveBlanks  
ascii,32,section:.pdata,-,-,-,lmidslatJokyCombdрубChefBilkSale  
ascii,21,section:.pdata,-,-,-,USER32.GetShellWindow  
ascii,56,section:.pdata,-,-,-,lzararfsFlamWostAirsconsMouefemelallPoretweeSacsOxidMinx  
ascii,24,section:.pdata,-,-,-,SHLWAPI.PathAddExtension  
ascii,39,section:.pdata,-,-,-,JabsNaveFateLariManyLeeksecshiesBawlwoo  
ascii,31,section:.pdata,-,-,-,KERNEL32.CreateloCompletionPort  
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,-,-,-,MaarSectFiscNextMattbamsErasmusstoeaBadshon  
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,-,-,-,NextLoveOralwanySurfhn  
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,-,-,-,RemsSlaySoreAnoaaxalbuffusesemeuMapsयोगाHangLoud  
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,-,-,-,SiretomsbritGrewlckyNapaLumsBoaren  
ascii,24,section:.pdata,-,-,-,KERNEL32.OpenFileMapping  
ascii,60,section:.pdata,-,-,-,SlabKitsSlayseptPfftjiffSabsdeskOafsNowtMemskirnKepiMiffDunt  
ascii,22,section:.pdata,-,-,-,KERNEL32.OpenSemaphore  
ascii,28,section:.pdata,-,-,-,SoldKartAgueliaRushWauldhal  
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.PathParselconLocation  
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

- SHLWAPI.dll
- KERNEL32.dll
- USER32.dll

## Advanced Static Code Analysis:



## Dynamic Code Analysis

chrome.exe (7577)	Google Chrome	C:\Program Files\Google\Chrome\chrome.exe	Google LLC	DESKTOP-JGDA...	C:\U...
invoice_2318362983713_8239		C:\Users\Daniel\...		DESKTOP-JGDA...	"C:\U...
InstallFlashPlayer.exe (832)	Adobe® Flash® Pl...	C:\Users\Daniel\...	Adobe Systems, I...	DESKTOP-JGDA...	"C:\U...
WerFault.exe (5896)	Windows Problem...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-JGDA...	C:\W...
InstallFlashPlayer.exe (5...	Adobe® Flash® Pl...	C:\Users\Daniel\...	Adobe Systems, I...	DESKTOP-JGDA...	"C:\U...
cmd.exe (4156)	Windows Comma...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-JGDA...	"C:\W...
Conhost.exe (296)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-JGDA...	\??\C...

The .exe that the malware used to run

invoice_2318362983713_8239		C:\Users\Daniel\...
InstallFlashPlayer.exe (832)	Adobe® Flash® Pl...	C:\Users\Daniel\...
WerFault.exe (5896)	Windows Problem...	C:\Windows\Sys...
InstallFlashPlayer.exe (5)	Adobe® Flash® Pl...	C:\Users\Daniel\...
cmd.exe (4156)	Windows Comma...	C:\Windows\Sys...
Conhost.exe (296)	Console Window ...	C:\Windows\Syst...
GoogleCrashHandler.exe (3288)	Google Crash Han...	C:\Program Files (...)
GoogleCrashHandler64.exe (3300)	Google Crash Han...	C:\Program Files (...)

Description:	Console Window Host		
Company:	Microsoft Corporation		
Path:	C:\Windows\System32\Conhost.exe		
Command:	\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1		
User:	DESKTOP-JGDAB3P\Daniel		
PID:	296	Started:	1/25/2024 9:40:26 PM
		Exited:	1/25/2024 9:40:27 PM

Hidden terminal session behind screen executing