**Analysis of Zeus Banking Trojan Report**

**Fingerprint**

-

|  |  |
| --- | --- |
| **Hashes** | ea039a854d20d7734c5add48f1a51c34 **MD5**  69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169 **SHA256**  9615dca4c0e46b8a39de5428af7db060399230b2 SHA1 |

A screenshot of a computer

Description automatically generated

A screenshot of a computer code

Description automatically generated

**CPU: 32-bit**

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

**Basic Static Analysis**

**Domain: corect.com**

**corect.com yielded no interesting results.**

**A screenshot of a computer

Description automatically generated**

**API Calls**

* **AllowSetForegroundWindow**: Enables the specified process to set the foreground window using the SetForegroundWindow function. The calling process must already be able to set the foreground window.
* **GetEnvironmentVariable**
* **GetEnvironmentVariable**
* **VkKeyScan**
* **GetAsyncKeyState**
* **PathRenameExtension**
* **WriteFile**
* **FindNextFile**
* **GetCurrentThread**
* **WinExec**
* **GlobalAddAtom**
* **GetClipboardOwner**
* **GetClipboardData**
* **EnumClipboardFormats**
* **DdeQueryNextServer**
* **GetConsoleAliasExesLength**
* **SetCurrentDirectory**
* **CallWindowProc**
* **UpdateWindow**
* **GetCapture**
* **IsWindowEnabled**
* **GetWindowTextLength**
* **DeleteCriticalSection**
* **SizeofResource**
* **GetLogicalDrives**
* **GetTickCount**
* **GetDriveType**
* **LocalUnlock**
* **HeapFree**
* **VirtualQueryEx**
* **LocalAlloc**
* **LocalFree**
* **CopyAcceleratorTable**
* **SwapMouseButton**
* **PathQuoteSpaces**
* **PathCombine**
* **GetCompressedFileSize**
* **CreateFileMapping**
* **GetPrivateProfileInt**
* **FreeLibrary**
* **GetModuleHandle**

**Suspected Function Calls**

* **AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimChaoLyreroeno**
* **KERNEL32.MulDiv**
* **BagsSpicDollBikeAzonPoopHamsPyasmap**
* **KERNEL32.SetCurrentDirectory**
* **BardHolyawe**
* **SHLWAPI.SHFreeShared**
* **BathEftsDawnvilepughThroCymakohloverMitefuzerat**
* **SHLWAPI.PathMakeSystemFolder**
* **BemaCadsPodsWavyCedeRadsbrioOustPerefenom**
* **USER32.SetDlgItemText**
* **BullbonyaweeWaitsnugTierDriblibye**
* **KERNEL32.VirtualQuery**
* **CameValeWauler**
* **USER32.IsIconic**
* **CedeSalsshulLimyThroliraValeDonabox**
* **USER32.CreateCaret**
* **CellrotoCrudUntohighCols**
* **KERNEL32.CreateFile**

A screenshot of a computer

Description automatically generated

* **DenyLubeDunssawsOresvarut**
* **SHLWAPI.PathRemoveFileSpec**
* **DragRoutflusCrowPeatmownNewsyaksSerfmare**
* **USER32.DestroyIcon**
* **Dumpcotsavo**
* **USER32.SetDlgItemInt**
* **DungBadebankBangGelthoboCocaBozotsksWheyVaryShoghoseNipsCadisi**
* **USER32.EndPaint**
* **ExitRollWoodGumsgamaSloerevsWussletssinkYearZitiryesHypout**
* **USER32.GetClassInfo**
* **FociTalcileador**
* **KERNEL32.ConvertDefaultLocale**
* **GeneAilshe**
* **KERNEL32.FindFirstFile**
* **GhisGoodHowlCoonCigscateged**
* **KERNEL32.GetWindowsDirectory**
* **GimpWadsdashHoraYardSeatDeanScanscowRantKeasfib**
* **KERNEL32.LCMapString**
* **Haesourfe**
* **USER32.GetKeyNameText**
* **HoggSoonLasstwaeNapeCeilBawlscopdub**
* **KERNEL32.SystemTimeToFileTime**
* **Icontellnoway**
* **SHLWAPI.PathRemoveBlanks**
* **ImidslatJokyCombdrubChefBilkSale**
* **USER32.GetShellWindow**
* **IzararfsFlamWostAirsconsMouefemelallPoretweeSacsOxidMinx**
* **SHLWAPI.PathAddExtension**
* **JabsNaveFateLariManyLeeksecshiesBawlwoo**
* **KERNEL32.CreateIoCompletionPort**
* **KatsDoreOmerBetsKoraKeef**
* **KERNEL32.GetShortPathName**
* **KineChamLows**
* **KERNEL32.SetCurrentDirectory**
* **LeerMiff**
* **KERNEL32.LeaveCriticalSection**
* **MaarSectFiscNextMattbamsErasnimstoeaBadshon**
* **USER32.GetClassInfo**
* **MarkMokeOsesShwaSkegpornlimemim**
* **KERNEL32.GetStartupInfo**
* **MeanOrrabirogirtWorkGawpSassPirnVinoLotaPledEidefe**
* **SHLWAPI.SHLockShared**
* **NextLoveOralwanySurfhm**
* **KERNEL32.VerSetConditionMask**
* **NisiBoyolineJiaoveryObiaowedblamHaetMaulweensky**
* **SHLWAPI.PathCanonicalize**
* **OastcabskamiKartDumbInksSomsMass**
* **KERNEL32.SetCurrentDirectory**
* **PeckQuinFillrillsaw**
* **KERNEL32.GetThreadPriority**
* **RamilimaputtHastJobs**
* **KERNEL32.FindNextFile**
* **RemsSlaySoreAnoaaxalbuffusesemeuMapsyogaHangLoud**
* **SHLWAPI.PathMakePretty**
* **RidsFineZingMickMomsdue**
* **USER32.GetMonitorInfo**
* **SeminerdsoloseenYaginobox**
* **SHLWAPI.PathIsLFNFileSpec**
* **SiretomsbritGrewIckyNapaLumsBoaren**
* **KERNEL32.OpenFileMapping**
* **SlabKitsSlayseptPfftjiffSabsdeskOafsNowtMemsKirnKepiMiffDunt**
* **KERNEL32.OpenSemaphore**
* **SoldKartAgueiliaRushWauldhal**
* **SHLWAPI.PathIsUNC**
* **SuitplieGunsMaidBaitFeusJiaotodycolyAlbsLuneToyspe**
* **USER32.GetProp**
* **SungActaKopsMaarposyparefuzedeck**
* **SHLWAPI.PathIsDirectory**
* **ToeaTailecusGeesSoliCadeSpueEndsPlaykaphall**
* **SHLWAPI.PathRemoveArgs**
* **Vavsrubepodsjadebrooli**
* **USER32.GetUpdateRgn**
* **VeerCrawFlateel**
* **SHLWAPI.PathParseIconLocation**
* **WainMeekPinyWonkpooflaudsir**
* **KERNEL32.GetWindowsDirectory**
* **WhopTestrangrapsdebsTzarNipaYins**
* **KERNEL32.DeleteFile**
* **YeukMags**
* **KERNEL32.GlobalHandle**
* **ZetaBeduPirnhipsjailTingSrisTeleAposhuskNameHoerflagemuwo**
* **USER32.LoadIcon**

**Libraries:**

* **SHLWAPI.dll - Shell Light-weight Utility Library**
* **KERNEL32.dll - Windows NT BASE API Client**
* **USER32.dll - Multi-User Windows USER API Client Library**

**Capa Output**

**A screenshot of a computer

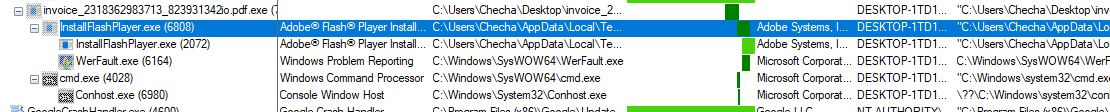
Description automatically generated**

**Advance Static Analysis**

**A screenshot of a computer program

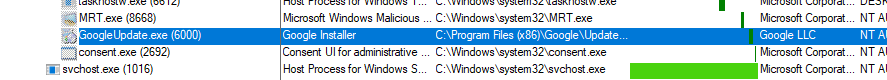
Description automatically generated**

**Basic Dynamic Analysis**

****

**A screenshot of a computer

Description automatically generated**

****

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Msimg32.dll file**

**A screenshot of a computer

Description automatically generated**

**YARA (IOC)**