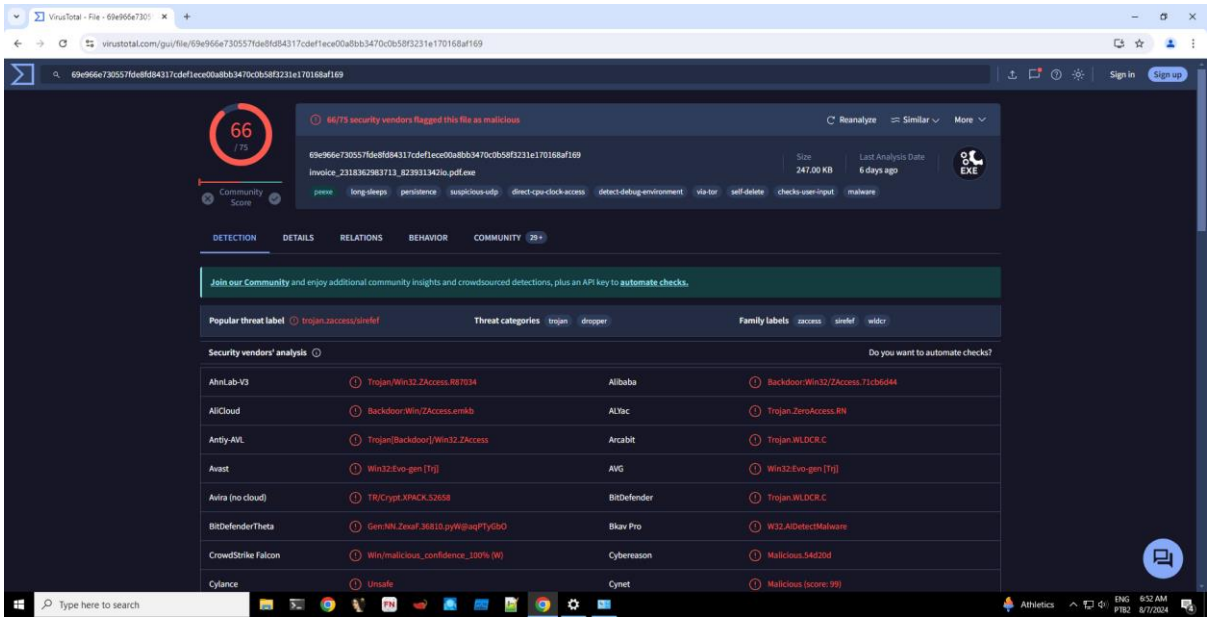
Fingerprint

VirusTotal Output



-VirusTotal output to the .exe archive

Hashes: sha256 > 69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169

Filename: invoice_2318362983713_823931342io.pdf.exe

property	value
footprint > sha256	69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z ..... @ .....
file > size	252928 bytes

-Hashes and first bytes provided by PeStudio

Basic Static Analysis

names	
file	c:\users\flarevm\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

-export domain reported by PeStudio

Nothing exceptional found in corect.com

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)

-Raw size and virtual size almost the same, probably the file isn't packed

API Calls

- AllowSetForegroundWindow
- GetEnvironmentVariable
- GetEnvironmentVariable
- VkKeyScan: Translates a character to the corresponding virtual-key code and shift state for the current keyboard.
- GetAsyncKeyState: Determines whether a key is up or down at the time the function is called, and whether the key was pressed after a previous call to **GetAsyncKeyState**.
- PathRenameExtension
- WriteFile
- FindNextFile
- GetCurrentThread
- WinExec
- GlobalAddAtom: Adds a character string to the global atom table and returns a unique value (an atom) identifying the string.
- GetClipboardOwner
- GetClipboardData
- EnumClipboardFormats: Clipboard data formats are stored in an ordered list. To perform an enumeration of clipboard data formats, you make a series of calls to the **EnumClipboardFormats** function. For each call, the *format* parameter specifies an available clipboard format, and the function returns the next available clipboard format.
- DdeQueryNextServer: Retrieves the next conversation handle in the specified conversation list.
- GetConsoleAliasExesLength
- SetCurrentDirectory
- CallWindowProc
- UpdateWindow
- GetCapture

- IsWindowEnabled
- GetWindowTextLength
- DeleteCriticalSection
- SizeofResource
- GetLogicalDrives
- GetTickCount
- GetDriveType
- LocalUnlock
- HeapFree: Frees a memory block allocated from a heap by the HeapAlloc or HeapReAlloc function.
- VirtualQueryEx: Retrieves information about a range of pages within the virtual address space of a specified process.
- LocalAlloc
- LocalFree
- CopyAcceleratorTable: Copies the specified accelerator table. This function is used to obtain the accelerator-table data that corresponds to an accelerator-table handle, or to determine the size of the accelerator-table data.
- SwapMouseButton
- PathQuoteSpaces
- PathCombine
- GetCompressedFileSize
- CreateFileMapping
- GetPrivateProfileInt
- FreeLibrary
- GetModuleHandle: Retrieves a module handle for the specified module. The module must have been loaded by the calling process.

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
- 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

KERNEL32.dll

USER32.dll

Capa Output

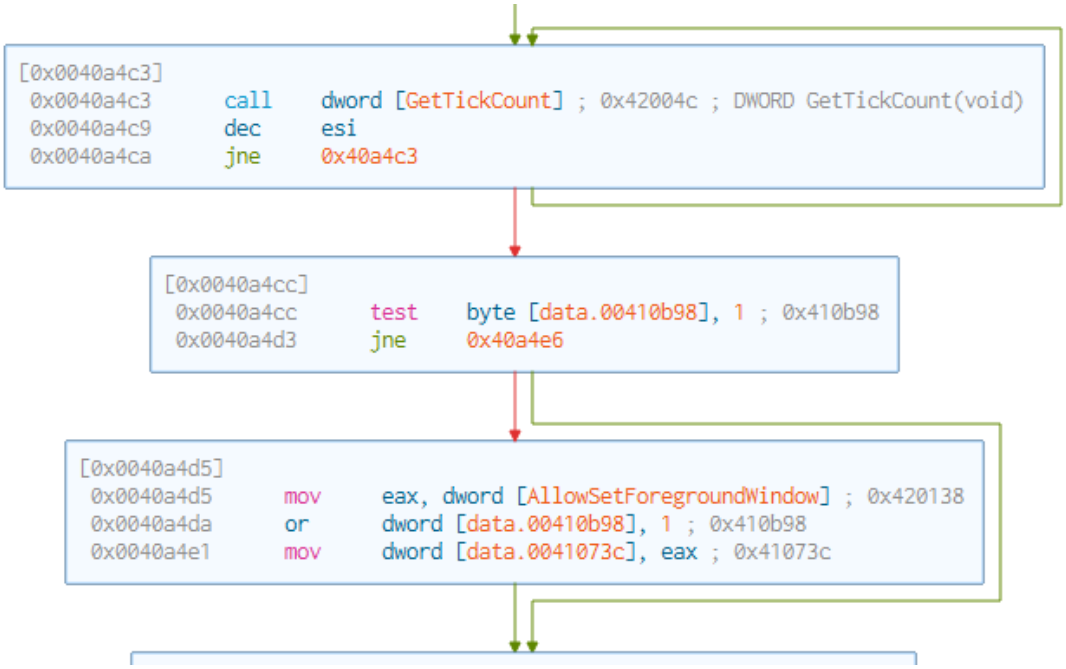
```
C:\Users\FlareVm\Desktop
λ capa .\invoice_2318362983713_823931342io.pdf.exe
┌──────────┬──────────────────────────────────────────────────────────────────┐
│ md5      │ ea039a854d20d7734c5add48f1a51c34                                 │
│ sha1     │ 9615dca4c0e46b8a39de5428af7db060399230b2                         │
│ sha256   │ 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169 │
│ analysis │ static                                                           │
│ os       │ windows                                                          │
│ format   │ pe                                                               │
│ arch     │ i386                                                             │
│ path     │ C:/Users/FlareVm/Desktop/invoice_2318362983713_8239313421o.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   │ anti-analysis/anti-vm/vm-detection │
│ resolve function by parsing PE exports       │ load-code/pe                 │
└──────────────────────────────────────────────┴──────────────────────────────┘
```

Advanced Static Analysis

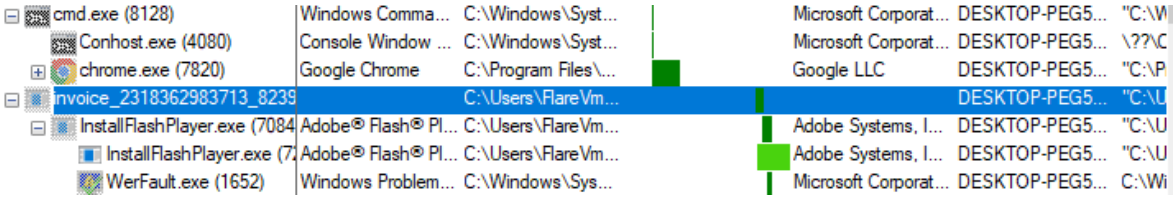


-Execution behavior on the API calls “GetTickCount” and “AllowSetForegroundWindow”

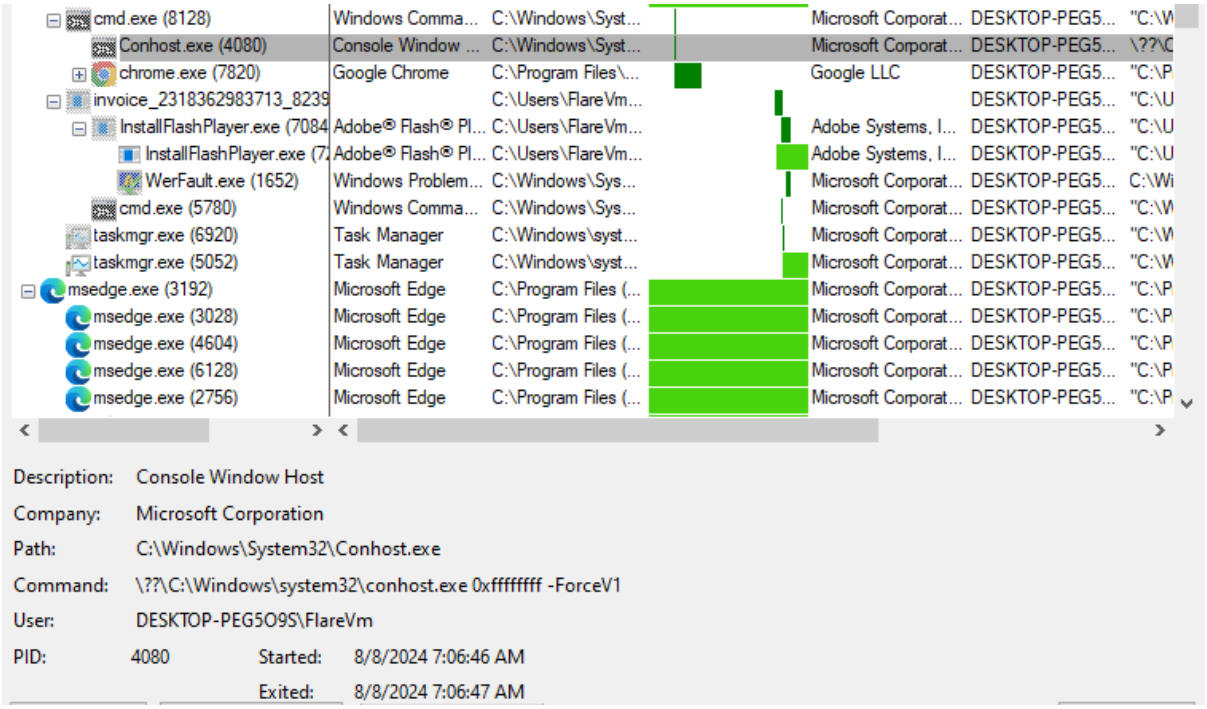
```
0x0043397a      je      0x4339eb
0x0043397c      push    0x43686769 ; 'ighC'
0x00433981      outsd   dx, dword [esi]
0x00433982      insb    byte es:[edi], dx
0x00433983      jae     0x433985
0x00433985      dec     ebx
```

- “CellrotoCrudUntohighCols” and “KERNEL32.CreateFile executions

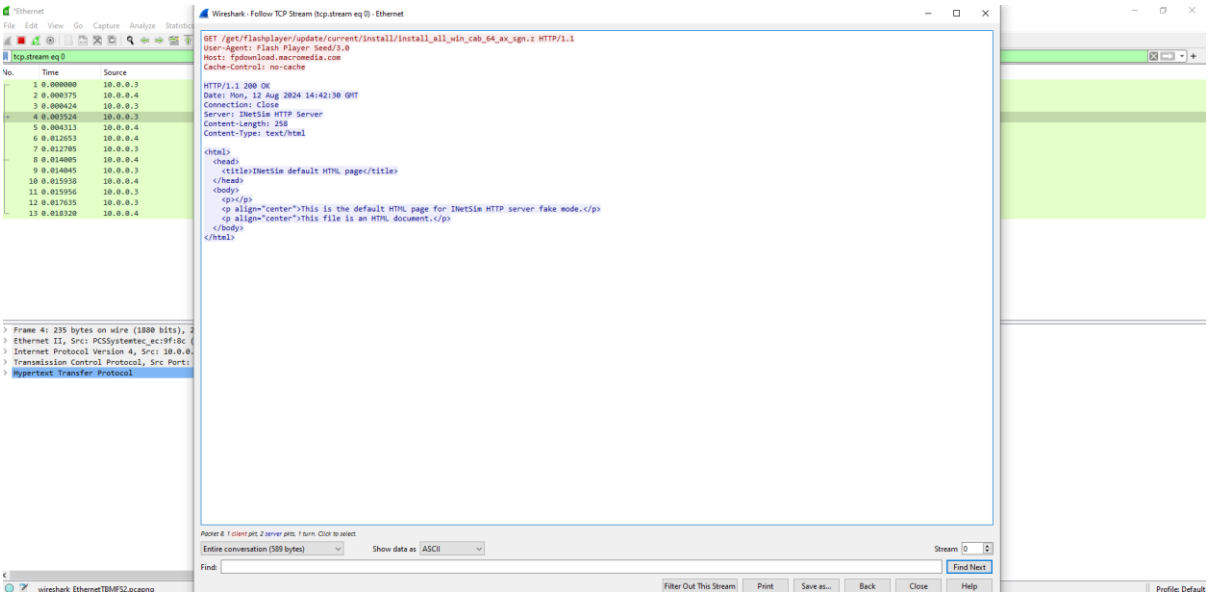
Basic Dynamic Analysis



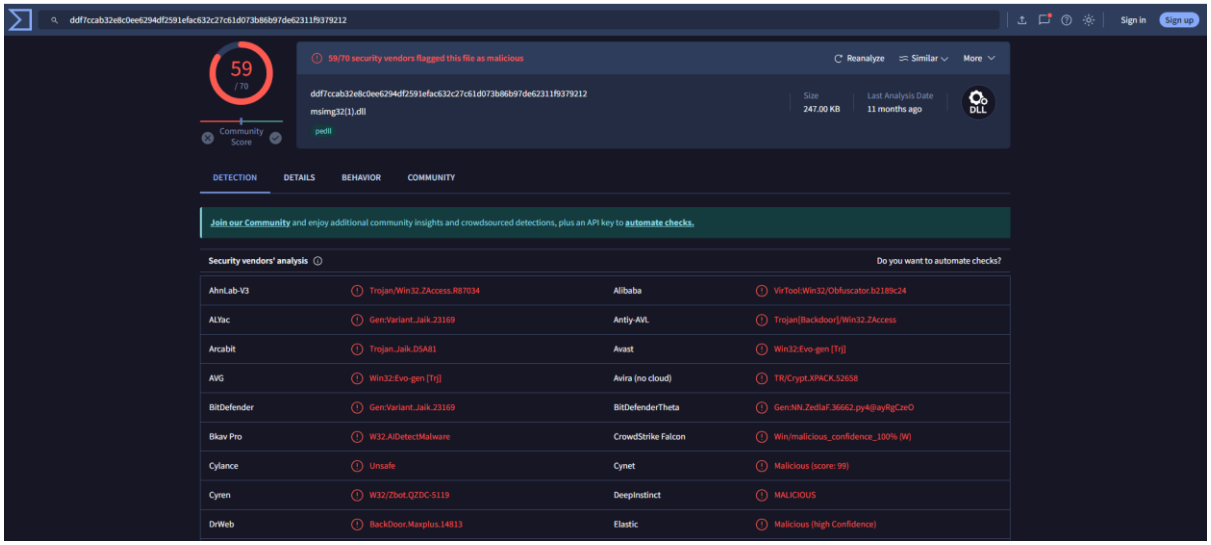
- After the .exe execution the file deleted itself, but a process with the same name stills running.



-Console running in background



-GET Request captured after the malware execution.



-DLL found in the same folder than the invoice.exe that is running in background, created after the malware execution.

YARA Rule

rule Zeus {

meta:

author="Gabriel Borges"

description="Detections rules for ZeusBankingVersion_26Nov2013"

strings:

$file_name="invoice_2318362983713_823931342io.pdf.exe" ascii

//Suspected name of functions and DLL functionalities.

$function_name_KERNEL32_CreateFileA="CellrotoCrudUntohighCols" ascii

// PE Magic Byte.

$PE_magic_byte="MZ"

//Hex String Function name.

$hex_string = {43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72}

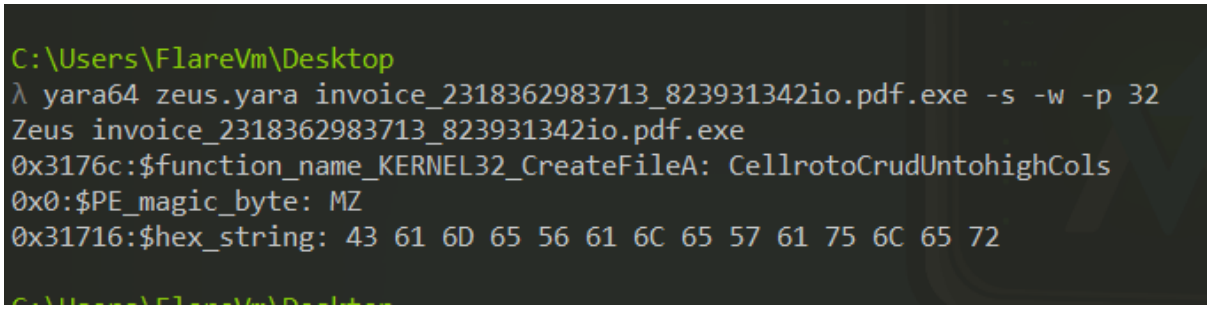
condition:

$PE_magic_byte at 0 and $file_name

and $function_name_KERNEL32_CreateFileA

or $hex_string

}



-Lines found in the malware that combines with the YARA rule.