

# **MALWARE ANALYSIS REPORT.**

**MALWARE FILE NAME :-** zeusbankingversion-  
26thnovember2013

## **ZEUS MALWARE INTRODUCTION.**

1. If you know about Greek myths or enjoy Marvel comics, you probably know the name "Zeus."
2. "Zeus" is the Greek god of sky and thunder.
3. but the "Zeus" we are referring is to is malware called(zbot)
4. it is a financial or banking trojan.
5. it was first created in the year 2007 by eastern Europe hackers.

## **NOTIFICATION: -**

Please Note That the Information Provided Here Are Given According to Our Findings. And IF You Want to Do Further Analysis You Can Do So But We Are Not Responsible for Any Loss You Go To. Please Be Careful While Dealing with Malware.

## **SUMMARY: -**

1. its main purpose is to steal the people financial data and adding machines to bot net.
2. the source code of this trojan came into public in early 2011.

3. the fbi and united states department of justice estimated in 2014 that up to 1 million computers around world are infected by this trojan.

### **TOOLS USED: -**

- |  |  |
|--|--|
| 1. pestudio(master),<br>2. virus total(antivirus scanning),<br>3. floss(strings),<br>4. cutter(strings),<br>5. hxd(hexbytes),<br>6. capa(string),<br>7. cmder(file type),<br>8. hashcal(hash),<br>9. hashmyfiles(hash),<br>10. xorsearch(url),<br>11. exeinfo pe(packing ).etc., | 12.procman(child process).<br>13.process hacker(windows process).<br>14.cutter, 15.yara(IOC).<br>16.wireshark(capture traffic).<br>17.regshot(winregkeys), etc., |
|--|--|

### **STATIC ANALYSIS: -**

this type of analysis does not involve the installation of malware into the system, its safe and a secure way to analyse the data.

### **FOOTPRINT: -**

### **HASHES: -**

md5 : - ea639a854d26d7734cSadd48f1851c34

Sha1 :- 9615dca4c6e46bSa39de54288'F7db666399236b2

sha256 :-

69e966e736557fde8fd84317cdef1eceeeaaSbb3476c6b58f3231e1761  
68af169

FLARE-VM 04-01-2024 13:32:10.00 C:\Users\flarevm\Desktop>capa.exe invoice_2318362983713_823931342io.pdf.exe	
md5	ea039a854d20d7734c5add48f1a51c34
sha1	9615dca4c0e46b8a39de5428af7db060399230b2
sha256	69e966e730557fde8fd84317cdef1ece00a8bb3476c0b58f3231e170168af169
os	windows
format	pe
arch	i386
path	C:/Users/flarevm/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

pestudio 9.56 - Malware Initial Assessment - www.winitor.com - [c:\users\flarevm\desktop\invoice_2318362983713_823931342io.pdf.exe] - [read-only]	
file settings about	
footprint (11)	value
general	69e966e730557fde8fd84317cdef1ece00a8bb3476c0b58f3231e170168af169 6960fdc23907135d98201041a838ba22d0d9d327c4a16ada1037bb1daa1197 5d85fea79e73b682ff8f35296c9c506b0960112f9bc275078e096295eff0844 cd3c66cd8241d5059fd2e1c841b183e51e14537ff84485de626a3a2e873abff6 830965d32083d39e25afdf577936b89d54a3aea6a99775963b08f3387b352 510a0ff9faf189356c7819a65cbef1da1094ea1101581e1c4d3bc8752c4598a5 4cdd509821cc0790a1d7031ef6c03dfa9e68b967279d1802f0de781ebc895389 70cc3e035cced2208e4eb21e54b904a2e0cce085c080e292a1e12e7c8190b0a5 c81c8914ad761c96bf86506306e31a094df71b078c94905efbf080d289c54f 7c2fc4cd849369f9082a41459cb3fb96e89e9ff008631b7c6562467fd0892a89 manifest sha256 781aa123142f5551abc80d75e34cb3e246863412352762a0580e4f3244616c9d
special	imphash > md5 n/a
cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0000A3B6	

FILE TYPE: -

text M 2.....

architect :- windows && arch i386-32bit

File analysis results for invoice\_2318362983713\_823931342i.pdf.exe:

- File Properties:**
  - Filepath: c:\users\flarevm\Desktop\invoice\_2318362983713\_823931342i.pdf.exe
  - File Type: executable
  - CPU: 32-bit
  - Subsystem: GUI
  - Entry Point: 0x0000A3B6
- Characteristics:**
  - indicators (directory > invalid)
  - footprints (count > 11)
  - virusotal (error)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 152 bytes)
  - rich-header (tooling > Visual Studio)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (invalid)
  - sections (characteristics > self-modifying)
  - libraries (count > 3)
  - imports (flag > 77)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (n/a)
  - resources (count > 11)
  - strings (count > 1416)
  - debug (n/a)
  - manifest (level > asInvoker)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)
- Stamps:**
  - compiler-stamp: Mon Nov 25 10:32:03 2013 | UTC
  - debug > stamp: n/a
  - resource-stamp: n/a
  - import-stamp: n/a
  - export-stamp: Mon Nov 25 10:32:01 2013 | UTC
- Names:**
  - file: c:\users\flarevm\Desktop\invoice\_2318362983713\_823931342i.pdf.exe
  - debug: n/a
  - export: corect.com
  - version: n/a
  - manifest: n/a
  - .NET > module: n/a

## SCANNING: -

libraries found =3 : -

SHLWAPI.dll

KERNEL32.dll

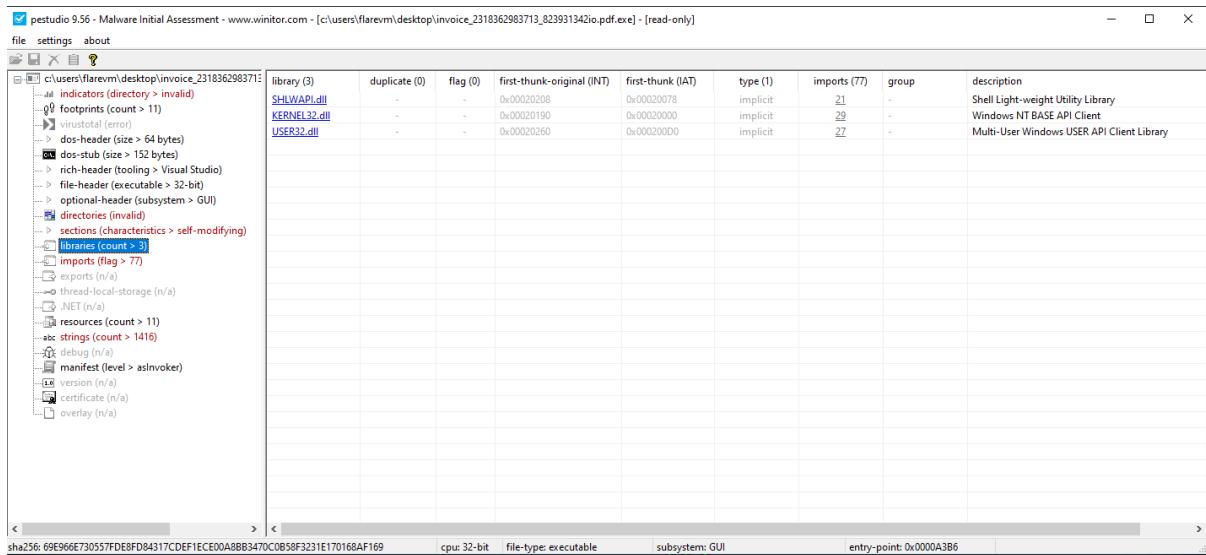
USER32.dll

VirusTotal Analysis for ZeusBankingVersion\_26Nov2013.zip

Community Score: 4 / 90

4 security vendors flagged this URL as malicious

Vendor	Detection	Notes	
Avira	Malware	Dr.Web	Malicious
Kaspersky	Malware	Sophos	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Anti-AVL	Clean	Artists Against 419	Clean



## STRINGS: -

+-----+

| FLOSS STATIC STRINGS: ASCII (799) |

+-----+

9x66664d !This program cannot be run in DOS mode.

9x6666c8 Rich

axeeelde .text

9x6661¥7 '.data

9x666229 .iText

9x666248 .pdata

9x666279 .rsrc

9x666297 @.reloc

9x666568 jrjy

9x6666e5 SVH;

9x66673d QATt

9x666846 SVHS

exeeeaez Km}e+

axeeded

=#NEwlTMMMONvJ2NRO+0sndo4deYoJ1qiQeJ3gyK8qRQQGyHDDzet  
olmnR7tLSH7SL

axeeeeas cT6b

9x666ebb

85+1ZPH41XHU4HObuTGHaOAzaZA[wib8g9FcaXIQRq,tuo{whoeBH  
GIINQNRk6n2[ONGla8p7etGiUY

9x66165d eQNP

Bxeelead 091RP3

6x6611a4 jxjp

Bxeellee fBA

9x66129c Q—m\$~hP

9x661749 we'.

9x66175d

cRR/3dQ7BZ4+hGiCezccLHVghOVupeij6X9n¥V7FUHijTtxFPttcPdNSHIT  
o

9x66194d \erP

9x661eb8 VH

6x662254

KmsKrGNXcleaNvgLK[E5395tN737Rt/fteq3tLHXNBIRXNZvZ{AtVR8b  
VP59jVsLREmc4GF

9x6622dc ul—n

axeezzfa

4a26X6:9F9HG[OSOX/viSQL6YEHRi5H1d0564wbvpsdgoih£1h{Bv40:1

2mFgGv1K9si3a50yv{ppH[eYuyzUeJa

9x6624ac

UJ6tr3h3xivEdiGTmuHHemlqkyx7CwEX[ey+8xf9:BmIpvJAcGIH61{eX3,  
T1bq3woZImjGOVN{bSBhZBQHKETIKnL8cR

9x682613 j\tY3

9x96328b \_(hRP

9x6632ca }nRV

9x663568 j%H?

9x66357e

YoHQGRRSPP[C[euJDeQUEnSHhZzI[CxukluNeeV/StqKDCy7HnZJOcaaip21Hd2P1DOPctgYEYHgl

9x663643

frysBj+zSKXOJZiVJBRI+dSlo182meEGoS4jlUPn77IK9dIKH8utP4iScHEmy4yZF/Sg6

6x663764

veaSTZZHKISKnFcuo7LReZQVsVH[y153v4tTrSkikjT1jK82m31be:+6rihZ  
GableuctQL

6x66393f uisq/

9x66395d

NfL4bNeVlBVSGkyY+ZZqQ89VBGOXOqIXbK8P+TE9ejaG4hxF8,aEa832  
L3v651uu82xF+2Hz8viTe

9x663bba

efj4xot2vZRJjEoRX38+YvXqQEy6b+EnHHjqmyiBGfpSFIHcBodHlxIBHd:  
HDGIIURyPGQ

9x663cee

OIUigAtF7ryLy4FbZ/eYt2KZ[bzntHbm6JeItCykvwHtZZt4sI{j,zu9b+3

6x663def qF

9x663e6b

i:sgDkISilzgl:JOCybhZRVQF[lkhSuS4w7Dx56:p57ctRgKE{BwICHuMTSs  
HQdcnnebVw4Px7jieewJS3Y

9x663ebd —

TTUQ14DQix58HLScboyKRSSrwoqgeKTHvK4QIGxNOKv9smBabFieVbl  
AneNHeHeJXRSStBlecnGHy{/onsEf

9x664b5e jqjm

9x664c97 jojb

0x01e6d2 PathRelativePathTow

0x01e6e8 PathParseIconLocationH

0x01e702 ChPCmpIA

0x01e70e PathIsPrefixA

0x01e71e PathRenameExtensionA

0x01e736 PathIsRootH

0x61e744 PathQuoteSpacesA

0x01e758 PathCombineH

0x01e768 PathAddExtensionH

0x01e77c ChPCmpIH

0x01e788 PathIsUNCSeePA  
0x01e79c PathIsSameRootA  
6x01e7ae PathIsRelativeA  
6x01e7c0 PathHakeSystemFoldePA  
6x01e7d8 IsChaPSpaceA  
6x61e7e8 PathHatchSpecH  
6x61e7fa StPCmpNIA  
6x61e866 PathRemoveAPgsA  
6X61e816 SHLHAPI.dll  
6x61e824 LocalUnlock  
6x61e832 GetEnvironmentVaPiableH  
6x61e84c GetSystemDefaultUILanguage  
0x01e868 FreeLibPaPy  
0X01e878 GlobalAddAtomA  
0x01e88a HeapFPe  
0x01e896 GetLogicalDPives  
0x01e8aa GetSystemDefaultLCID  
0x61e8c2 GetHoduleHandleH  
0X61e8d6 GetTickCount  
6X61e8e6 GetCurrentThread  
0x61e8fa IsBadReadPtr  
0xe1eQGa VirtualQueryEx

0x01e91c HriteFile  
0x01e928 GetDriveTypeA  
0x01e938 SizeofResource  
0x01e94a GetConsoleAliasExesLengthw  
0x01e968 GetCompressedFileSizeA  
0x01e982 GetEnvironmentVariableA  
0x01e99c GetPrivateProfileIntH  
0x01e9b4 CreateFileHappingA  
0x01e9ca LocalAlloc  
0x01e9d8 SetCurrentDirectoryH  
0x61e9f6 GetOEHCP  
0x61e9fc FindNextFileA  
exe1eaec GetUserDefaultUILanguage  
0x61e828 DeleteCPiticalSection  
0x61ea40 HinExeC  
0x61ea4a LocalFPe  
exe1ea54 KERNEL32.dll  
0x01e864 VkKeyScanA  
0x01ea72 GetClipboardOwner  
0x01e886 CallHindowPPocH  
9x919398 GPTPPaqqnpfAUTTlavnuT

## | FLOSS STATIC STRINGS: UTF-16LE (1) |

```
+-----+
```

0x9311bc C”#\$%&'{}“+,—.f6123456789:;<

## FLOSS STACK STRINGS (2)

Function | Function Offset | Frame Offset | String

```
-----+-----+-----+
```

9x49142f | ex4ebc18 | 6x34 | celv

0x401a5f | ex4ebc68 | 0x9f | 091p

## FLOSS TIGHT STRINGS (6)

## FLOSS DECODED STRINGS (66)

```
+-----+-----+
```

## | FUNCTION at 6X462aaf (1) |

```
+-----+-----+
```

Offset | Called At | String

```
-----+-----+
```

[stack] | 6x49887f | GBKn

```
+-----+-----+
```

## | FUNCTION at 6x46592c (28) |

```
+-----+-----+
```

Offset | Called At | String

```
-----+-----+
```

[stack] | 6x497337 | PiAb:\$a

[stack] | 0x497337 | piAc:\$a

[stack] | 6x497337 | iAda

[stack] | 6x497337 | iAea

[stack] | 6x497337 | iAfa

[stack] | 6x497337 | iAga

r.|-.l.'l|n-nn~r::7|1M"

```
FLOSS STATIC STRINGS (791)

+-- FLOSS STATIC STRINGS: ASCII (790) |
+-----+
0x00004d !This program cannot be run in DOS mode.
0x0000c8 Rich
0x0001d0 .text
0x0001f7 ` .data
0x000220 .iText
0x000248 .pdata
0x000270 .rsrc
0x000297 @.reloc
0x000568 jrjy
0x0006e5 SVW;
0x00073d 9ATt
0x000846 SVWS
0x000a02 Km}@+
0x000ded =#NEw1zUTMNNONvJ2NRo+OjJzndo4djQeYoJ1UoqiQeJ3gyK8RpqRQ9GyWDDzetolmnR7tLSM7SL
0x000ea5 cT6b
0x000ebb 85+IZrM4lXHU4HObuTGHa0AzaZA[w1b8g0FcaXI9HRuGp,tuo{who0BHGlNQNRk6n2[ON0Ia8p7etGiUY
0x00105d e9NP
0x0010ad 091RP3
0x0011a4 jxjp
0x0011ee f3A
0x00129c Q-m$~hP
0x001740 we'.
0x00175d cRR/3dQ7BZ4+hGiCezccLHVgh0Vupxr2Rjmj6X9qgVfV7FUHi9bjTlhYxFPxVttgXcPdNSHITo
0x00194d \erP
0x001eb8 Vw<S
0x002254 KmsKr6NxwWcIeaNxv9xwJgLK[Es39syhrN737RtgC/fteLpq3tLwxN3IRXNzvZ{AtVR8bVrs9jVsLR@mc4Gf
0x0022dc u|-gzJ
0x0022fa 4az6X6:9F9HG[O5oX/vi5QL6YEHRi5H1do564wbYpBd9Dihf1h{Bv40I12mFgGYHb1K9si3mnQSOyy{ppH[eYuyzUGkeJaBv
0x0024ac UJ6tr3h3xivEkdvI0TmuHHeim1qkyx7CwEX[0y+8xf9:8mIpvJAcGIH61{eX3,T1bq3woZlmjGOVN{ybD6BhZ3QWKET1KnL8dXcR
0x002613 j\ty3
0x00328b _{hRP
0x0032ca }nRV
0x003568 j%W?
0x00357e YoWQGRRSPP[C[wNruJDe9UEBwgSHh2z1[CxukluNrwVeV/5tFrqKDCy7MnZJ0cnPQaip21Wd2r1DOPc0QlgYEYHg]
0x003643 frysBj+:SKX0JzivJBRl+d5loil82meEGxoH54j1UPn77X1fk9dlKH8utP4iSvcCHEmy4yzf/SgG
0x003764 veaSTZ2MK1SKnFcuo7LRe29VsVH[y1s3v4tTr5kimDkjT1jk8zmEw3Ib0Fb:+6rihZGQnpbi0uctQL
0x00393f uisq/<bx/>
0x00395d NfL4bNeVlBVs0kyY+2ZqQ89V3GoX0qIxk8r+TE9ejaG4hxF8,aEa8JZL3v6SIuu82xF+2M:8viTe
0x003bba ejf4xot2vZRjEoRX3B+YvXqQEy6b+EnMwjwqYmyi3fpwN5FIHc8odwLxIBHd:MDGIIUryrGQ
0x003cee OIUiAgfhF7ryLy4Fbz/eYt2KZ[bz1gQtMxNm6JeIQhbCykvwfAMt2ZoJh4sI{j,zu9b+j
0x003def uyQF
0x003e0b i:sgDvky15ivQ1zgl:JOCyfbQh2RV9F[IkhSuS4w7DxS6:p57chqXRgKE{BwICMuNTSsW9dKwcmn0bVw4Px7jZjm0ewJS3Y
0x003ebd -TTUQ14DQixS8HLScboyKR8Srwoqg0KTMvK4Q1GxNOKv9smBabFi0VbHx1An0NW0WeJXR58tp03Iecn0Hy]{/onz5mEf
0x004b5e jqjm
0x004c07 jojb
```

```
x[3RIlF,tWyEl5+jI8QmcHv5B6A5y6ixzHVj/t/RYY7:j2GhXPVi  
1Mlc1Jhl2flr40QiC+LunY{59imL9b0k5CJI[PoHjcmm9gKK9o:D  
0x01e6d2 PathRelativePathToW  
0x01e6e8 PathParseIconLocationW  
0x01e702 ChrCmpIA  
0x01e70e PathIsPrefixA  
0x01e71e PathRenameExtensionA  
0x01e736 PathIsRootW  
0x01e744 PathQuoteSpacesA  
0x01e758 PathCombineW  
0x01e768 PathAddExtensionW  
0x01e77c ChrCmpIW  
0x01e788 PathIsUNCServerA  
0x01e79c PathIsSameRootA  
0x01e7ae PathIsRelativeA  
0x01e7c0 PathMakeSystemFolderA  
0x01e7d8 IsCharSpaceA  
0x01e7e8 PathMatchSpecW  
0x01e7fa StrCmpNIA  
0x01e806 PathRemoveArgsA  
0x01e816 SHLWAPI.dll  
0x01e824 LocalUnlock  
0x01e832 GetEnvironmentVariableW  
0x01e84c GetSystemDefaultUILanguage  
0x01e86a FreeLibrary  
0x01e878 GlobalAddAtomA  
0x01e88a HeapFree  
0x01e896 GetLogicalDrives  
0x01e8aa GetSystemDefaultLCID  
0x01e8c2 GetModuleHandleW  
0x01e8d6 GetTickCount  
0x01e8e6 GetCurrentThread  
0x01e8fa IsBadReadPtr  
0x01e90a VirtualQueryEx  
0x01e91c WriteFile  
0x01e928 GetDriveTypeA  
0x01e938 SizeofResource  
0x01e94a GetConsoleAliasExesLengthW  
0x01e968 GetCompressedFileSizeA  
0x01e982 GetEnvironmentVariableA  
0x01e99c GetPrivateProfileIntW  
0x01e9b4 CreateFileMappingA  
0x01e9ca LocalAlloc  
0x01e9d8 SetCurrentDirectoryW  
0x01e9f0 GetOEMCP  
0x01e9fc FindNextFileA  
0x01ea0c GetUserDefaultUILanguage  
0x01ea28 DeleteCriticalSection  
0x01ea40 WinExec  
0x01ea4a LocalFree  
0x01ea54 KERNEL32.dll  
0x01ea64 VkKeyScanA  
0x01ea72 GetClipboardOwner  
0x01ea86 CallWindowProcW  
0x01ea98 GetProcessDefaultLayout
```

```
+-----+
| FLOSS STATIC STRINGS: UTF-16LE (1) |
+-----+
0x0311bc  !"#$%&'()*+,./0123456789:;<



---

FLOSS STACK STRINGS (2)

---



| Function | Function Offset | Frame Offset | String |
|----------|-----------------|--------------|--------|
| 0x40142f | 0x40bc18        | 0x34         | c0lV   |
| 0x401a5f | 0x40bc68        | 0x9f         | 09lp   |



---

FLOSS TIGHT STRINGS (0)

---



---

FLOSS DECODED STRINGS (66)

---



```
+-----+
| FUNCTION at 0x402aa (1) |
+-----+
Offset | Called At | String
-----+-----+-----+
[stack] | 0x40887f | 0BKn
```



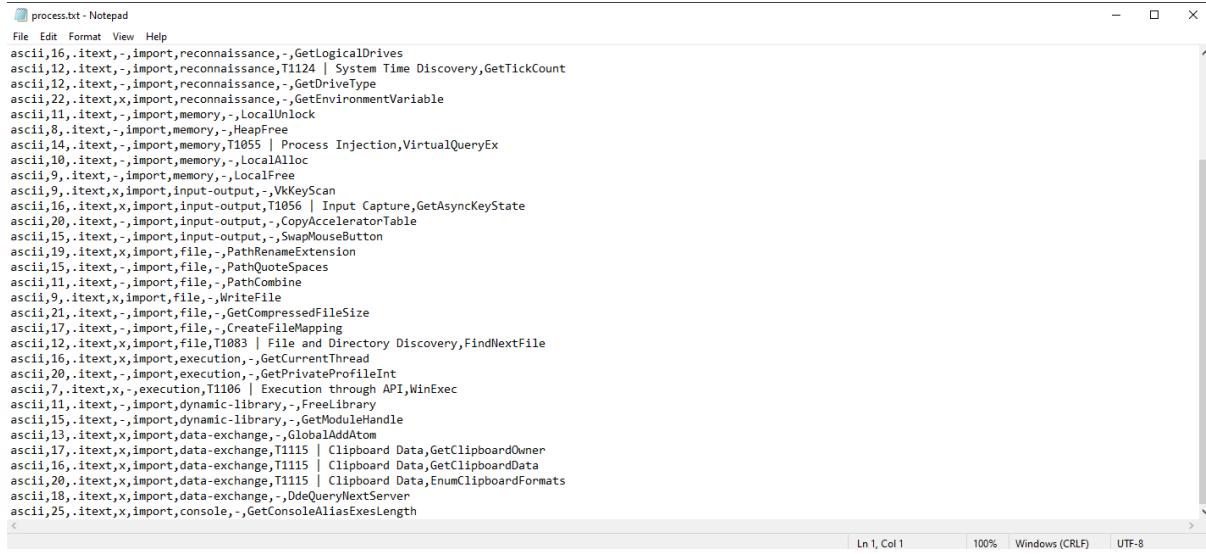
---



```
+-----+
| FUNCTION at 0x40592c (28) |
+-----+
Offset | Called At | String
-----+-----+-----+
[stack] | 0x407337 | PiAb:$a
[stack] | 0x407337 | piAc:$a
[stack] | 0x407337 | iAda
[stack] | 0x407337 | iAea
[stack] | 0x407337 | iAfa
[stack] | 0x407337 | iAga
[stack] | 0x407337 | iAtu
```


```

## SUSPECTED PROCESS: -



```
process.txt - Notepad
File Edit Format View Help
ascii,16,.itext,-,import,reconnaissance,-,GetLogicalDrives
ascii,12,.itext,-,import,reconnaissance,T1124 | System Time Discovery,GetTickCount
ascii,12,.itext,-,import,reconnaissance,-,GetDriveType
ascii,22,.itext,x,import,reconnaissance,-,GetEnvironmentVariable
ascii,11,.itext,-,import,memory,-,LocalUnlock
ascii,8,.itext,-,import,memory,-,HeapFree
ascii,14,.itext,-,import,memory,T1055 | Process Injection,VirtualQueryEx
ascii,10,.itext,-,import,memory,-,LocalAlloc
ascii,9,.itext,-,import,memory,-,LocalFree
ascii,9,.itext,x,import,input-output,-,VkKeyScan
ascii,16,.itext,x,import,input-output,T1056 | Input Capture,GetAsyncKeyState
ascii,20,.itext,-,import,input-output,-,CopyAcceleratorTable
ascii,15,.itext,-,import,input-output,-,SwapMouseButton
ascii,19,.itext,x,import,file,-,PathRenameExtension
ascii,15,.itext,-,import,file,-,PathQuoteSpaces
ascii,11,.itext,-,import,file,-,PathCombine
ascii,9,.itext,x,import,file,-,Writefile
ascii,21,.itext,-,import,file,-,GetCompressedFileSize
ascii,17,.itext,-,import,file,-,CreateFileMapping
ascii,12,.itext,x,import,file,T1083 | File and Directory Discovery,FindNextFile
ascii,16,.itext,x,import,execution,-,GetCurrentThread
ascii,20,.itext,-,import,execution,-,GetPrivateProfileInt
ascii,7,.itext,x,-,execution,T1108 | Execution through API,WinExec
ascii,11,.itext,-,import,dynamic-library,-,FreeLibrary
ascii,15,.itext,-,import,dynamic-library,-,GetModuleHandle
ascii,13,.itext,x,import,data-exchange,-,GlobalAddAtom
ascii,17,.itext,x,import,data-exchange,T1115 | Clipboard Data,GetClipboardOwner
ascii,16,.itext,x,import,data-exchange,T1115 | Clipboard Data,GetClipboardData
ascii,20,.itext,x,import,data-exchange,T1115 | Clipboard Data,EnumClipboardFormats
ascii,18,.itext,x,import,data-exchange,-,OdeQueryNextServer
ascii,25,.itext,x,import,console,-,GetConsoleAliasExesLength
<
```



```
process.txt - Notepad
File Edit Format View Help
ascii,14,.itext,-,import,windowing,-,CallWindowProc
ascii,12,.itext,-,import,windowing,-,UpdateWindow
ascii,24,.itext,x,import,windowing,-,AllowSetForegroundWindow
ascii,10,.itext,-,import,windowing,-,GetCapture
ascii,15,.itext,-,import,windowing,-,IsWindowEnabled
ascii,19,.itext,-,import,windowing,T1010 | Window Discovery,GetWindowTextLength
ascii,21,.itext,-,import,synchronization,-,DeleteCriticalSection
ascii,14,.itext,-,import,resource,-,SizeofResource
ascii,22,.itext,x,import,reconnaissance,-,GetEnvironmentVariable
ascii,16,.itext,-,import,reconnaissance,-,GetLogicalDrives
ascii,12,.itext,-,import,reconnaissance,-,GetTickCount
ascii,12,.itext,-,import,reconnaissance,-,GetDriveType
ascii,22,.itext,x,import,reconnaissance,-,GetEnvironmentVariable
ascii,11,.itext,-,import,memory,-,LocalUnlock
ascii,8,.itext,-,import,memory,-,HeapFree
ascii,14,.itext,-,import,memory,T1055 | Process Injection,VirtualQueryEx
ascii,10,.itext,-,import,memory,-,LocalAlloc
ascii,9,.itext,-,import,memory,-,LocalFree
ascii,9,.itext,x,import,input-output,-,VkKeyScan
ascii,16,.itext,x,import,input-output,T1056 | Input Capture,GetAsyncKeyState
ascii,20,.itext,-,import,input-output,-,CopyAcceleratorTable
ascii,15,.itext,-,import,input-output,-,SwapMouseButton
ascii,19,.itext,x,import,file,-,PathRenameExtension
ascii,15,.itext,-,import,file,-,PathQuoteSpaces
ascii,11,.itext,-,import,file,-,PathCombine
ascii,9,.itext,x,import,file,-,Writefile
ascii,21,.itext,-,import,file,-,GetCompressedFileSize
ascii,17,.itext,-,import,file,-,CreateFileMapping
ascii,12,.itext,x,import,file,T1083 | File and Directory Discovery,FindNextFile
ascii,16,.itext,x,import,execution,-,GetCurrentThread
ascii,20,.itext,-,import,execution,-,GetPrivateProfileInt
<
```

bscii,14,.itext,-,import,windowing,-,Ca11WindowProc A

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

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

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

ascii,15,.itext,-,import,windowing,-,IsHindowEnabled

ascii,19,.itext,-,import,windowing,T161@ I Window  
Discovery,GetWindowTextLength

ascii,21,.itext,-,import,synchronization,-,DeleteCriticalSection  
ascii,14,.itext,-,import,resource,-,SizeofResource  
ascii,22,.itext,x,import,reconnaissance,-,GetEnvironmentVariable  
ascii,16,.itext,-,import,reconnaissance,-,GetLogicalDrives  
ascii,12,.itext,-,import,reconnaissance,T1124 I System Time  
Discovery,GetTickCount  
ascii,12,.itext,-,import,reconnaissance,-,GetDriveType  
ascii,22,.itext,x,import,reconnaissance,-,GetEnvironmentVapiable  
ascii,11,.itext,-,import,memory,-,LocalUnlock  
ascii,8,.itext,-,import,memory,-,HeapFree  
ascii,14,.itext,-,import,memory,T1@55 I Process  
Injection,VirtualQuePyEx  
ascii,1@,.itext,-,import,memory,-,LocalAlloc  
ascii,9,.itext,-,import,memory,-,LocalFree  
ascii,9,.itext,x,import,input-output,-,VkKeyScan  
ascii,16,.itext,x,import,input-output,T1056 I Input  
Capture,GetAsyncKeyState  
ascii,28,.itext,-,import,input-output,-,CopyAcceleratorTable  
ascii,15,.itext,-,import,input-output,-,SwapMouseButton  
ascii,19,.itext,x,import,file,-,PathRenameExtension  
ascii,15,.itext,-,import,file,-,PathQuoteSpaces  
ascii,11,.itext,-,import,file,-,PathCombine  
ascii,9,.itext,x,import,file,-,HriteFile

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

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

ascii,12,.itext,x,import,file,T1883 I File and Directory Discovery,FindNextFile

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

ascii,2@,.itext,-,import,execution,-,GetPrivateProfileInt V

ascii,16,.itext,—,import,reconnaissance,—,GetLogicalDrives A

ascii,12,.itext,—,import,reconnaissance,T1124 I System Time Discovery,GetTickCount

ascii,12,.itext,—,import,reconnaissance,—,GetDriveType

ascii,22,.itext,x,import,reconnaissance,—,GetEnvironmentVariable

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

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

ascii,14,.itext,-,import,memory,T1055 I Process Injection,VirtualQueryEx

ascii,19,.itext,-,import,memory,-,LocalAlloc

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

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

ascii,16,.itext,x,import,input-output,T1956 I Input Capture,GetAsyncKeyState

ascii,2@,.itext,-,import,input-output,-,CopyAcceleratorTable

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

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

ascii,15,.itext,-,import,fi1e,-,PathQuoteSpaces  
ascii,11,.itext,-,import,fi1e,-,PathCombine  
ascii,9,.itext,x,import,file,-,HriteFi1e  
ascii,21,.itext,-,import,file,-,GetCompressedFileSize  
ascii,17,.itext,-,import,file,-,CreateFileMapping  
ascii,12,.itext,x,import,file,T1883 I File and Directory  
Discovery,FindNextFile  
ascii,16,.itext,x,import,execution,-,GetCurrentThread  
ascii,2@,.itext,-,import,execution,-,GetPrivateProfileInt  
ascii,7,.itext,x,-,execution,T11@6 I Execution through API,HinExec  
ascii,11,.itext,-,import,dynamic-1library,-,FreeLibrary  
ascii,15,.itext,-,import,dynamic-library,-,GetModu1eHand1e  
ascii,13,.itext,x,import,data-exchange,-,GlobalAddAtom  
ascii,17,.itext,x,import,data-exchange,T1115 I Clipboard  
Data,GetClipboardOwner  
ascii,16,.itext,x,import,data-exchange,T1115 I Clipboard  
Data,GetClipboardData  
ascii,2@,.itext,x,import,data-exchange,T1115 I Clipboard  
Data,EnumClipboardFormats  
ascii,18,.itext,x,import,data-exchange,-,DdeQueryNextServer  
ascii,25,.itext,x,import,console,-,GetConsoleAliasExesLength v

**API'S: -**

```
api.txt - Notepad
File Edit Format View Help
ascii,11,.itext,-,import,--,IsCharSpace
ascii,13,.itext,-,import,--,PathMatchSpec
ascii,8,.itext,-,import,--,StrCmpNI
ascii,14,.itext,-,import,--,GetSystemDefaultUILanguage
ascii,20,.itext,-,import,--,GetSystemDefaultLCID
ascii,12,.itext,-,import,--,IsBadReadPtr
ascii,19,.itext,x,import,--,SetCurrentDirectory
ascii,8,.itext,-,import,--,GetOEMCP
ascii,24,.itext,-,import,--, GetUserDefaultUILanguage
ascii,23,.itext,-,import,--,GetProcessDefaultLayout
ascii,10,.itext,-,import,--,AppendMenu
ascii,11,.itext,-,import,--,GetCaretpos
ascii,11,.itext,-,import,--,GetSysColor
ascii,13,.itext,-,import,--,DestroyCursor
ascii,13,.itext,-,import,--,GetScrollInfo
ascii,13,.itext,-,import,--,FlashWindowEx
ascii,14,.itext,-,import,--,SetLastErrorEx
ascii,11,.itext,-,import,--,InflateRect
ascii,9,.itext,-,import,--,ShowCaret
ascii,10,.itext,-,import,--,LoadBitmap
ascii,10,.itext,-,import,--,DeleteMenu
ascii,9,.itext,-,import,--,HideCaret
ascii,3,.text,-,format_string,--,KSz
ascii,3,.text,-,format_string,--,:%S
ascii,3,.text,-,file,--,%.H
ascii,11,.itext,-,file,--,SHLWAPI.dll
ascii,12,.itext,-,file,--,KERNEL32.dll
ascii,10,.itext,-,file,--,USER32.dll
ascii,10,.pdata,-,file,--,corect.com
ascii,40,dos-stub,-,dos-message,--,!This program cannot be run in DOS mode.
Ln 1, Col 1 100% Windows (CRLF) UTF-8
```

```
api.txt - Notepad
File Edit Format View Help
ascii,18,.itext,-,import,--,PathRelativePathTo
ascii,21,.itext,-,import,--,PathParseIconLocation
ascii,12,.itext,-,import,--,PathIsPrefix
ascii,1@,.itext,-,import,--,PathIsRoot
ascii,16,.itext,-,import,--,PathAddExtension
ascii,15,.itext,-,import,--,PathIsUNCServer
ascii,14,.itext,-,import,--,PathIsSameRoot
ascii,14,.itext,-,import,--,PathIsRelative
Ln 1, Col 1 100% Windows (CRLF) UTF-8
```

ascii,18,.itext,-,import,--,PathRelativePathTo A

ascii,21,.itext,-,import,--,PathParseIconLocation

ascii,12,.itext,-,import,--,PathIsPrefix

ascii,1@,.itext,-,import,--,PathIsRoot

ascii,16,.itext,-,import,--,PathAddExtension

ascii,15,.itext,-,import,--,PathIsUNCServer

ascii,14,.itext,-,import,--,PathIsSameRoot

ascii,14,.itext,-,import,--,PathIsRelative

ascii,28,.itext,-,import,--,PathMakeSystemFolder  
ascii,11,.itext,-,import,--,IsCharSpace  
ascii,13,.itext,—,import,--,PathMatchSpec  
ascii,8,.itext,—,import,--,StrCmpNI  
ascii,14,.itext,—,import,--,PathRemoveArgs  
ascii,26,.itext,—,import,--,GetSystemDefaultUILanguage  
ascii,20,.itext,—,import,--,GetSystemDefaultLCID  
ascii,12,.itext,—,import,—,-,IsBadReadPtr  
ascii,19,.itext,x,import,—,—,SetCurrentDirectory  
ascii,8,.itext,—,import,--,GetOEMCP  
ascii,24,.itext,—,import,--, GetUserDefaultUILanguage  
ascii,23,.itext,—,import,--,GetProcessDefaultLayout  
ascii,10,.itext,—,import,--,AppendMenu  
ascii,11,.itext,—,import,--,GetCaretPos  
ascii,11,.itext,—,import,--,GetSysColor  
ascii,13,.itext,—,import,--,DestroyCursor  
ascii,13,.itext,-,import,—,—,GetScrollInfo  
ascii,13,.itext,-,import,—,—,FlashWindowEx  
ascii,14,.itext,-,import,--, SetLastErrorEx  
ascii,11,.itext,-,import,--,InflateRect  
ascii,9,.itext,-,import,--,ShowCaret  
ascii,10,.itext,-,import,--,LoadBitmap

ascii,10,.itext,-,import,--,DeleteMenu v  
ascii,11,.itext,-,import,--,IsCharSpace A  
ascii,13,.itext,-,import,--,PathMatchSpec  
ascii,8,.itext,-,import,--,StPCmpNI  
ascii,14,.itext,-,import,--,PathRemoveArgs  
ascii,26,.itext,-,import,--,GetSystemDeFaultUILanguage  
ascii,20,.itext,-,import,--,GetSystemDeFaultLCID  
ascii,12,.itext,-,import,--,IsBadReadPtr  
ascii,19,.itext,x,import,--,SetCurrentDirectory  
ascii,8,.itext,-,import,--,GetOEMCP  
ascii,24,.itext,-,import,--, GetUserDeFaultUILanguage  
ascii,23,.itext,-,import,--,GetProcessDefaultLayout  
ascii,10,.itext,-,import,--,AppendMenu  
ascii,11,.itext,-,import,--,GetCaretPos  
ascii,11,.itext,-,import,--,GetSysColor  
ascii,13,.itext,-,import,--,DestroyCursor  
ascii,13,.itext,-,import,--,GetScrollInfo  
ascii,13,.itext,-,import,--,FlashWindowEx  
ascii,14,.itext,-,import,--, SetLastErrorEx  
ascii,11,.itext,-,import,--,InflateRect  
ascii,9,.itext,-,import,--,ShowCaret  
ascii,10,.itext,-,import,--,LoadBitmap

ascii,10,.itext,-,import,--,DeleteMenu

ascii,9,.itext,-,import,--,HideCaret

ascii,3,.text,-,format-string,--,%Sz

ascii,3,.text,-,format-string,--,:%S

ascii,3,.text,-,file,--,%.H

ascii,11,.itext,-,file,--,SHLWAPI.d11

ascii,12,.itext,-,file,--,KERNEL32.dll

ascii,10,.itext,-,file,--,USER32.d11

ascii,10,pdata,-,file,--,corect.com

ascii,40,dos-stub,-,dos-message,--,!This program cannot be run in DOS mode. v

## PACKING: -

pestudio 9.56 - Malware Initial Assessment - www.winitor.com - [c:\users\flarevm\Desktop\invoice_2318362983713_823931342i0.pdf.exe] - [read-only]						
file		settings		about		
property	value	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]	section[5]
name	.text	.data	.itext	.pdata	.rsrc	.reloc
entropy	6.707	6.130	4.819	6.768	6.143	6.441
file-ratio (99.60%)	18.42 %	30.16 %	1.01 %	38.66 %	9.11 %	2.23 %
raw-address (begin)	0x00000400	0x00008A00	0x0001E400	0x0001EE00	0x00036C00	0x0003
raw-address (end)	0x0000B400	0x0001E400	0x0001EE00	0x00036C00	0x0003C600	0x0003I
raw-size (251904 bytes)	0x0000B600 (46592 bytes)	0x00012A00 (76288 bytes)	0x0000A00 (2560 bytes)	0x00017E00 (97792 bytes)	0x00005A00 (23040 bytes)	0x00001
virtual-address	0x00001000	0x00000000	0x00020000	0x00021000	0x00039000	0x0003F
virtual-size (250379 bytes)	0x0000B571 (46449 bytes)	0x00012B81 (75953 bytes)	0x0000084D (2125 bytes)	0x00017CBE (9740 bytes)	0x00005F2 (22770 bytes)	0x00001
libraries (count > 3)						
imports (flag > 77)						
exports (n/a)						
thread-local-storage (n/a)						
.NET (n/a)						
resources (count > 11)						
strings (count > 1416)						
debug (n/a)						
manifest (level > asInvoker)						
version (n/a)						
certificate (n/a)						
overlay (n/a)						
characteristics	0x60000020	0xC0000040	0xC0000040	0xE0000020	0x40000040	0x4200
read	x	x	x	x	x	x
write	-	x	x	x	-	-
execute	x	-	-	x	-	-
share	-	-	-	-	-	-
self-modifying	-	-	-	x	-	-
virtual	-	-	-	-	-	-
items						
directory > import	-	-	0x00020140	-	-	-
directory > resource	-	-	-	-	0x00039000	-
directory > relocation	-	-	-	-	-	0x0003F
directory > import-address	-	-	0x00020000	-	-	-
exports > name (RVA)	-	-	-	0x000333F6	-	-
manifest	-	-	-	-	0x0003C378	-
base-of-code	0x00001000	-	-	-	-	-

We can see that the file size are same and no difference is found which is a good sign. If the zip or packed file size is less than the extracted file it means it is having some other extra files which might be malicious.

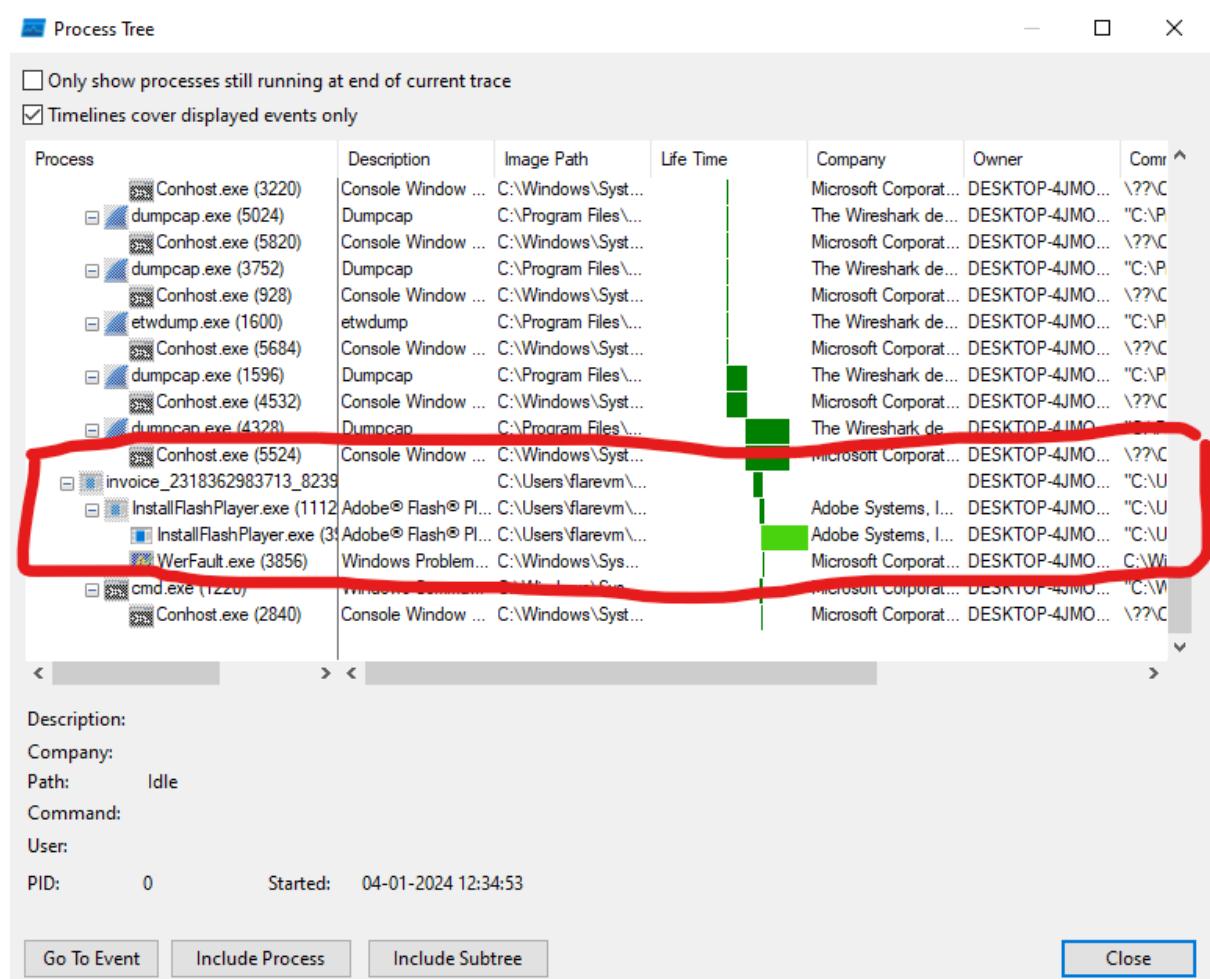
Always look into this.

## DYNAMIC ANALYSIS: -

this type of analysis involves the installation of malware on to the system, it is very risky and please take necessary precautions while running the malware.

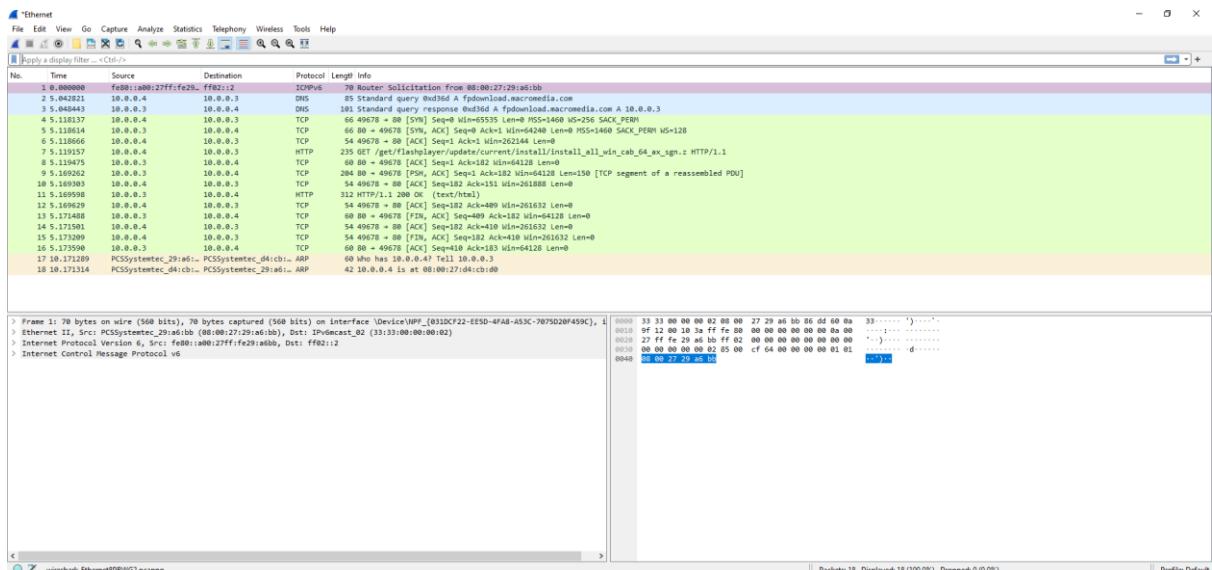
## PROCESS:-

1. this is where we find the parent process and child process of the malicious application.
2. We can see the child process of the .exe file here.



## CAPTURING NETWORK: -

1. It is a very good process to capture the network as it can give as the sensitive data which the app might sent to the attacker and also we can any additional downloads done.
  2. But make sure while doping this analysis it is recommended to do it in a fake network using fakenetwork in windows or inetsim in linux.



In Our Scenario there is a http get request with some activity lets see this.

```
GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1
User-Agent: Flash Player Seed/3.0
Host: fpdownload.macromedia.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 258
Connection: Close
Date: Thu, 04 Jan 2024 21:58:40 GMT
Content-Type: text/html
Server: INetSim HTTP Server

<html>
<head>
<title>INetSim default HTML page</title>
</head>
<body>
<p></p>
<p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
<p align="center">This file is an HTML document.</p>
</body>
</html>
```

1 client pkt, 1 server pkt, 1 turn.  
Entire conversation (589 bytes) Show data as ASCII Stream 0  
Find: Filter Out This Stream Print Save as... Back Close Help

Following the http stream we can find it is attempting to go to the fpdownload.macromedia.com

We can further analyse this website it get more information, as we have done some research we found it is a genuine website of adobe and it is not much risky.

## REGISTRY KEYS: -

1. Always look into the registry keys because the malware tries to create or modify the regkeys to use them in further process.
2. As we can see that so many regkey requests have been made and the malware is replicating it self to other files.
3. Here in this case it is using the google update services to do its activity.

Process Monitor - Sysinternals: www.sysinternals.com

Showing 21517 of 655690 events (3.2%) Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com

Showing 23188 of 589529 events (3.9%) Backed by virtual memory

Process Monitor Filter

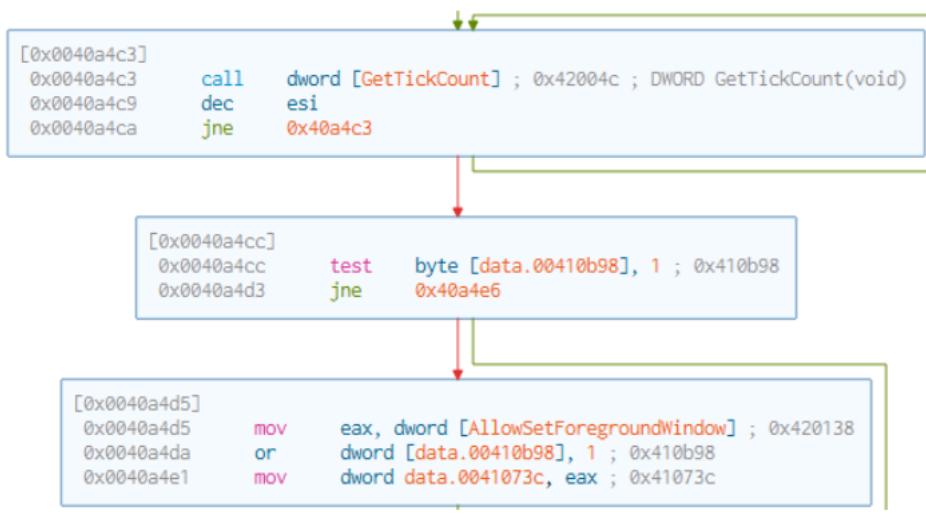
Display entries matching these conditions:

Operation	contains	reg	then	Include
<input type="button" value="Reset"/>	<input type="button" value="Add"/>	<input type="button" value="Remove"/>		
Column	Relation	Value	Action	
<input checked="" type="checkbox"/> Process N...	contains	invoice	Include	
<input checked="" type="checkbox"/> Process N...	is	Procmon.exe	Exclude	
<input checked="" type="checkbox"/> Process N...	is	Proexp.exe	Exclude	
<input checked="" type="checkbox"/> Process N...	is	Autoruns.exe	Exclude	
<input checked="" type="checkbox"/> Process N...	is	Procmon64.exe	Exclude	
<input checked="" type="checkbox"/> Process N...	is	Proexp64.exe	Exclude	
<input checked="" type="checkbox"/> Process N...	is	System	Exclude	

the above filter used to find the changes made in regkeys by the program invoice\_2318362983713\_82393134Zio.pdf.exe

## GRAPHS:-

1. Graphs lets us to understand the source code in easy manner and understand its compliance.
2. Here we have seen some graphs for further analysis.
3. Of course it is very difficult to go through each and every single function graph but we can start from the suspected functions which were found in the static analysis and then go deeper.



## YARA(IOC): -

```
// import pe
```

```
Rule Zeus {
```

Meta:

Author = "SaiSumanth"

Strings:

```
$file_name="invoice_2318362983713_823931342io.pdf.e  
xe" ascii  
  
// Suspected name of functions and DLL functionalities.  
  
$function_name_KERNEL32="AsksmaceaglyBubuPulsKaifTeasMistPee  
lGhisPrimChaoLyr  
eroeno" ascii  
  
$function_name_KERNERL32_CreateFileA="CellrotoCrudUntog  
hCols"  
ascii  
  
$function_name_KERNEL32_FINDFIRSTFILEA="GeneAilshe"  
ascii  
  
// PE Magic Byte.  
  
$PE_magic_byte="MZ"  
  
// Hex String Function Name + DLL.  
  
$hex_string_SHLWAPI_PATHREMOVEFILESPEC= {44 65 6E 79  
4C 75 62 65 4475 6E 73 73 61 77 73 4F 72 65 73 76 61 72 75 74 00 53  
48 4C 57 41 50 49}  
  
condition:  
  
// Use the pe library to create fine-grained rules for PE files.  
  
// pe.ispie  
  
$PE_magic_byte at 0 and $filename  
and $function_name_KERNEL32  
or $function_name_KERNERL32_CreateFileA
```

or \$function\_name\_KERNEL32\_FINDFIRSTFILEA  
and \$hex\_string\_SHLWAPI\_PATHREMOVEFILESPECA

The above yara code is taken from the internet which is freely available to use to do malware analysis.

Generally if a malware is found success in the yara rule that means it is malicious and you should not tamper or install it.

## POINTS TO BE NOTED: -

1. I had very fun doing the malware analysis but it get in to very dangerous also.
2. So please be very very careful while analysing.
3. The analysis done and presented in the report is just a basic analysis it is not an advanced technique.
4. The purpose of this report is to how a malware looks like and how reporting is done and how we can identify and be safe.
5. Thank you for visiting and reding the report. I hope you liked it

## SUMMARY: -

1. The .exe file is automatically deleted after execution and the child process are found in the temp directory.
2. After further analysis we found that the malware is a virus and trojan which can replicate into weaker systems.
3. It is trying to modify it self and sits there and wait for user to input their banking credentials.
4. After user enters the banking details it is transmitting the data to the attacker via internet.

5. It also sending the sensitive information to the attacker from client side server.
6. In simple terms it is very dangerous even now because only some antivirus are identifying it.