ANALYSIS REPORT

Malware Analysis Report

v1 NUMBER

2024-07-13 DATE

Analysis of Zeus Banking Trojan

Analyzed by : Chandra Kant Bauri

2024-07-13

Version 1.0

Table of Contents

Executive Summary

SHA256 hash	69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169

The Zeus banking trojan has cast a long shadow over the world of online banking security for over a decade. First appearing in 2007, this notorious malware has continuously evolved, employing ever-more sophisticated techniques to steal login credentials, account details, and hijack financial transactions. This report dissects a specific variant, ZeusBankingVersion_26Nov2013, highlighting its technical capabilities, potential impact, and essential mitigation strategies.

YARA signature rules are attached. Malware samples and hashes have been submitted to VirusTotal for further examination.

Technical Summary

Conducted a static and dynamic analysis on the After detonating it tried downloading adobe flash player and then deleted itself.

The invoice_2318362983713_823931342io.pdf.exe binary Drops two files after detonating, in “C:\Users\kant\AppData\Local\Temp” location.

- InstallFlashPlayer.exe
- msimg32.dll

“InstallFlashPlayer.exez” is not flagged by antivirus engines in virustotal.
“msimg32.dll” is flagged by many antivirus engines in virustotal.

Tools Used:

- Virustotal
- Floss
- Fake net
- capa
- PEStudio
- Cutter
- Wire shark
- Procmon
- yara
- hxd

Fingerprint

File: **invoice_2318362983713_823931342io.pdf.exe**

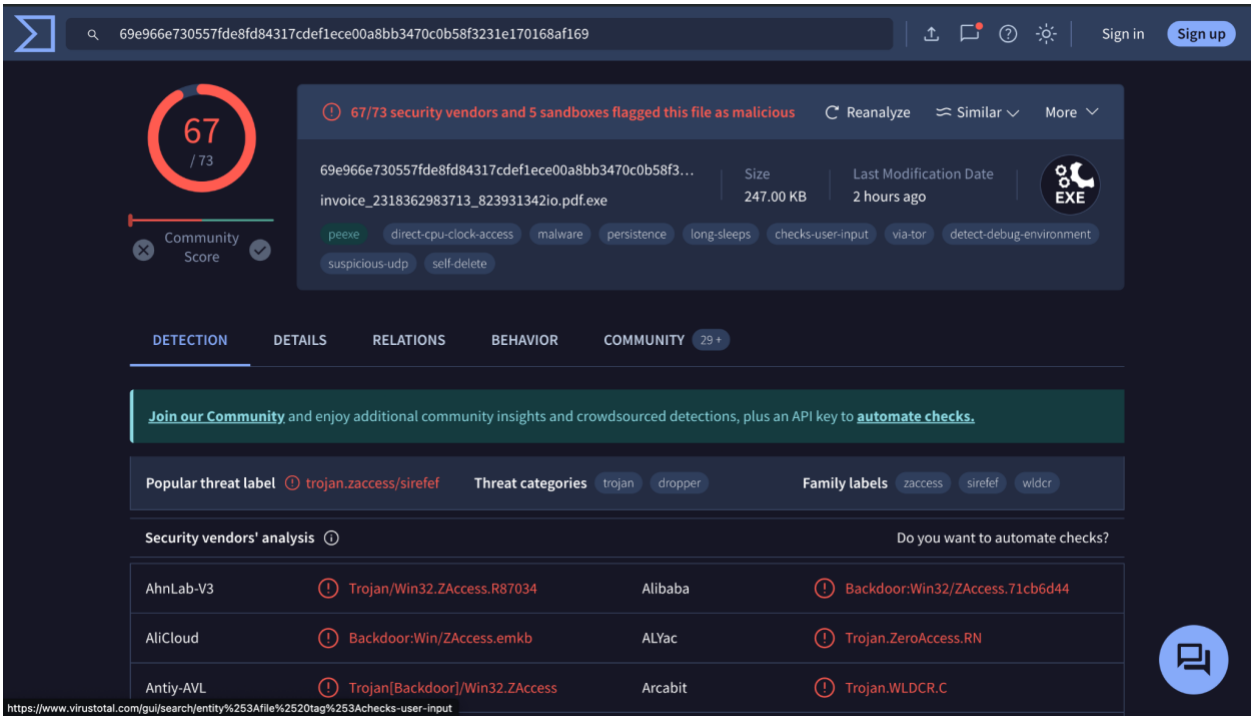

Fig 1 : invoice_2318362983713_823931342io.pdf.exe *Virus Total Results*

invoice_2318362983713_823931342io.pdf.exe consists of the following components:

- invoice_2318362983713_823931342io.pdf.exe
- InstallFlashPlayer.exe
- msimg32.dll

invoice_2318362983713_823931342io.pdf.exe

Data	Value
File Name:	invoice_2318362983713_823931342io.pdf.exe
Category:	Trojan
Language:	N/A
Architecture:	32-Bit
SHA256SUM:	69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
File Path:	C:/Users/kant/Desktop
File Size:	247 KB (252,928 bytes)
Internet Connection:	REQUIRED
Debugger Detection:	FALSE
Virtual Machine Detection:	FALSE
Description:	
invoice_2318362983713_823931342io.pdf.exe displays two different extensions at once, one after another.	

msimg32.dll

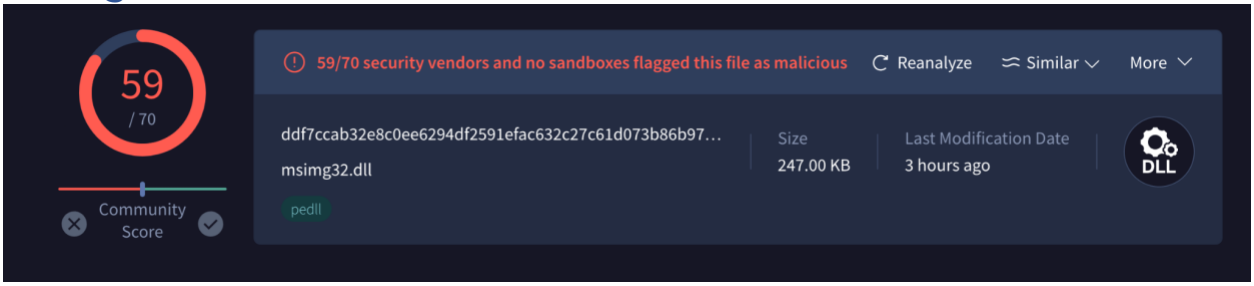

Fig 2 :msimg32.dll Virus Total Results

Data	Value
File Name:	msimg32.dll
Category:	Trojan
Language:	N/A
Architecture:	32-Bit
SHA256SUM:	DDF7CCAB32E8C0EE6294DF2591EFAC632C27C61D073B86B97DE62311F9379212
File Path:	C:/Users/kant/Desktop
File Size:	247 KB (252,928 bytes)
Internet Connection:	REQUIRED
Debugger Detection:	FALSE
Virtual Machine Detection:	FALSE
Description:	
Application extension (.dll)	

Pestudio Analysis

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
entropy	6.982
signature	n/a
tooling	Visual Studio 2008
file-type	executable
cpu	32-bit
subsystem	GUI

Fig 3 : invoice_2318362983713_823931342io.pdf.exe *Pestudio Results*

Basic Static Analysis

names	
file	c:\users\kant\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

Fig 4 : invoice_2318362983713_823931342io.pdf.exe *Pestudio Results found corect.com*

corect.com yielded no interesting results.

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)

Fig 5 : invoice_2318362983713_823931342io.pdf.exe *raw-address, virtual address*

Raw address size and virtual address size are close in size. Meaning most likely is not packed

API CALLS

- CallWindowProc
- UpdateWindow
- AllowSetForegroundWindow
- GetCapture
- IsWindowEnabled
- GetWindowTextLength
- DeleteCriticalSection
- SizeofResource
- GetEnvironmentVariable
- GetLogicalDrives
- GetTickCount
- GetDriveType
- GetEnvironmentVariable
- LocalUnlock
- HeapFree

- VirtualQueryEx
- LocalAlloc
- LocalFree
- VkKeyScan
- GetAsyncKeyState: GetAsyncKeyState is a function in the Windows API (specifically from the `windows.h` header) used to retrieve the state of a virtual key on the keyboard.
- CopyAcceleratorTable
- SwapMouseButton
- PathRenameExtension
- PathQuoteSpaces
- PathCombine
- WriteFile
- GetCompressedFileSize
- CreateFileMapping
- FindNextFile
- GetCurrentThread
- GetPrivateProfileInt
- WinExec
- FreeLibrary
- GetModuleHandle
- GlobalAddAtom
- GetClipboardOwner
- GetClipboardData
- EnumClipboardFormats
- DdeQueryNextServer
- GetConsoleAliasExesLength

—----------

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

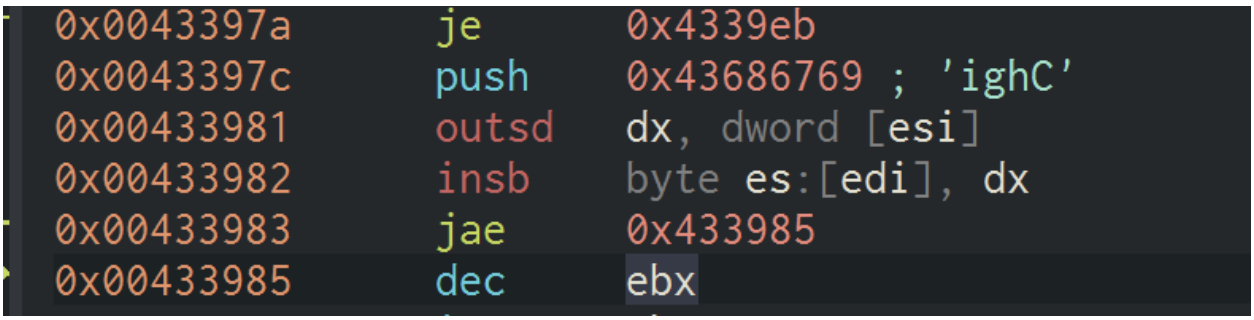

Fig 6 : invoice_2318362983713_823931342io.pdf.exe *Cutter disassembly*

- 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

```
PS C:\Users\kant\Desktop > capa .\invoice_2318362983713_823931342io.pdf.exe
```

md5	ea039a854d20d7734c5add48f1a51c34
sha1	9615dca4c0e46b8a39de5428af7db060399230b2
sha256	69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
analysis	static
os	windows
format	pe
arch	i386
path	C:/Users/kant/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

Fig 7 : invoice_2318362983713_823931342io.pdf.exe *capa output*

Advanced Static Analysis

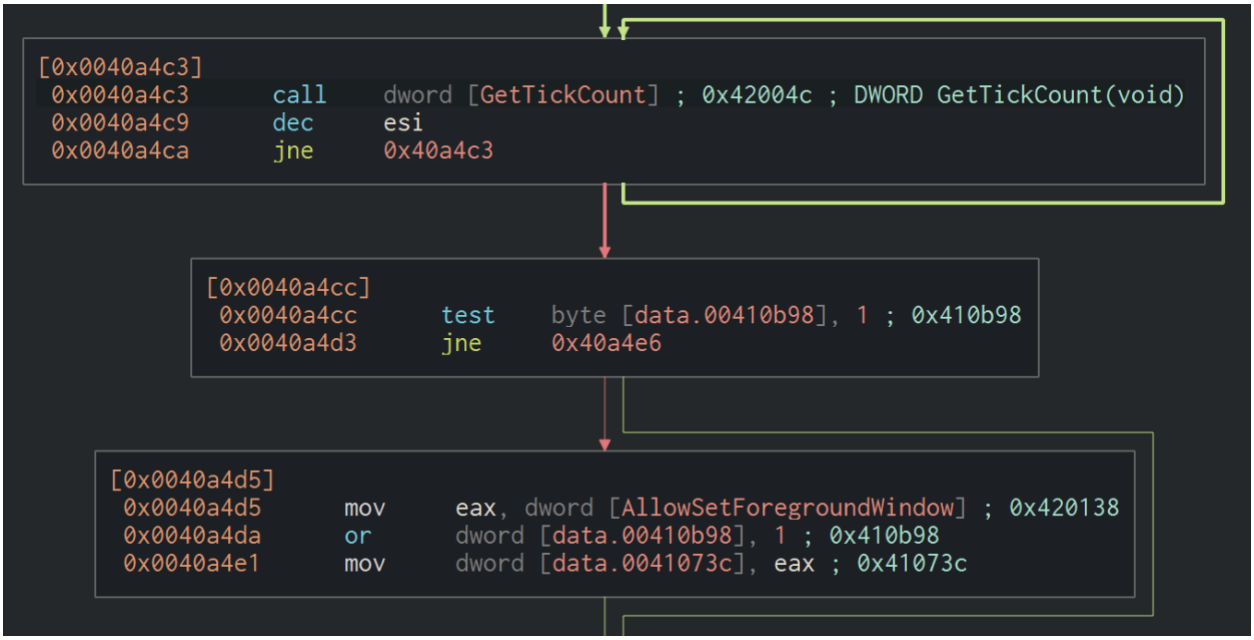

Fig 8 : invoice_2318362983713_823931342io.pdf.exe *cutter api calls disassembly*

Basic Dynamic Analysis

After detonating the binary tries to install an adobe flash player.

Procmon Analysis

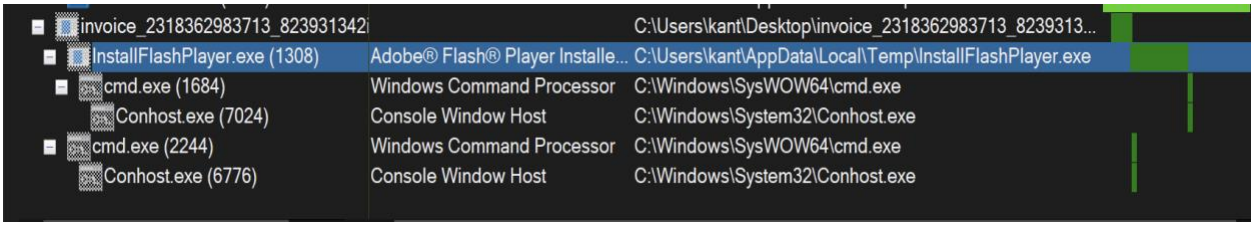

Fig 9 : invoice_2318362983713_823931342io.pdf.exe *Procmon*

Another sub process “conhost.exe” under the parent process invoice_2318362983713_823931342io.pdf.exe

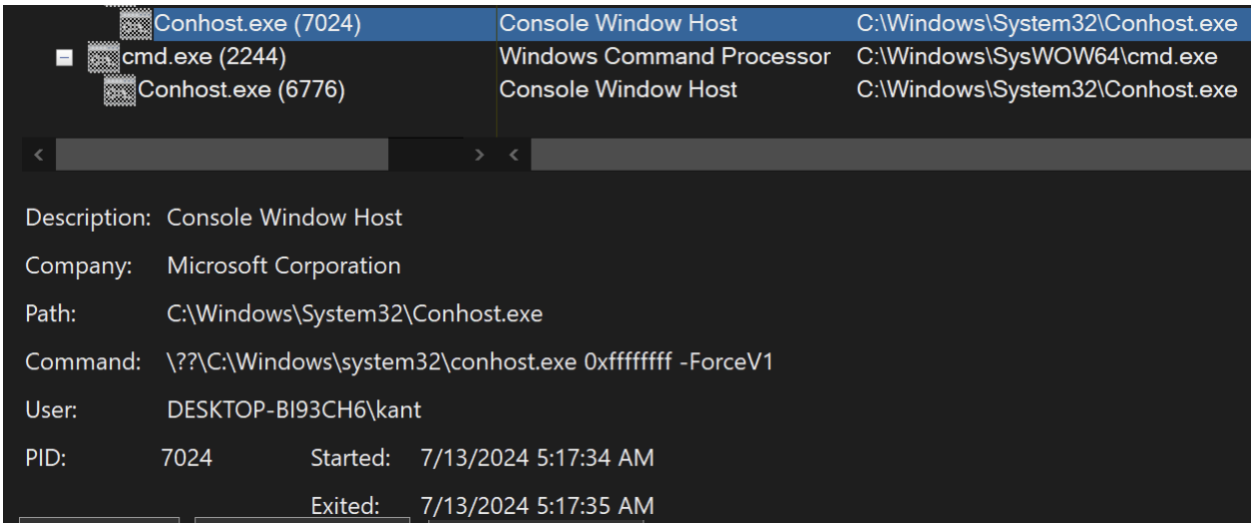

Fig 10 : invoice_2318362983713_823931342io.pdf.exe *Procmon sub processes*

The binary keeps persistence by using google updater.exe

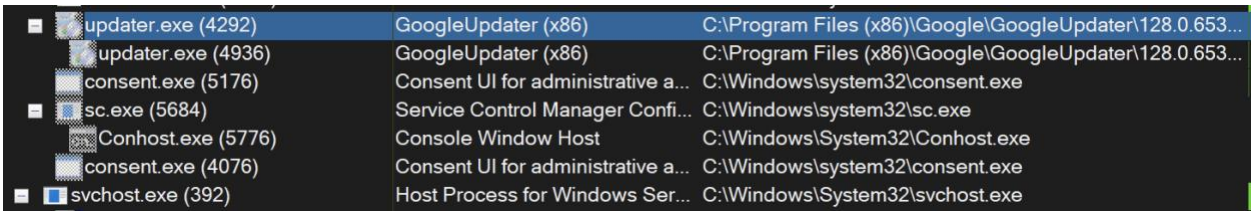

Fig 11 : invoice_2318362983713_823931342io.pdf.exe *persistence using google updater*

The binary tries to reach “fpdownload.macromedia.com”

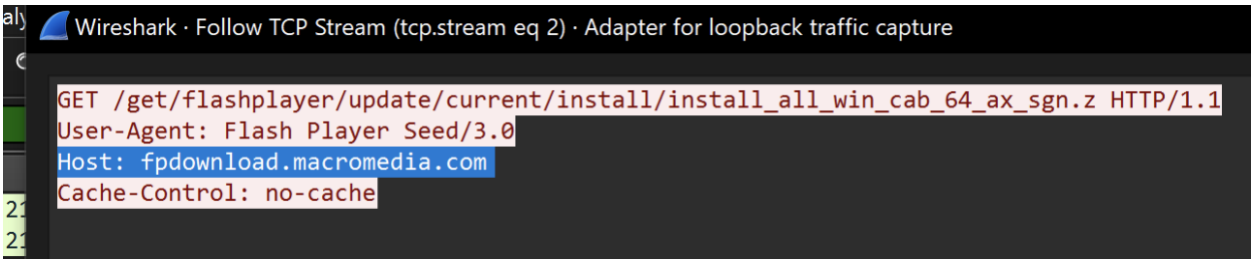

Fig 12 : wireshark fpdownload.macromedia.com

YARA (IOC)

yara rules:

```
rule Zeus {
      meta:

            author="Chandra Kant Bauri"
            description="A detection rule against 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 Strings Function name.

            $hex_string = {42 61 72 64 48 6F 6C 79 61 77 65}

      condition:

            $PE_magic_byte at 0 and $file_name
            and $function_name_KERNEL32_CreateFileA
            or $hex_string
}
```

```
Cmder

C:\Users\kant\Desktop
λ yara64.exe zeus.yara invoice_2318362983713_823931342io.pdf.exe -s -w -p 32
Zeus invoice_2318362983713_823931342io.pdf.exe
0x3176c:$function_name_KERNEL32_CreateFileA: CellrotoCrudUntohighCols
0x0:$PE_magic_byte: MZ
0x3162e:$hex_string: 42 61 72 64 48 6F 6C 79 61 77 65
```

Fig 13 : yara rules