Malware Analysis Report – Zeus Banking Trojan

**Author**: Mihir Sathvara

**Date**: 06 September 2025

# Executive Summary

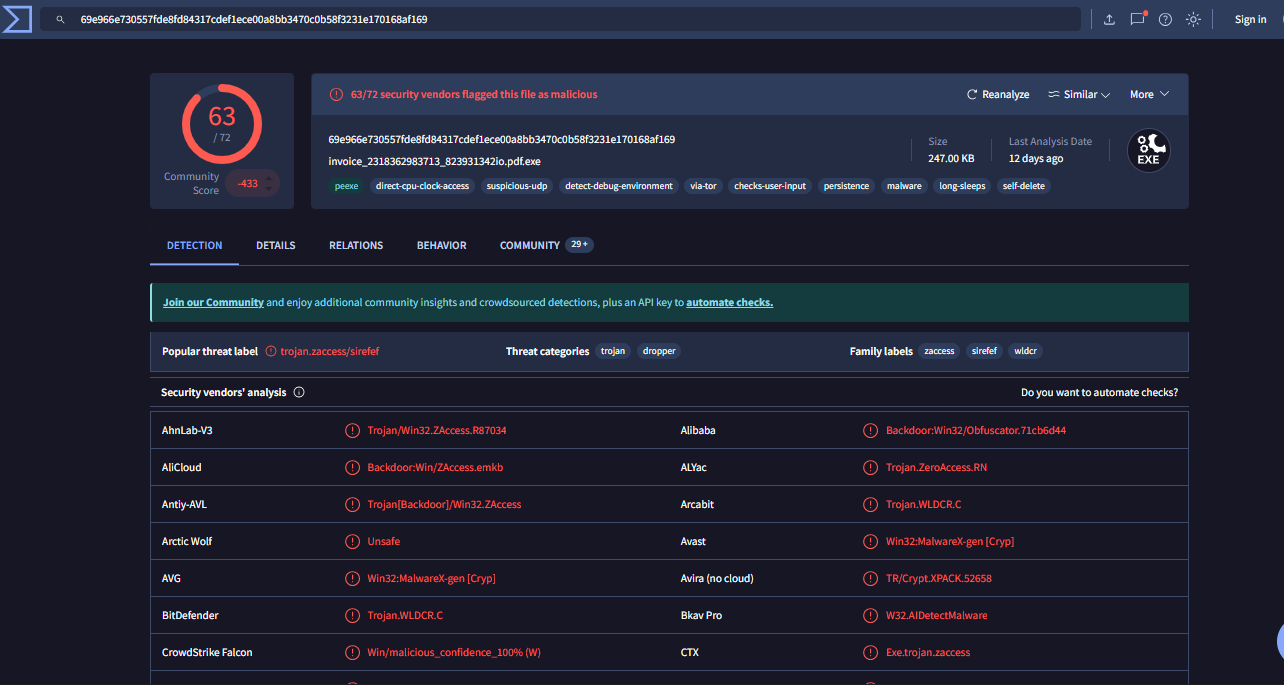
This report documents the analysis of a Zeus Banking Trojan sample. Zeus is a well-known banking Trojan used to steal sensitive financial information, primarily by capturing keystrokes, form-grabbing in browsers, and injecting malicious code into banking websites. The analyzed sample masqueraded as a PDF but was actually an executable file. Our analysis revealed its use of multiple Windows API calls related to keylogging, file manipulation, and persistence. This report outlines its static and dynamic characteristics, indicators of compromise, and a custom YARA rule for detection.

# Fingerprint

| **Attribute** | **Value** |
| --- | --- |
| **File Name** | invoice\_2318362983713\_823931342io.pdf.exe |
| **File Type** | Windows Executable (PE) |
| **MD5** | ea039a854d20d7734c5add48f1a51c34 |
| **SHA-1** | 9615dca4c0e46b8a39de5428af7db060399230b2 |
| **SHA-256** | 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169 |

**VirusTotal Output:**

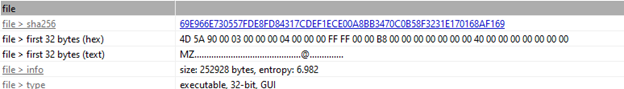
* 63/72 security vendors flagged this file as malicious.
* Detection names include: Trojan.Win32.ZAccess, Backdoor.Win32.Access, Win32:Malware-gen, Exe.trojan.zaccess, etc.
* See attached screenshot for full details.



# Static Analysis

The sample is a 32-bit Windows executable (PE format).

PE header and file info:



Suspicious API Calls (grouped):

**API Calls**

The malware leverages a wide range of Windows API calls, including but not limited to:

* AllowSetForegroundWindow, CallWindowProc, CreateFileMapping, DeleteCriticalSection, DestroyCursor, EnumClipboardFormats, FindNextFile, FlashWindowEx, FreeLibrary, GetAsyncKeyState, GetClipboardData, GetCurrentThread, GetEnvironmentVariable, HeapFree, IsBadReadPtr, LoadBitmap, LocalAlloc, PathAddExtension, PathCombine, PathMakeSystemFolder, PathMatchSpec, PathRemoveArgs, PathRenameExtension, VirtualQueryEx, VkKeyScan, WinExec, WriteFile, etc.

**Suspected Function Calls**

The following Windows API and function calls were observed or suspected during analysis. These are commonly leveraged by Zeus for persistence, data theft, and evasion:

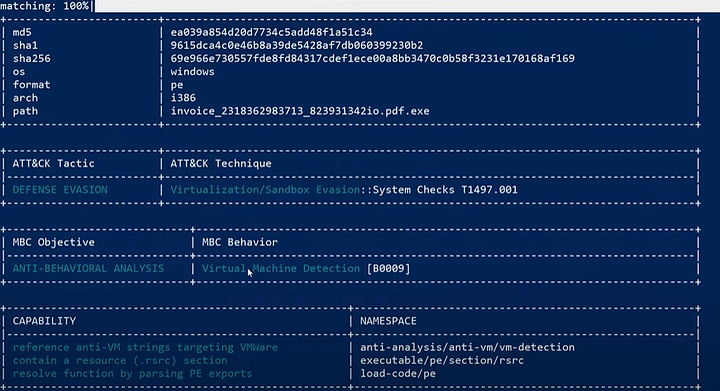
* KERNEL32.SetCurrentDirectory
* KERNEL32.VirtualQuery
* USER32.CreateCaret
* KERNEL32.CreateFile
* SHLWAPI.PathRemoveFileSpec
* USER32.DestroyIcon
* USER32.SetDlgItemText
* SHLWAPI.PathMakeSystemFolder
* KERNEL32.FindFirstFile
* KERNEL32.GetWindowsDirectory
* KERNEL32.DeleteFile
* KERNEL32.GlobalHandle
* KERNEL32.WriteFile
* KERNEL32.GetAsyncKeyState
* KERNEL32.LoadLibraryA
* KERNEL32.GetProcAddress
* KERNEL32.GetModuleHandleA
* KERNEL32.GetEnvironmentVariableA
* KERNEL32.LocalAlloc
* KERNEL32.FreeLibrary
* KERNEL32.WinExec
* USER32.FlashWindowEx
* USER32.CallWindowProc
* USER32.EnumClipboardFormats
* USER32.GetClipboardData
* USER32.SetForegroundWindow
* SHLWAPI.PathAddExtension
* SHLWAPI.PathCombine
* SHLWAPI.PathMatchSpec
* SHLWAPI.PathRemoveArgs
* SHLWAPI.PathRenameExtension
* SHLWAPI.PathMakeSystemFolder
* SHLWAPI.PathMatchSpec
* SHLWAPI.PathCombine

**Libraries Used**

* SHLWAPI.dll
* KERNEL32.dll
* USER32.dll

**CAPA Output**

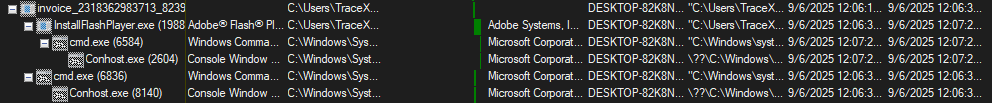
* The sample exhibits defense evasion, virtualization/sandbox evasion, and anti-behavioral analysis techniques.
* It checks for virtual machine environments and uses resources for anti-analysis.



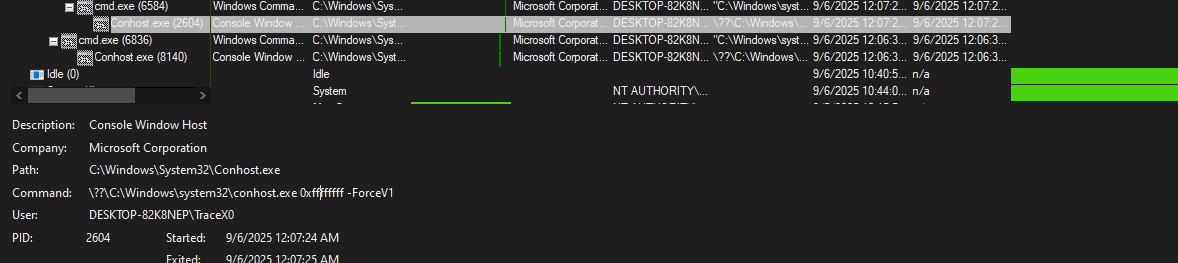
# Dynamic Analysis

# Process & Registry Activity

# The malware spawns child processes such as cmd.exe and conhost.exe for command execution.

****

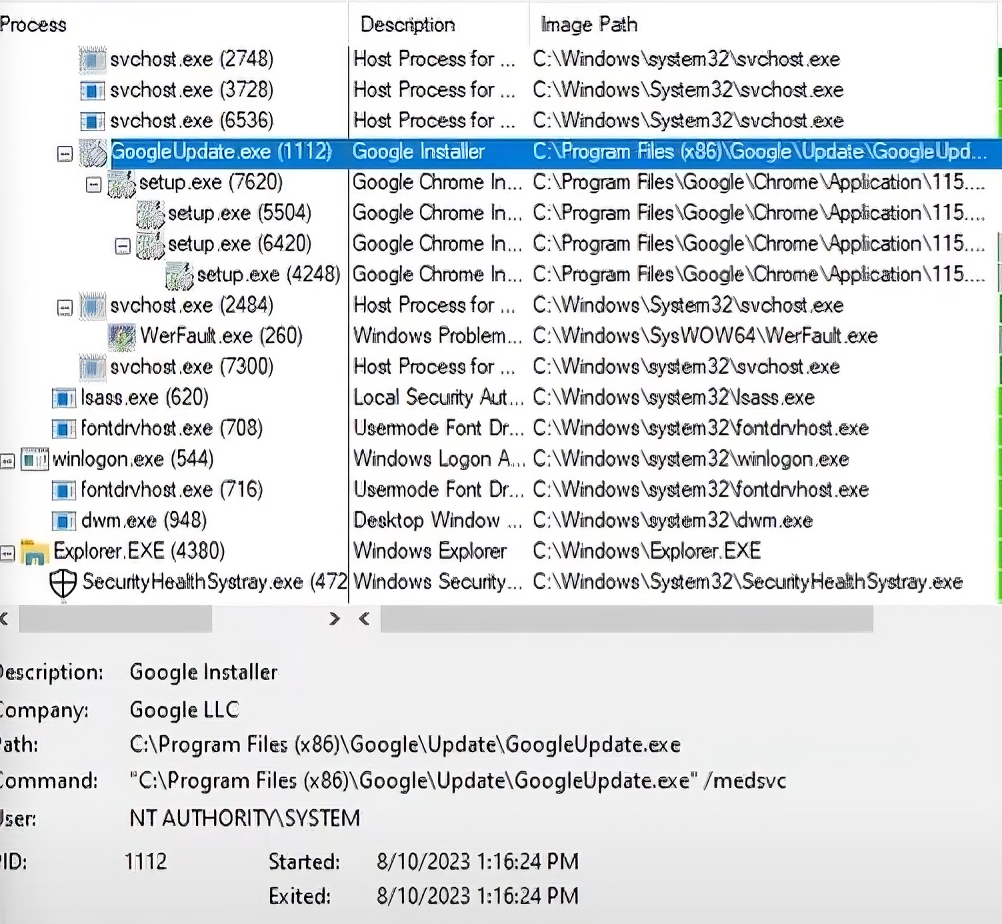
Some sort of commands run during execution, see attached image

****

Registry modifications are made for persistence, especially in startup keys.

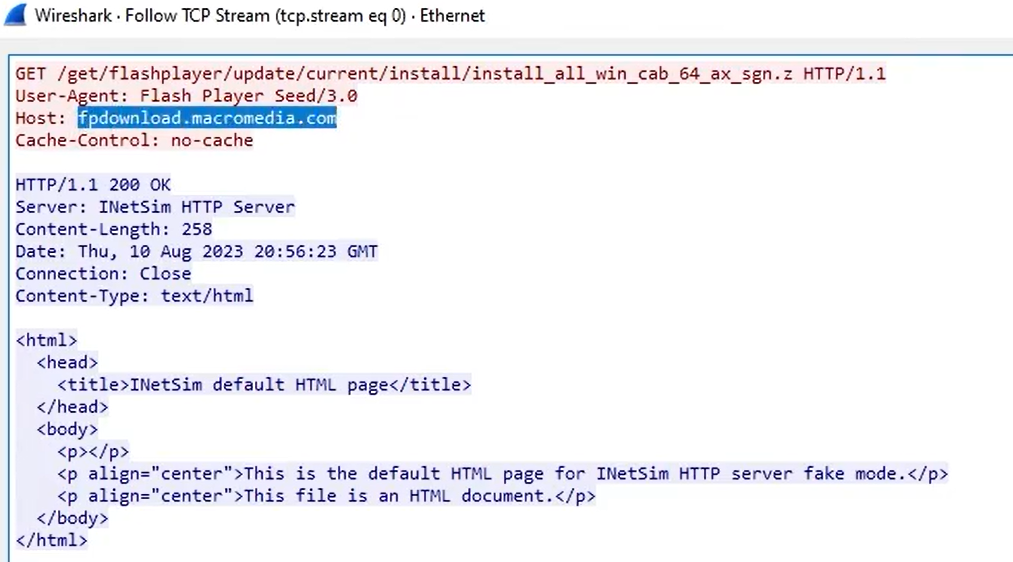
# Suspicious Activity

# A GoogleUpdate.exe process was observed, which may indicate masquerading or abuse of legitimate processes.



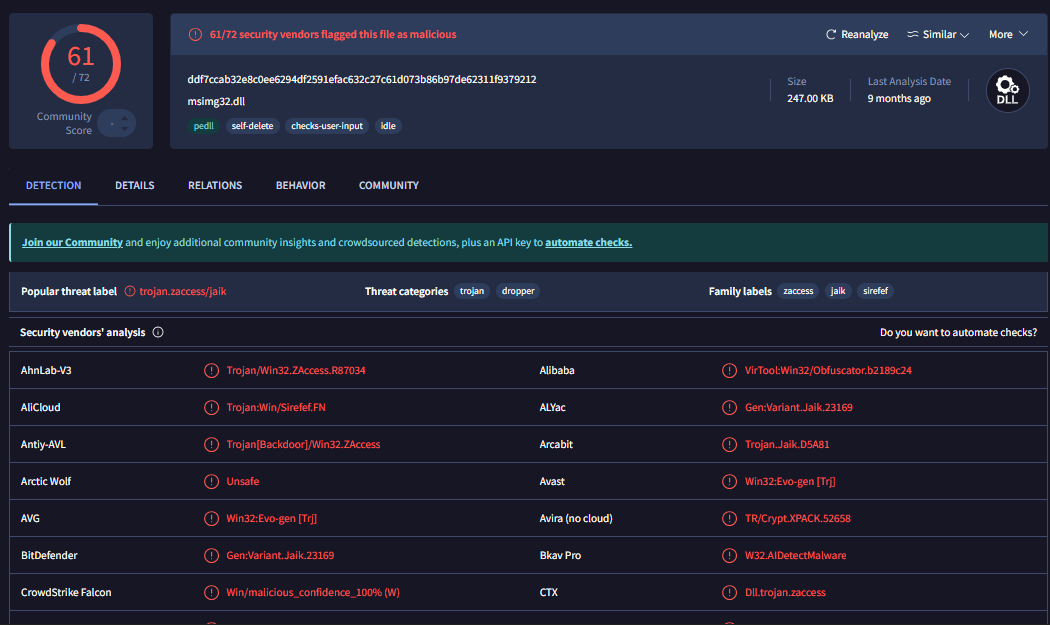
# Network Activity

# The malware attempts to download from fpdownload.macromedia.com using a fake Flash Player install request.



# Malicious DLL Discovery

# During execution, msimg32.dll was dropped and flagged as malicious by 61/72 security vendors.



# Indicators of Compromise (IOCs)

# File hashes:

# MD5: ea039a854d20d7734c5add48f1a51c34

# SHA-1: 9615dca4c0e46b8a39de5428af7db060399230b2

# SHA-256: 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169File name: invoice\_2318362983713\_823931342io.pdf.exe

# Dropped DLL: msimg32.dll

# C2 URL: fpdownload[.]macromedia[.]com

**Suspicious domain found in PEInfo (role unconfirmed)::** corect[.]com

# Registry keys for persistence:

# HKCU\Software\Microsoft\Windows\CurrentVersion\Run

# HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

# HKLM\Software\Microsoft\Windows\CurrentVersion\Run

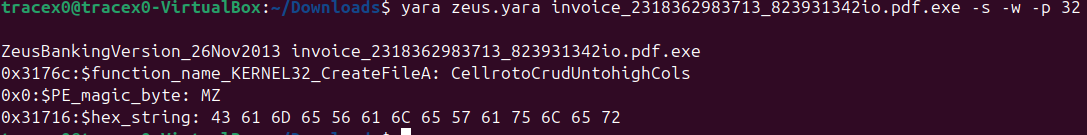
# HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

# HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

# YARA Rule

rule ZeusBankingVersion\_26Nov2013  
{  
 meta:  
 author = "Mihir Sathvara"  
 description = "A detection rule against ZeusBankingVersion\_26Nov2013"  
  
 strings:  
 $file\_name = "invoice\_2318362983713\_823931342io.pdf.exe" ascii  
 $function\_name\_KERNEL32\_CreateFileA = "CellrotoCrudUntohighCols" ascii  
 $PE\_magic\_byte = "MZ"  
 $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  
}

**Result:**



# Mitigation & Recommendations

- Deploy the above YARA rule for early detection of this malware family.  
- Monitor API calls associated with keylogging (e.g., GetAsyncKeyState, SetWindowsHookEx).  
- Restrict execution of suspicious files from email attachments and enforce strict attachment filtering.  
- Ensure EDR/AV solutions are updated to detect Zeus variants.  
- Educate users against opening suspicious email attachments disguised as invoices.

# References

- https://attack.mitre.org/ (for mapping tactics & techniques)  
- https://virustotal.com/