Malware Analysis Report – Zeus Banking Trojan

**Author**: Mihir Sathvara

**Date**: 06 September 2025

**Version:** 1.0

# 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 by capturing keystrokes, performing form-grabbing in browsers, and injecting malicious code into banking websites.

# The analyzed sample masqueraded as a PDF but was actually an executable file. Analysis revealed its use of multiple Windows API calls for keylogging, file manipulation, and persistence. It also dropped a malicious DLL, attempted network communication with a known C2, and modified registry keys for startup persistence.

# Impact: Successful infection may result in credential theft, unauthorized access to banking applications, and long-term persistence inside corporate environments.

**Table of Contents**

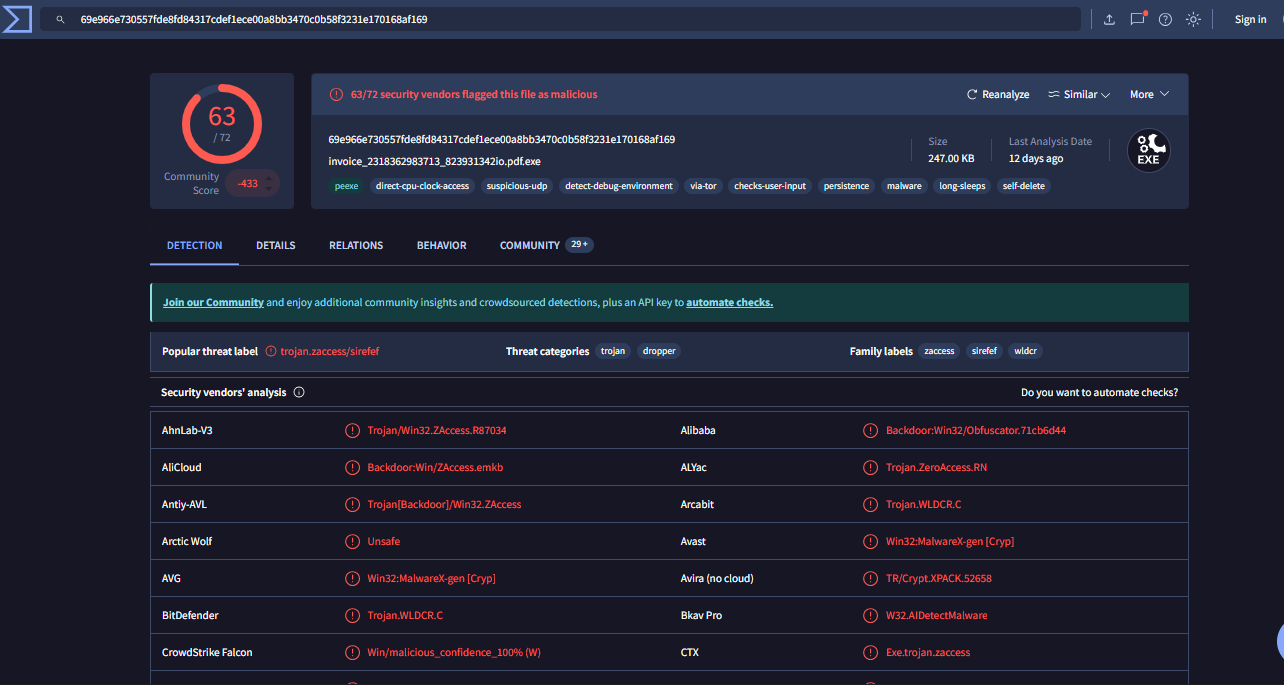
1. Executive Summary
2. Fingerprint / Sample Information
3. Static Analysis
   * Suspicious API Calls
   * Suspected Function Calls
   * Libraries Used
   * CAPA Output
4. Dynamic Analysis
   * Process & Registry Activity
   * Suspicious Activity
   * Network Behavior
   * Dropped Files
5. Indicators of Compromise (IOCs)
6. YARA Rule
7. MITRE ATT&CK Mapping
8. Mitigation & Recommendations
9. References

# 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:**

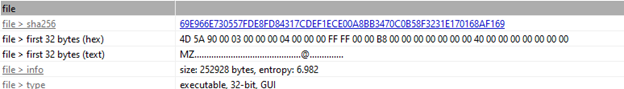
* 63/72 security vendors flagged this file as malicious.
* Detection names include: Trojan.Win32.ZAccess, Backdoor.Win32.Access, Win32:Malware-gen, Exe.trojan.zaccess, etc.
* See attached screenshot for full details.



# 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:

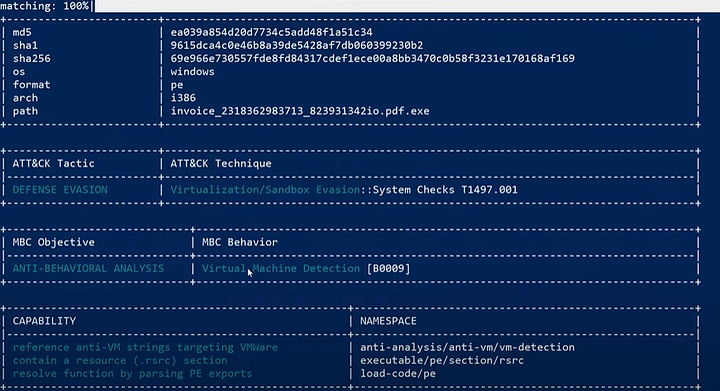
* KERNEL32.SetCurrentDirectory
* KERNEL32.VirtualQuery
* USER32.CreateCaret
* KERNEL32.CreateFile
* SHLWAPI.PathRemoveFileSpec
* USER32.DestroyIcon
* USER32.SetDlgItemText
* SHLWAPI.PathMakeSystemFolder
* KERNEL32.FindFirstFile
* KERNEL32.GetWindowsDirectory
* KERNEL32.DeleteFile
* KERNEL32.GlobalHandle
* 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**

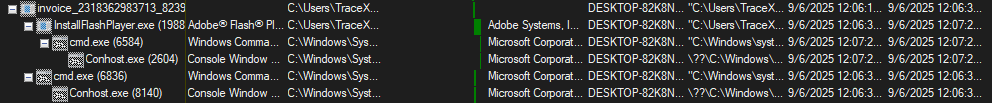
* The sample exhibits defense evasion, virtualization/sandbox evasion, and anti-behavioral analysis techniques.
* It checks for virtual machine environments and uses resources for anti-analysis.



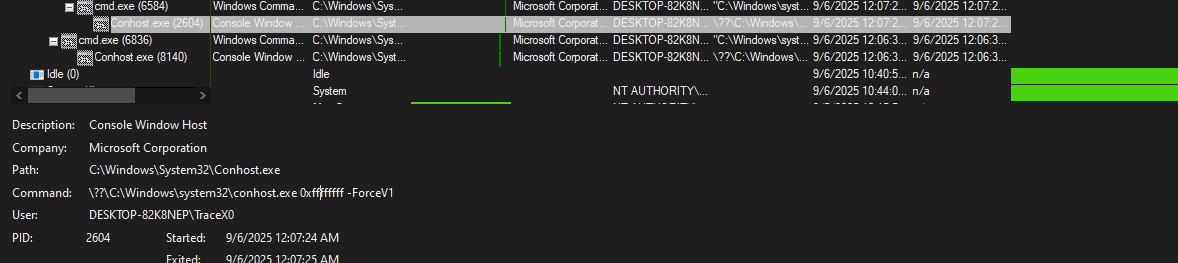
# Dynamic Analysis

# Process & Registry Activity

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

****

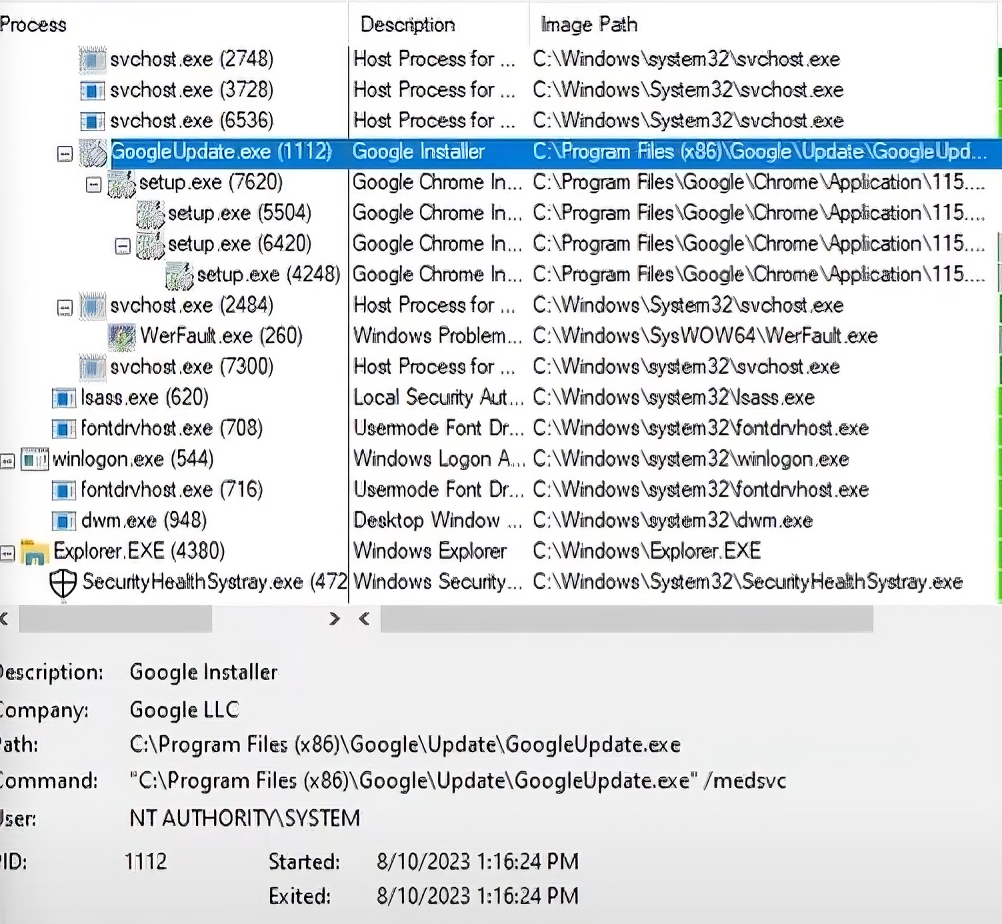
Some sort of commands run during execution, see attached image

****

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

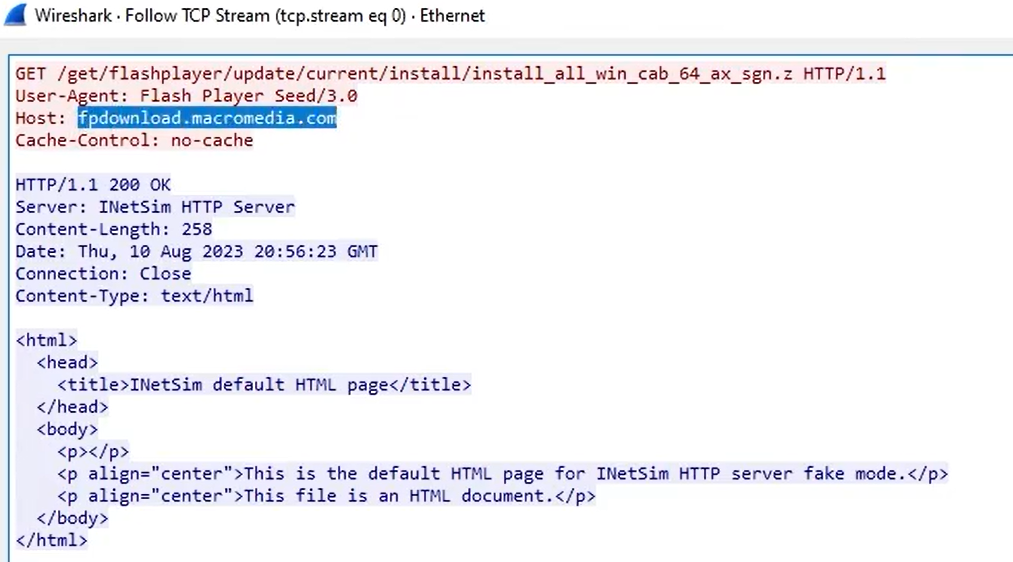
# Suspicious Activity

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



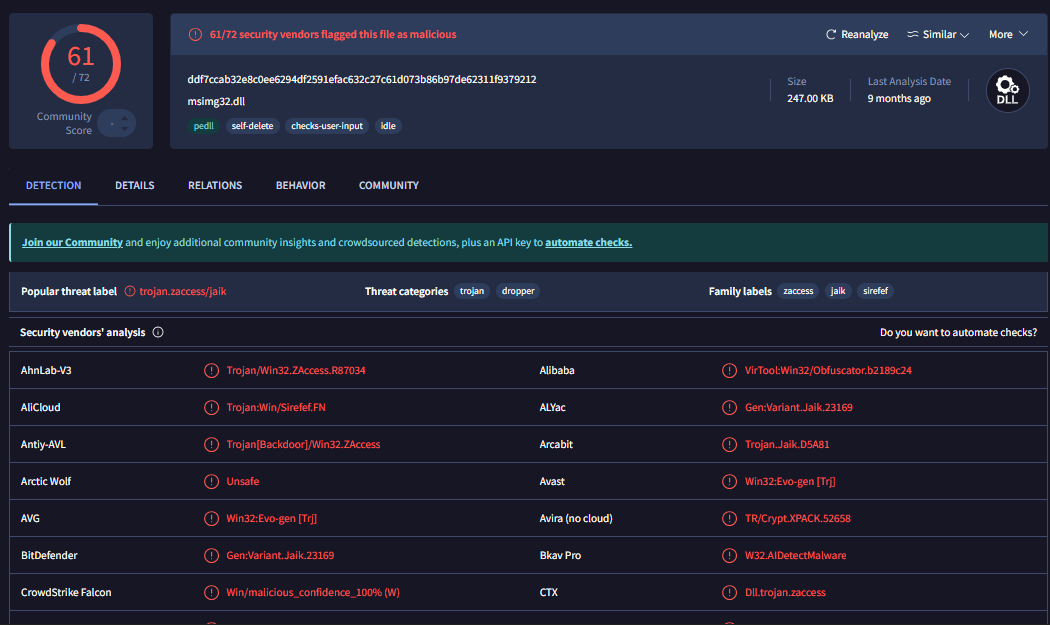
# Network Activity

# 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

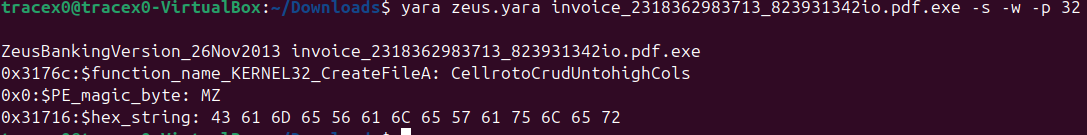
# HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

# 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:**



**MITRE ATT&CK Mapping**

This sample exhibits behaviors aligning with multiple MITRE ATT&CK tactics and techniques. The following table summarizes observed mappings.

| **Tactic (ATT&CK)** | **Technique ID** | **Technique Name** | **Evidence from Analysis** |
| --- | --- | --- | --- |
| **Persistence** | T1547.001 | Registry Run Keys / Startup Folder | Modifies HKCU\Software\Microsoft\Windows\CurrentVersion\Run |
| **Credential Access** | T1056.001 | Keylogging | Uses API GetAsyncKeyState for keylogging |
| **Defense Evasion** | T1497 | Virtualization/Sandbox Evasion | CAPA output showed VM/analysis evasion |
| **Execution** | T1204.002 | User Execution: Malicious File | Masqueraded as invoice.pdf.exe |
| **Command & Control (C2)** | T1071.001 | Application Layer Protocol: Web Traffic | Connects to fpdownload.macromedia[.]com |
| **Persistence / Defense Evasion** | T1036.005 | Masquerading: Match Legitimate Name | Spawned GoogleUpdate.exe as disguise |
| **Discovery** | T1082 | System Information Discovery | Uses Windows API calls to query environment variables |
| **Impact** | T1539 | Steal Web Session Cookie / Banking Injection | Zeus family known for form grabbing & injection (implied) |

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/