

Practical Malware Analysis & Triage

Malware Analysis Report

Droppper.DownloadFromURL Malware

FEB 2025 | Athiwat Tiprasaharn | Jitlada-Naomi Cybersecurity Inc. | v1.0

Table of Contents

[Executive Summary 3](#_Toc189939427)

[High-Level Technical Summary 4](#_Toc189939428)

[Malware Compositions 5](#_Toc189939429)

[Basic Static Analysis 6](#_Toc189939430)

[Basic Dynamic Analysis 8](#_Toc189939431)

[Advanced Static Analysis 11](#_Toc189939432)

[Advanced Dynamic Analysis 14](#_Toc189939433)

[Indicators of Compromise 16](#_Toc189939434)

[Network-based Indicators 16](#_Toc189939435)

[Host-based Indicators 16](#_Toc189939436)

[Rules and Signature 18](#_Toc189939437)

[Appendices 19](#_Toc189939438)

[A. YARA Rule 19](#_Toc189939439)

[B. Callback URL 19](#_Toc189939440)

# Executive Summary

|  |  |
| --- | --- |
| SHA 256 | 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a |

Droppper.DownloadFromURL is a dropper malware which first identified in Oct 8th, 2021. It is an executable file runs on the x86-Arch Windows system.

Network analysis revealed outbound connections to a remote URL. System artifacts include intermittent black screen pop-ups and a newly created executable ('CR433101.dat.exe') located in 'C:\Users\Public\Documents'.

Attached are the Yara rules developed for identifying this malware. The sample and its corresponding hash have been submitted to VirusTotal for community analysis.

# High-Level Technical Summary

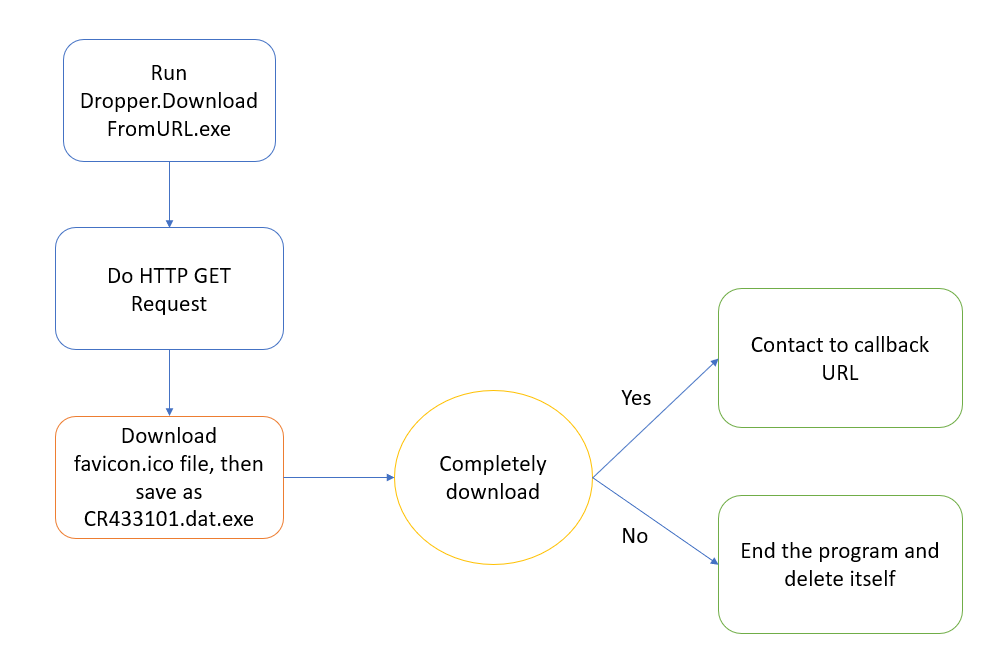


Figure Malware process summary chart

“Droppper.DownloadFromURL.exe” has two stages; First, download the malware component (“favicon.ico” but saved as “CR433101.dat.exe”) from “ssl-6582datamanager.helpdeskbros.local”. Second, if malware component had been downloaded completely, it contacted to callback URL “http://huskyhacks.dev”.

# Malware Compositions

|  |  |
| --- | --- |
| File name | SHA256 |
| Droppper.DownloadFromURL.exe | 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a |
| CR433101.dat.exe | c090fad79bc646b4c8573cb3b49228b96c5b7c93a50f0e3b2be9839ed8b2dd8b |

After finishing to run “Droppper.DownloadFromURL.exe” malware, it continued to make HTTP GET Request to download the initial file “favicon.ico”, however, the file was saved as “CR433101.dat.exe”

If it had succeeded to download and save the file, the malware stepped to contact with callback URL (which is in Appendices B). If it had failed, the malware ended its operation and deleted itself.

# Basic Static Analysis

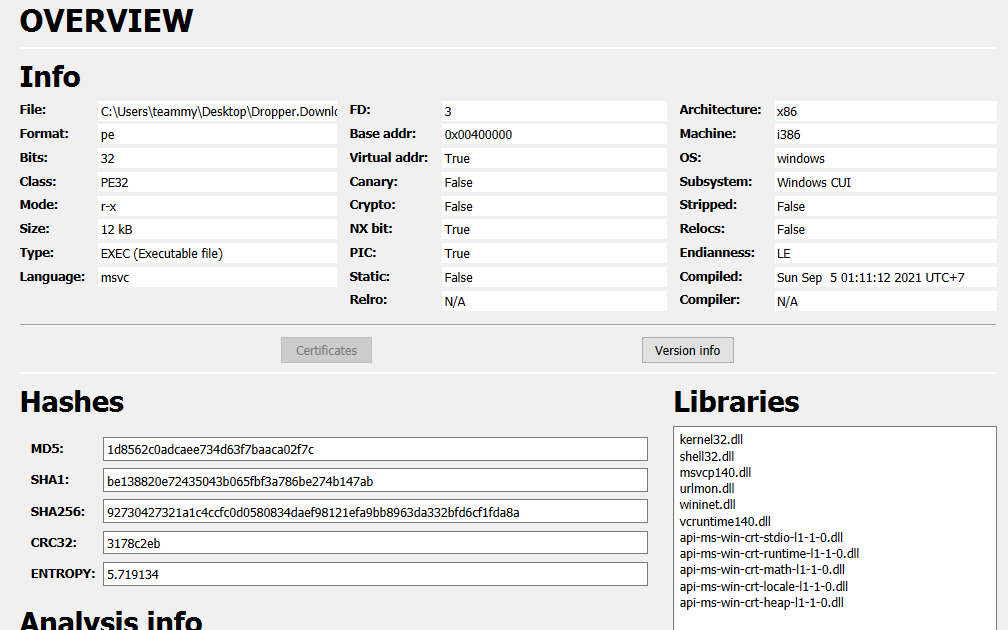


Figure File Hash from Cutter

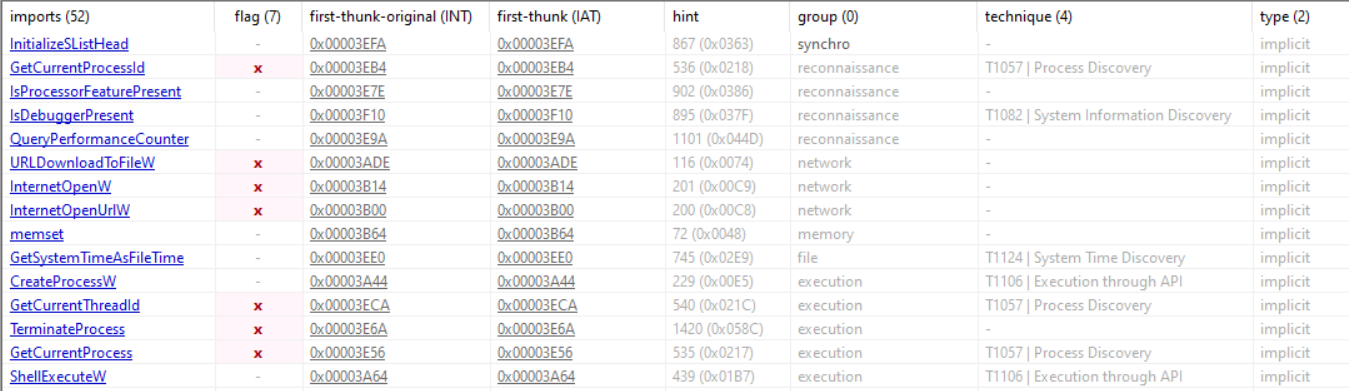


Figure Imports from PEStudio

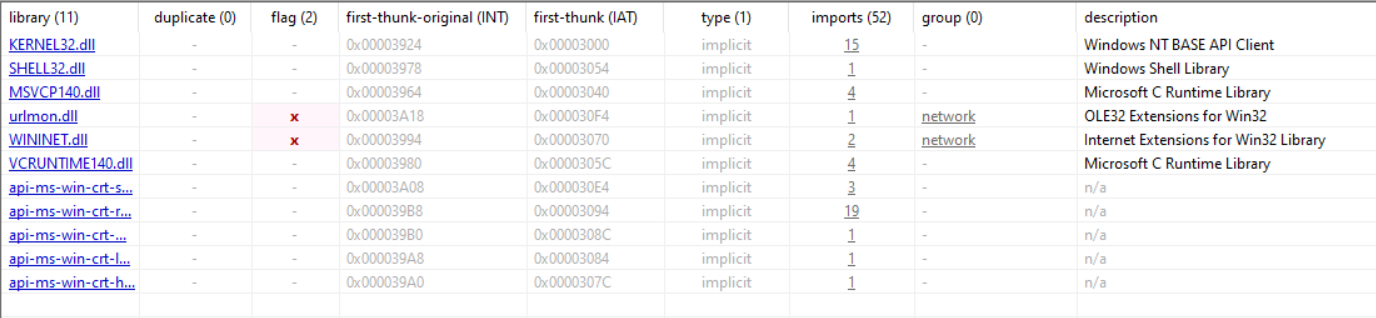


Figure Libraries from PEStudio

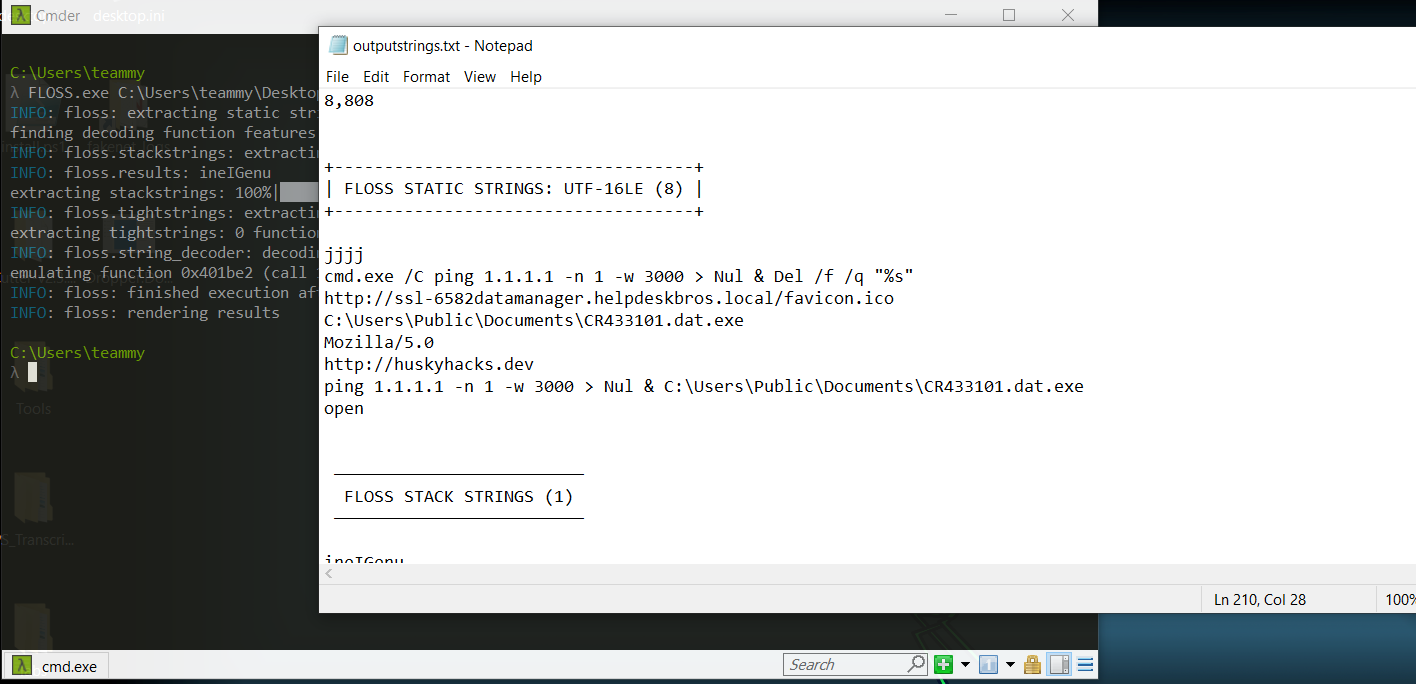


Figure Strings from Floss

# Basic Dynamic Analysis

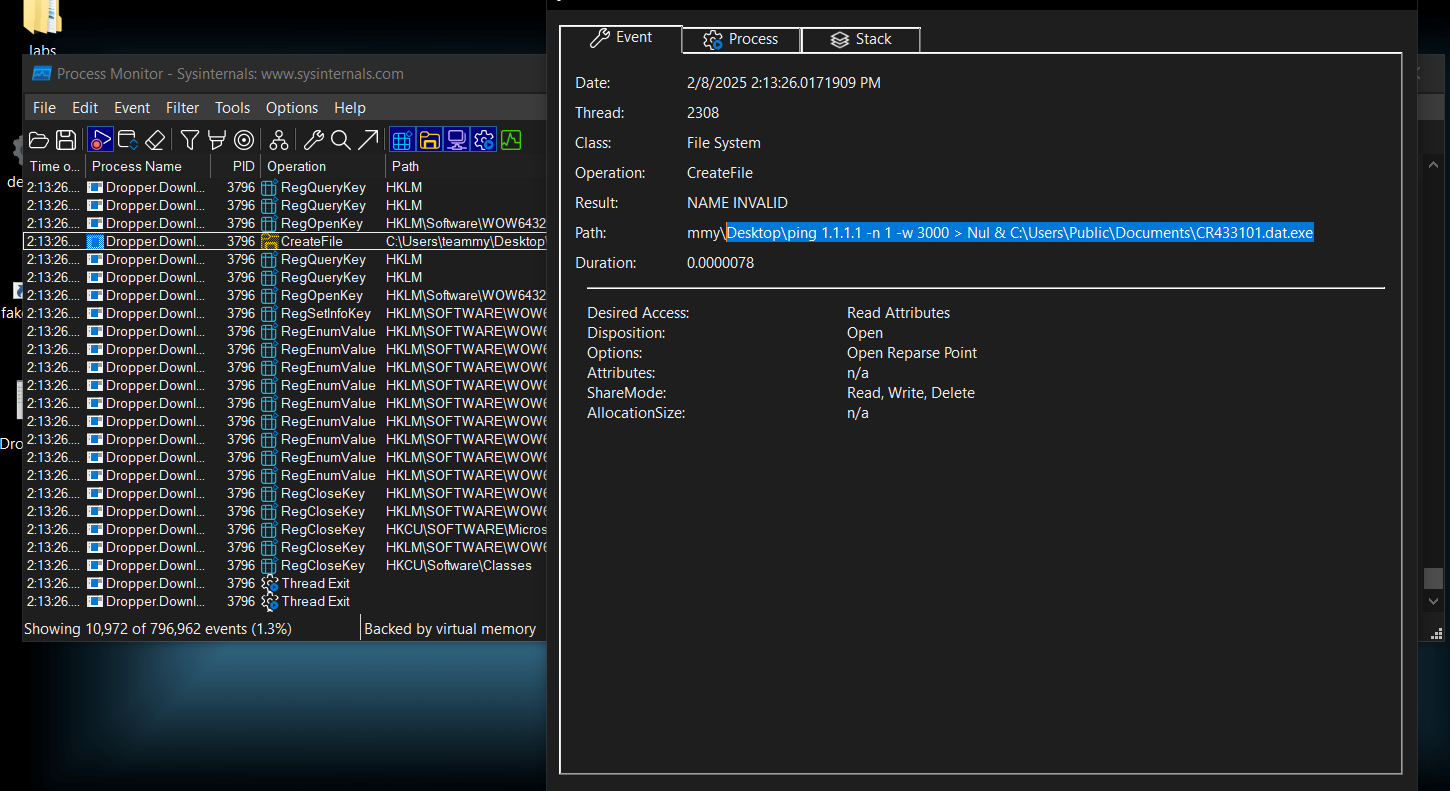


Figure Found a command to save a file on C:\Users\Public\Documents\ via Procmoc

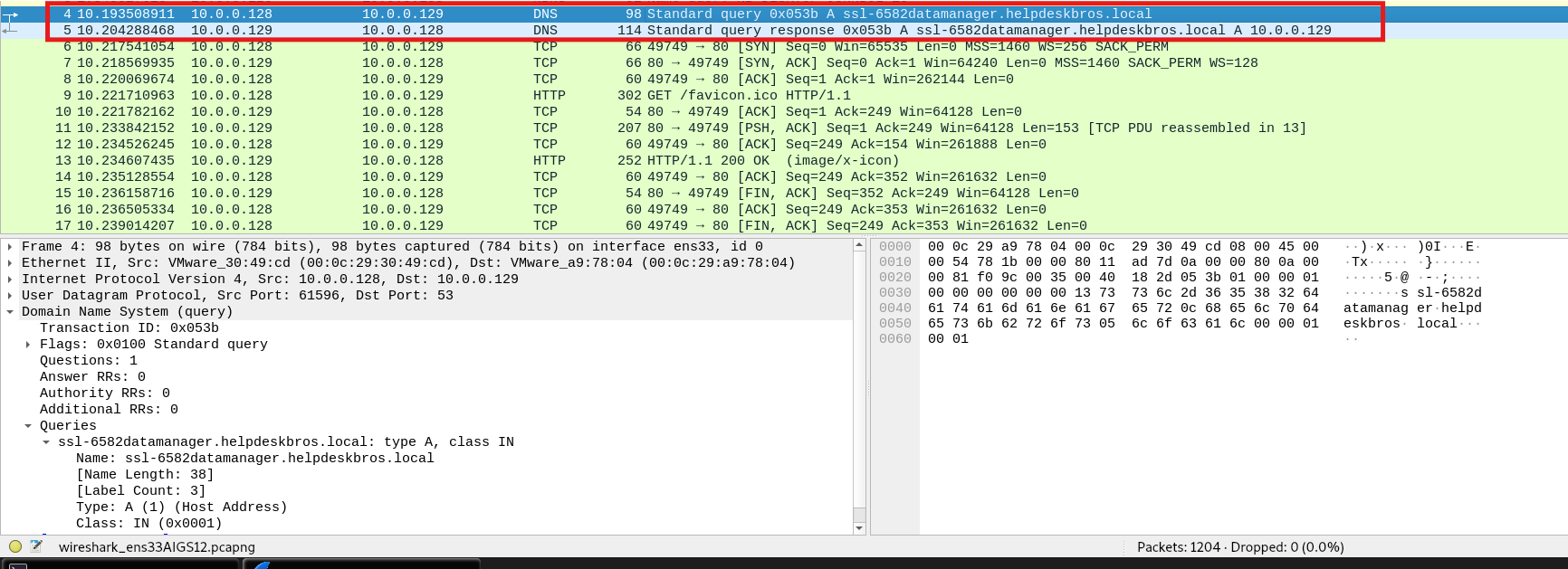


Figure Malware lets the victim ask for IP address of ssl-6582datamanager.helpdeskbros.local (captured from wireshark)

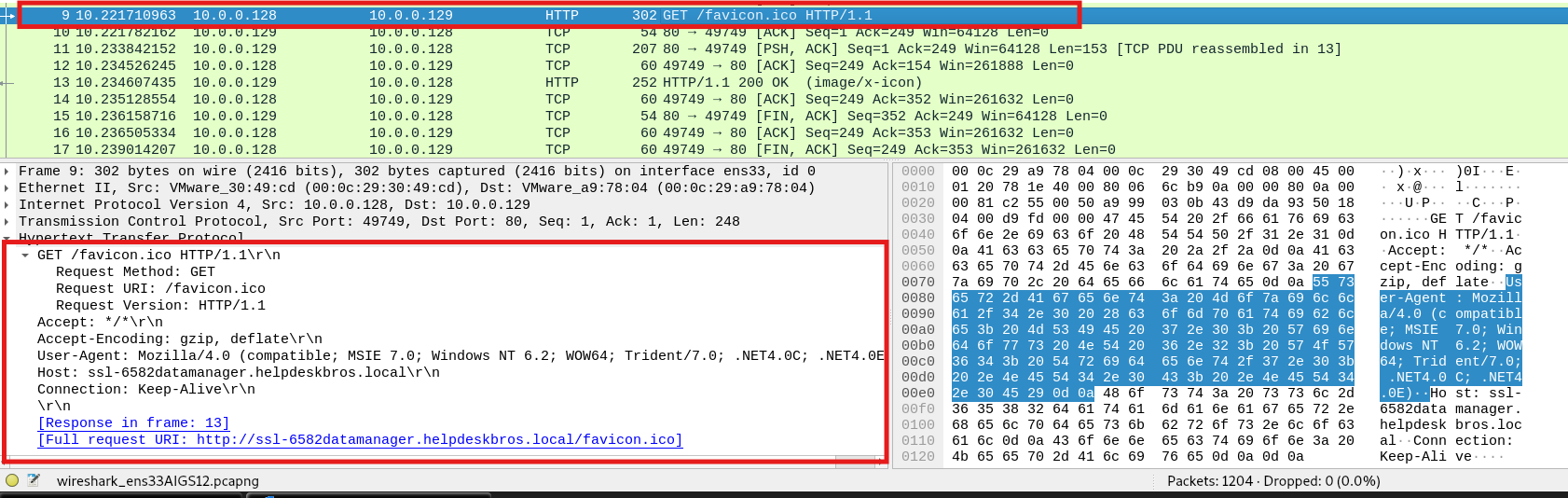


Figure Send HTTP Get Request for favicon.ico

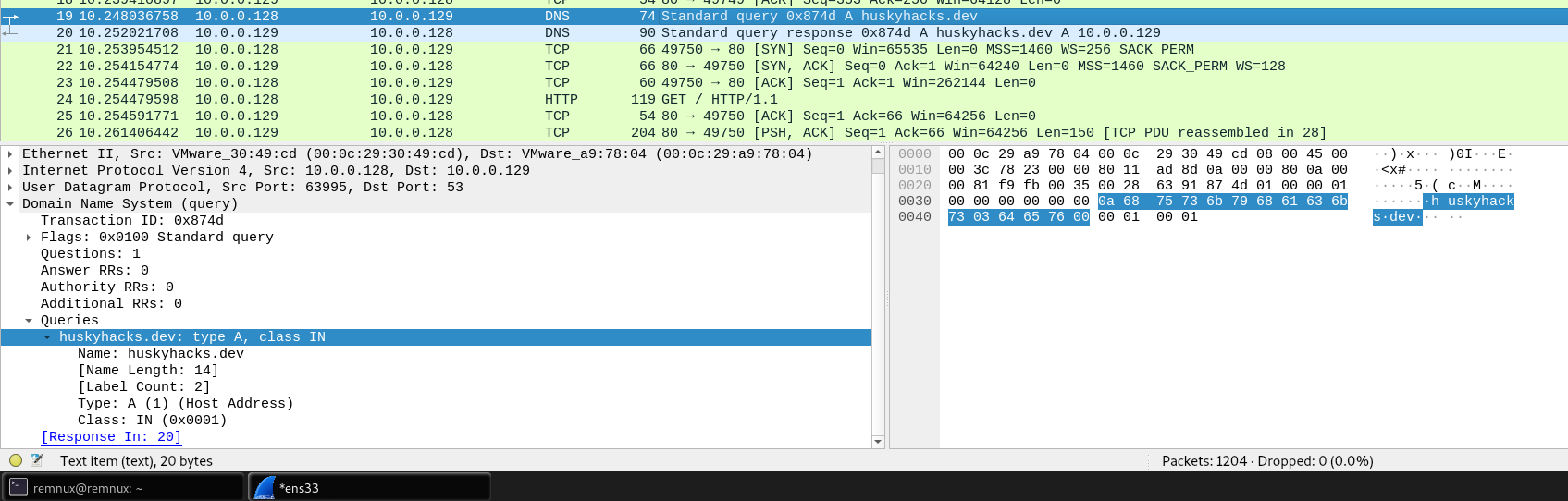


Figure Also ask for ip address of huskyhacks.dev

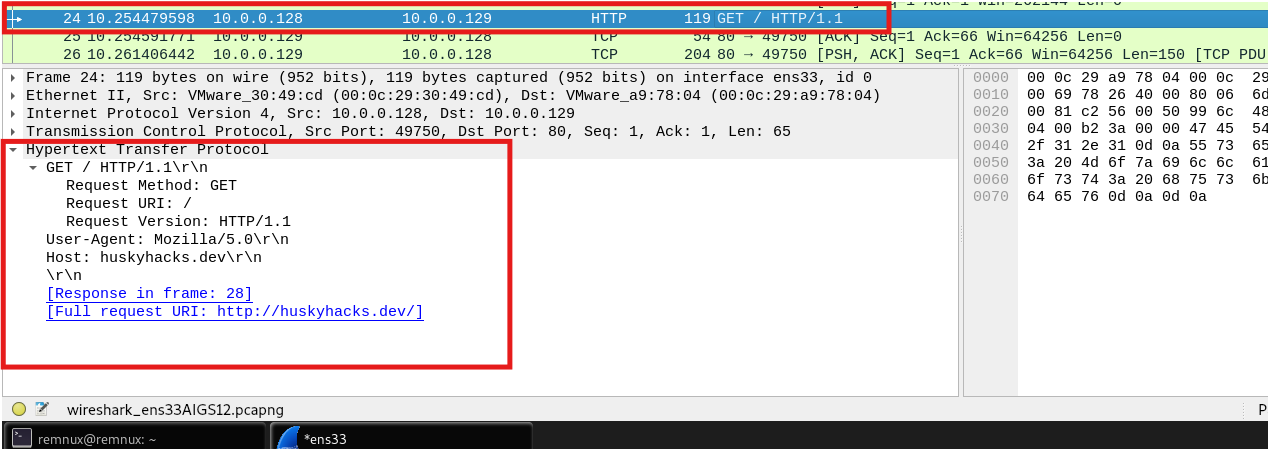


Figure Send HTTP Get Request to <http://huskyhacks.dev>

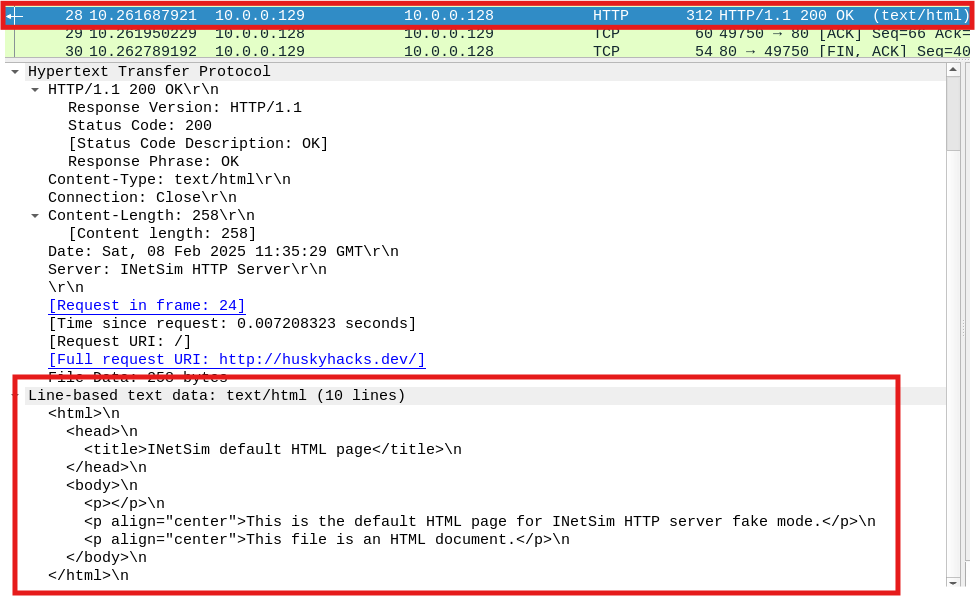


Figure Found the response after previous request, which INetSim acted as a huskyhacks.dev server

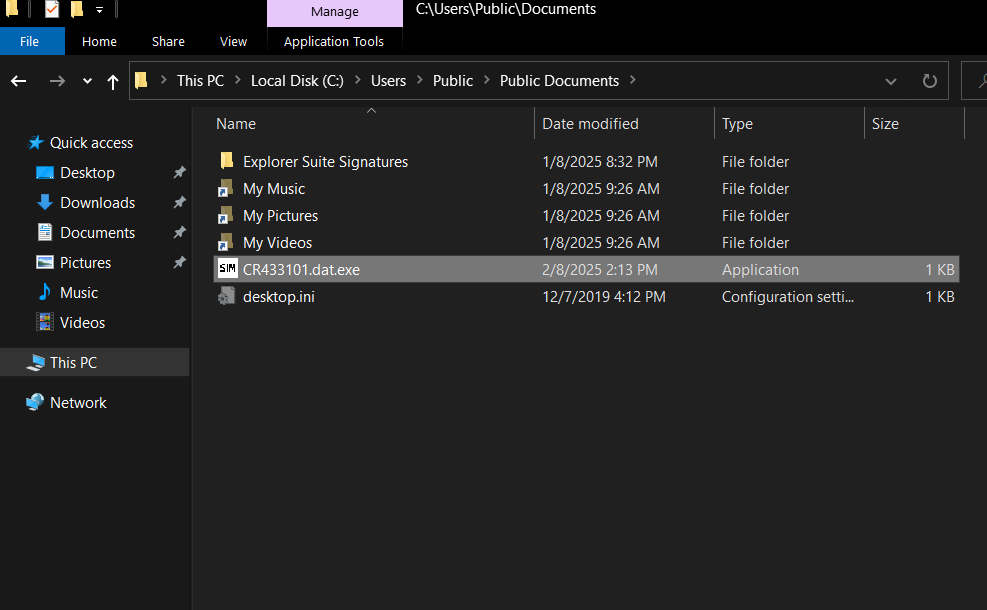


Figure Found the downloaded file after run malware

# Advanced Static Analysis



Figure main function

It called "URLDownloadToFileW" API to download file. Then test the value in eax, if file had been completely downloaded, eax = 0 and run the next operation. However, if eax was not equal 0, it jumped to 0x401142



Figure Completely download file

If the malware completely downloaded file, it continued to contact with <http://huskyhacks.dev>

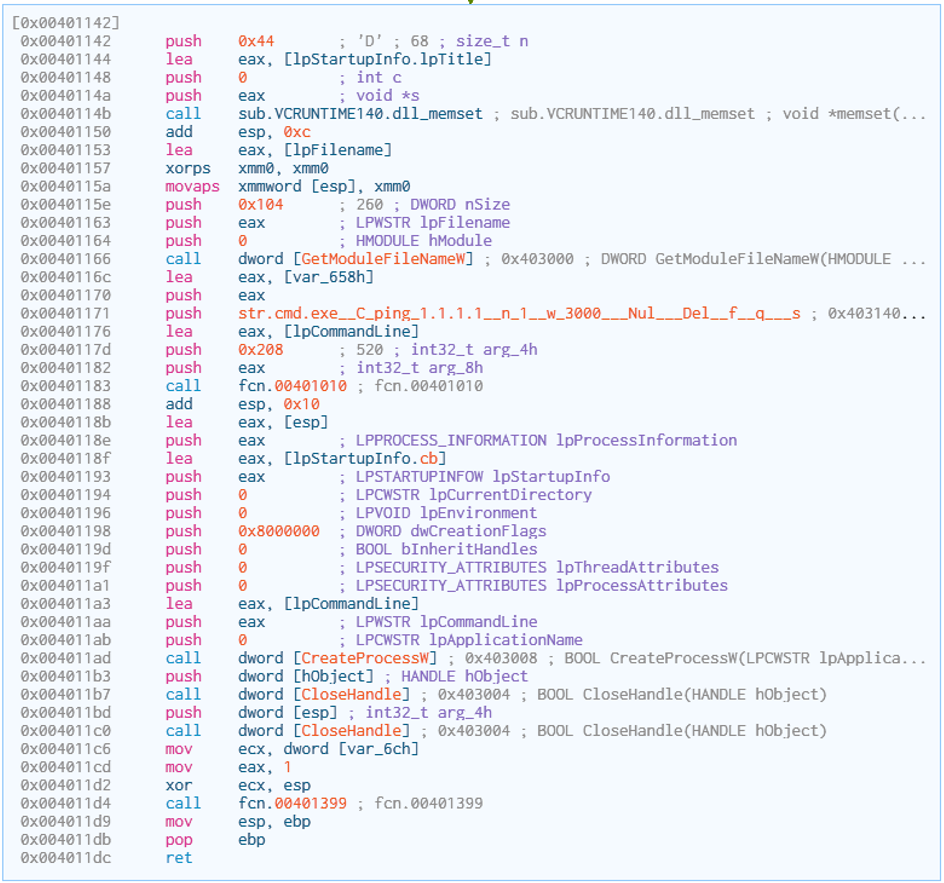


Figure Failed to download

If the malware cannot download the file, it jumped to 0x00401142. After that it ran the process to delete its activities and close the operation.

# Advanced Dynamic Analysis

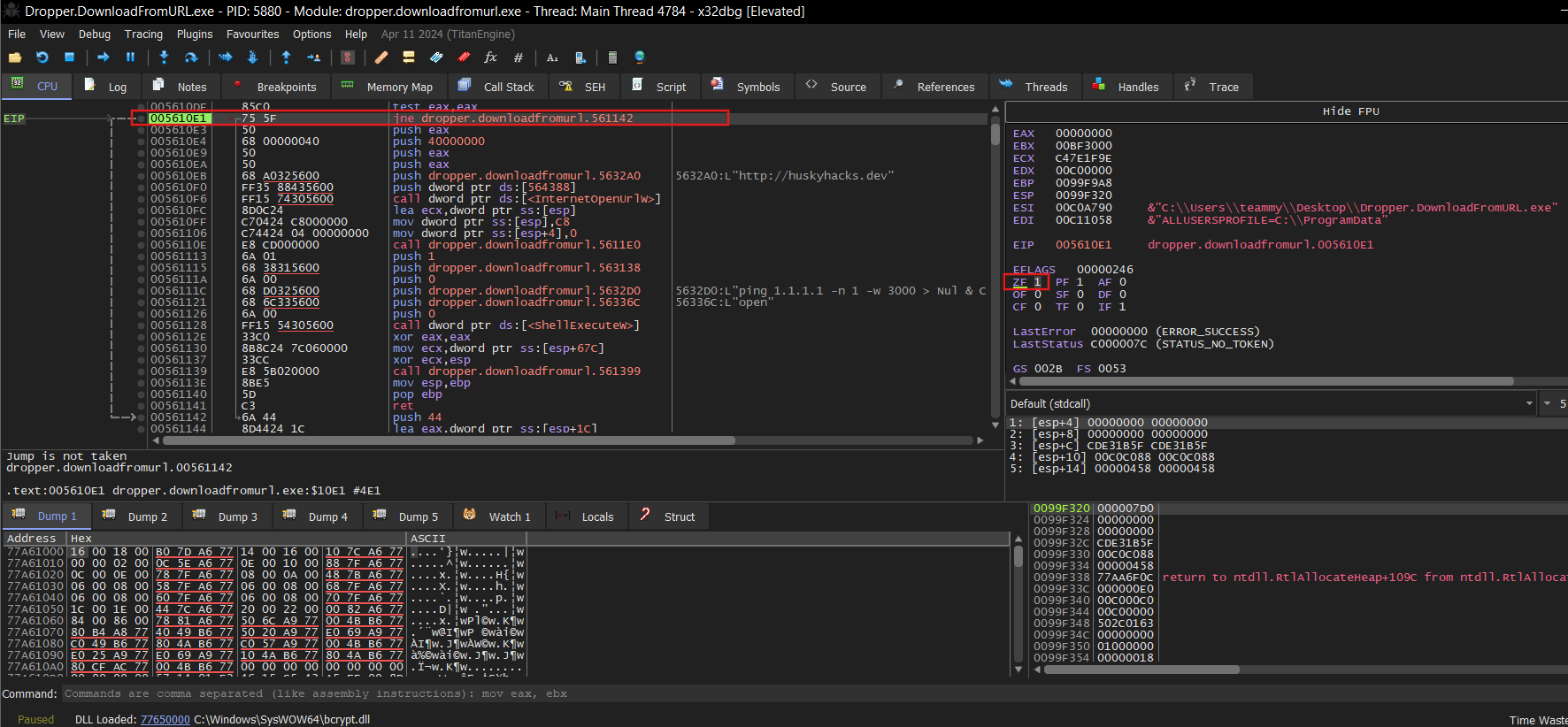


Figure x32dgb set ZF = 1

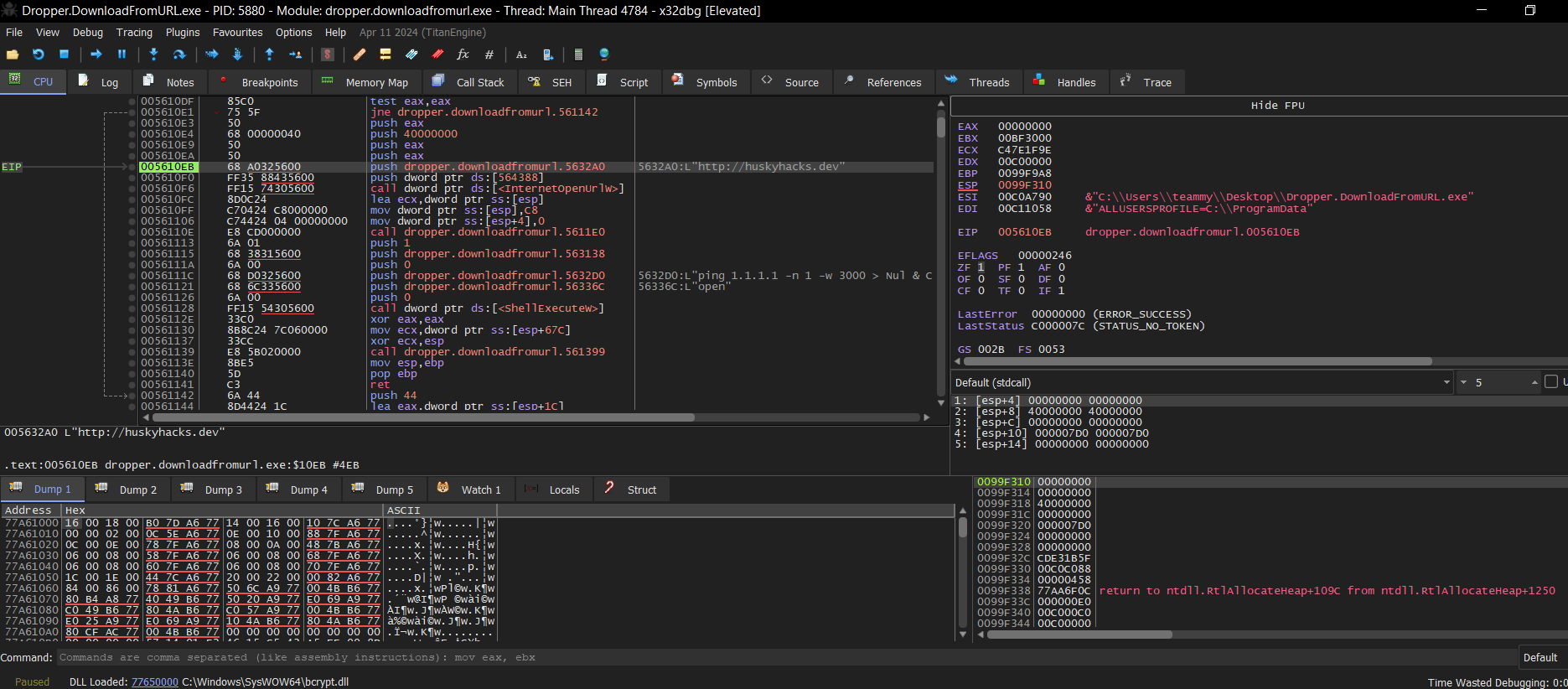


Figure Malware can contact huskyhacks.dev

If ZF = 1, the malware continued to the next process to contact <http://huskyhacks.dev>

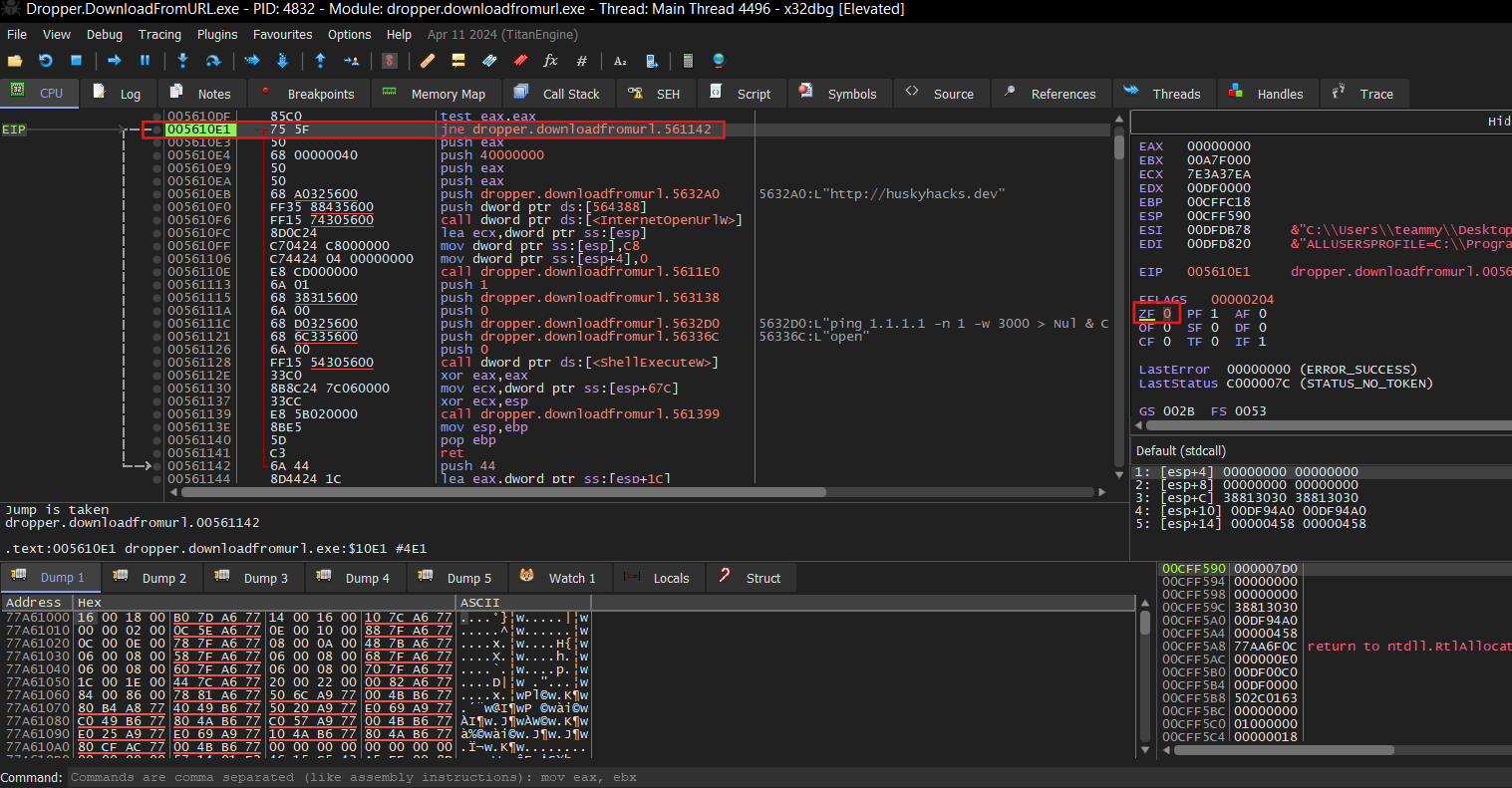


Figure x32dgb set ZF = 0

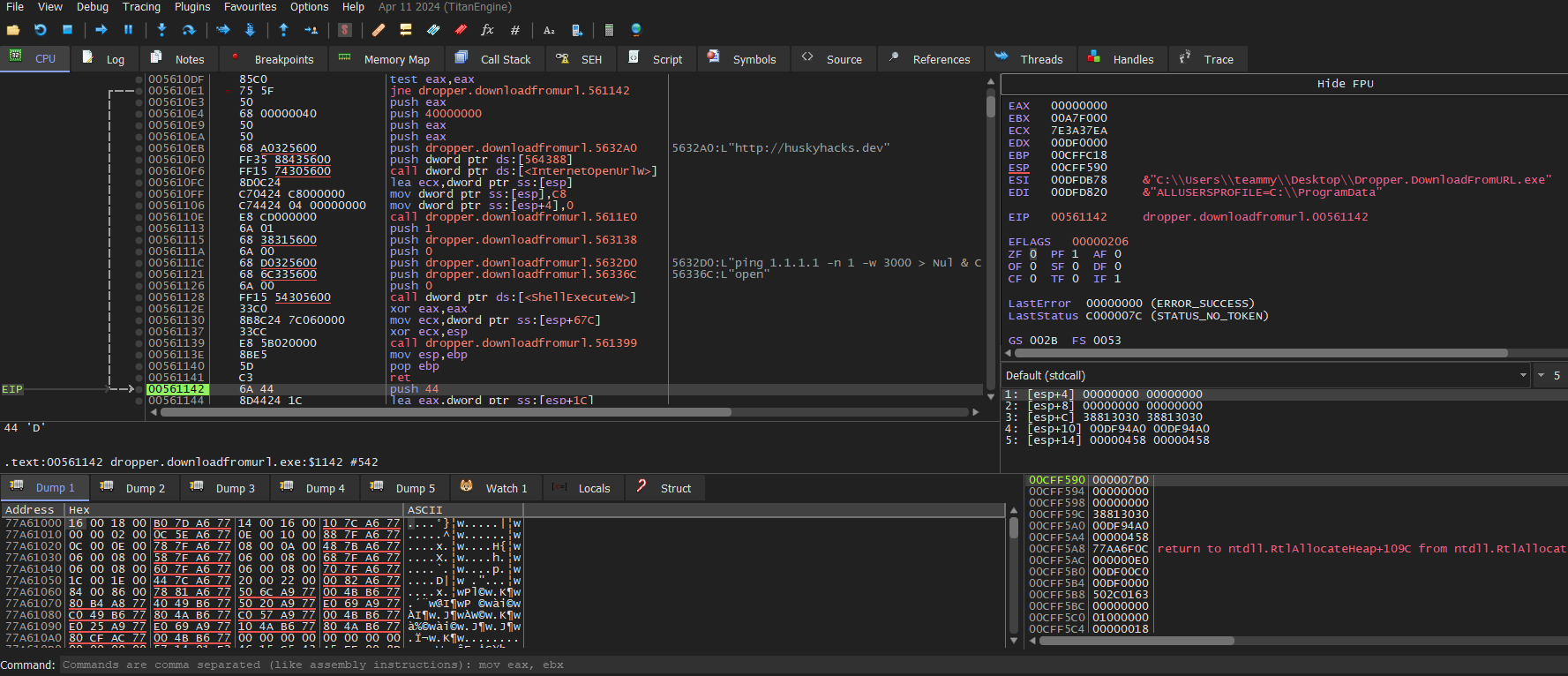


Figure Malware jump to 0x00401142 process

If ZF = 0, the malware jumped to the process which continued to delete itself

# Indicators of Compromise

## Network-based Indicators

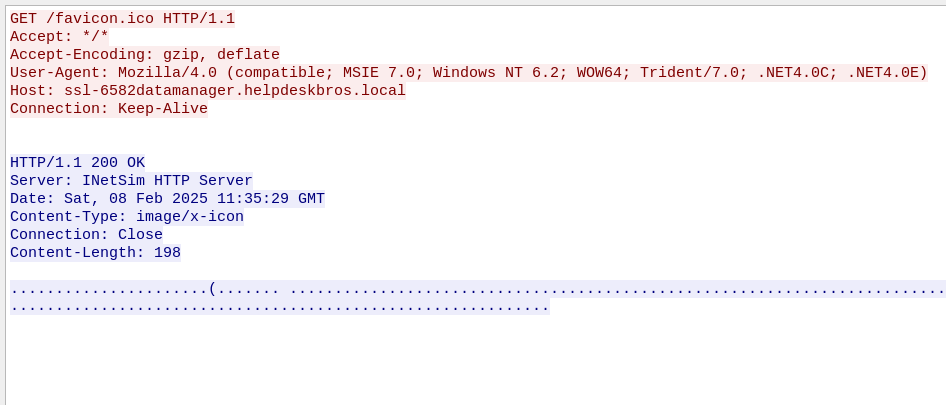


Figure This should be the initial step to download malware components

ssl-6582datamanager.helpdeskbros.local should be the site which contains malware component to do the next operation

## Host-based Indicators



Figure The downloaded file on the victim

From cutter, the malware downloaded the file favicon.ico, but saved the file as the name CR433101.dat.exe in path C:\Users\Public\Documents

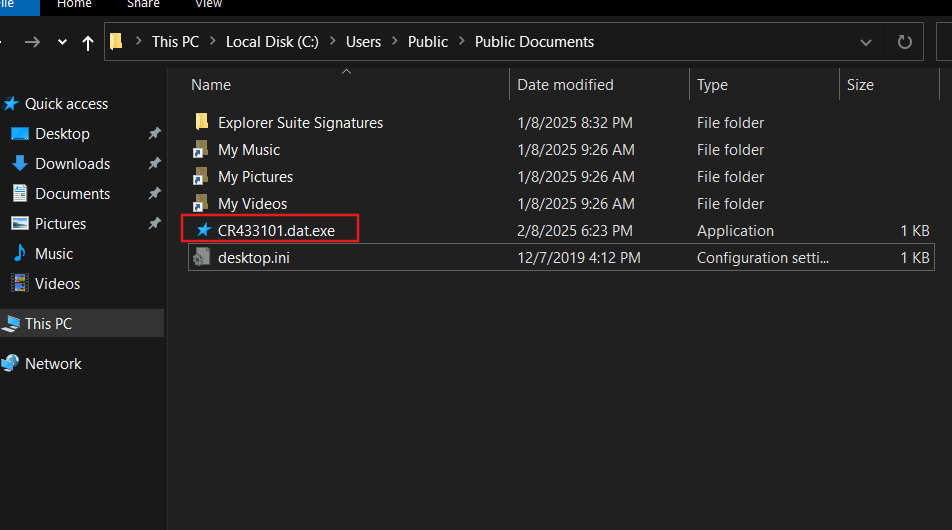


Figure Download file

# Rules and Signature

A full set of YARA rules is included in Appendix A.

# Appendices

## A. YARA Rule

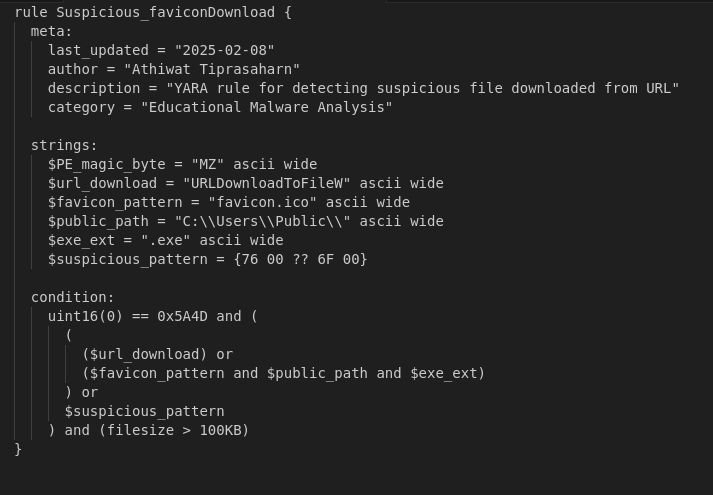


Figure Yara Rule

## B. Callback URL

|  |  |
| --- | --- |
| Domain | Port |
| http://ssl-6582datamanager.helpdeskbros.local | 80 |
| http://husky.hacks.dev | 80 |