Practical Malware Analysis & Triage
Malware Analysis Report

HuskyHacks Dropper Malware
(aka malware.unknown)

PRESENTED BY

DAVID GILMORE

June 2023

Table of Contents

Executive Summary

SHA256 hash	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
Md5 hash	1D8562C0ADCAEE734D63F7BAACA02F7C

The HuskyHacks malware.unknown.exe malware is a dropper malware I identified on 29th June 2023. HuskyHacks is a Windows 32bit self executable file that runs on Windows operating systems. The malware was created with Visual Studio 2008 and is written in C++. Information gathered from the static analysis phase indicates a compiler stamp of the 4th September 2008.

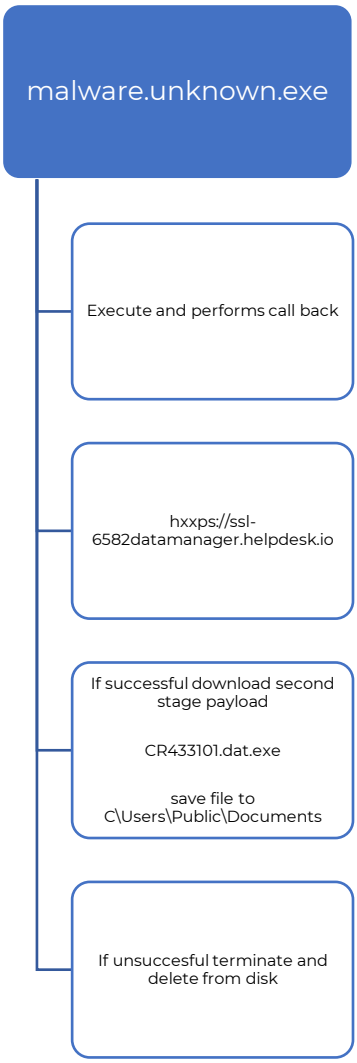
HuskyHacks malware, also known as malware.unknown.exe is a dropper malware that once executed downloads a second stage payload from a URL.

A search on VirusTotal.com shows that 53 out of the 71 vendors flag this file as malware. Reporting the file size as 12KB. Furthermore Virustotal.com has catagorised the threat as a Trojan, downloader and ransomware. HuskyHacks malware belongs to the bulz, vdmja and r002c0whh22 families of malware.

High-Level Technical Summary

HuskyHacks consists of two parts: an unencrypted stage 1 dropper and an unpacked and decoded stage 2 execution program called CR433101.dat.exe . It first attempts to contact its callback URL (hxxps://ssl-6582datamanager.helpdesk.io), if the URL can be reached the second stage payload is downloaded C:\Users\Public\Documents.

If the first stage is not able to reach the callback URL the malware does not run and deletes itself form disk with no further traces and no changes to the Windows file system or registry.



Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
Malware.unknown.exe	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
CR433101.dat.exe	A6AA84358130078F9455773AF1E9EF2C7710934F72DF8514C9A62ABEB83D2E81

Malware.unknown.exe
The initial executable that runs after a successful phishing campaign is a 32bit Windows application that is a dropper malware, it runs and then attempts to download a second stage payload calling back to a domain and requesting an ico file. The malware is written in C++.

Basic Static Analysis

During static analysis I used floss, Wireshark and PE Studio to analyze the malware sample. I identified several strings that were of interest:

Jjjj
Cmd.exe/ C ping 1.1.1.1 -n 1 -w 3000. nul and del /f fq "%s"
Cr433101.dat.exe
Mozilla/5.0
http://huskyhacks.dev

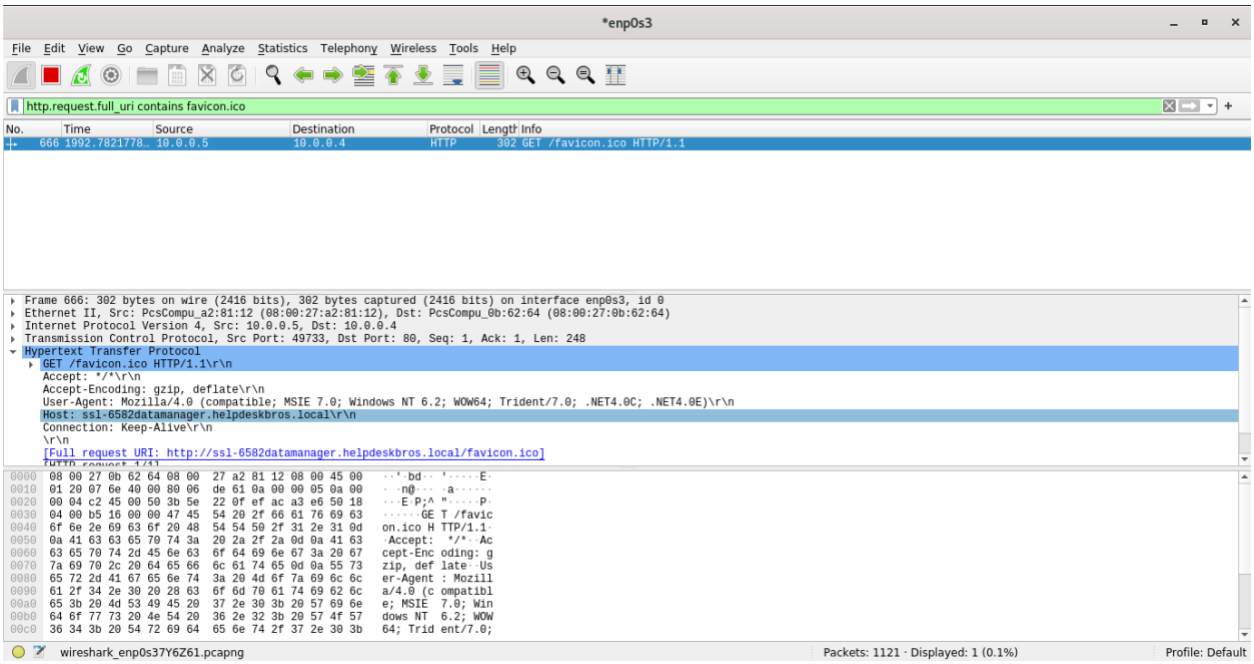
Using PE Studio I was able to identify the following Windows API calls:

- DownloadFromURL
- InternetOpenURLA
- ShellExec

Heuristic Analysis

During the heuristic phase of my analysis I used various tools including Procmon, Wire Shark and others to determine the malwares behavior.

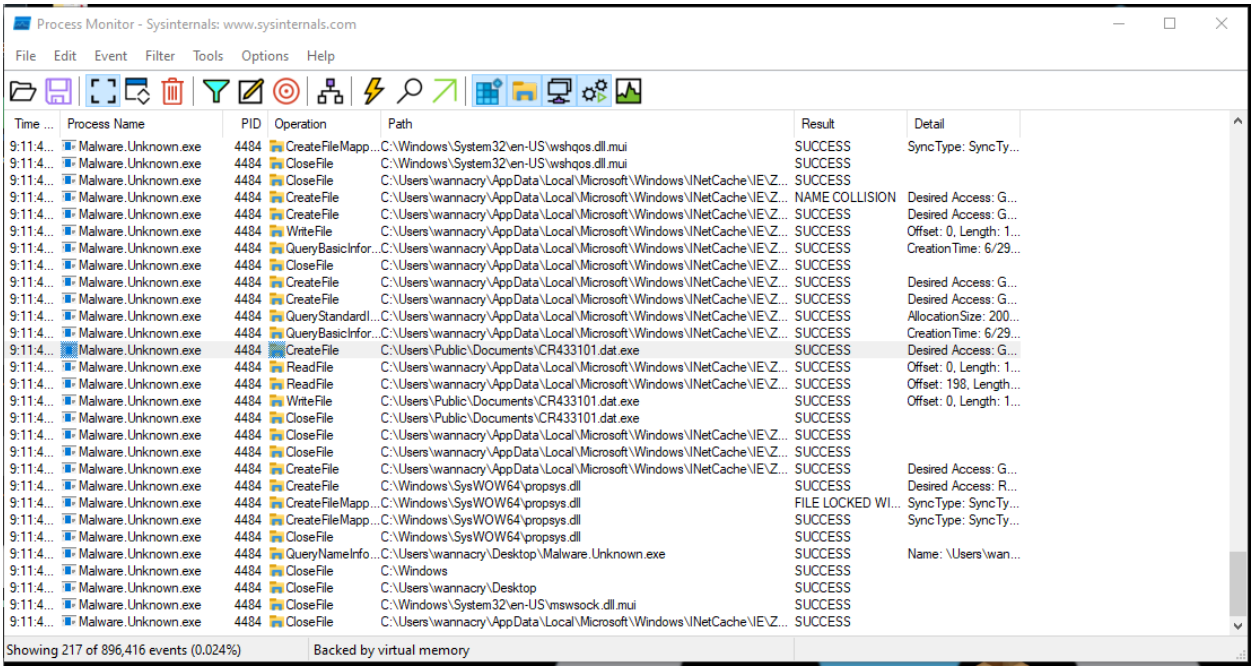
Once the malware had been executed I was able to capture packets using Wire Shark and filter the results to search for traffic related .ico files.



Wire Shark confirmed the malware was calling back to :

hxxp://ssl-6582datamanager.helpdeskbros.lo

Using Procmon I discovered the second stage malware file being written to disk



The file was named CR433101.dat.exe and was being written to :

C\Users\Public\Documents