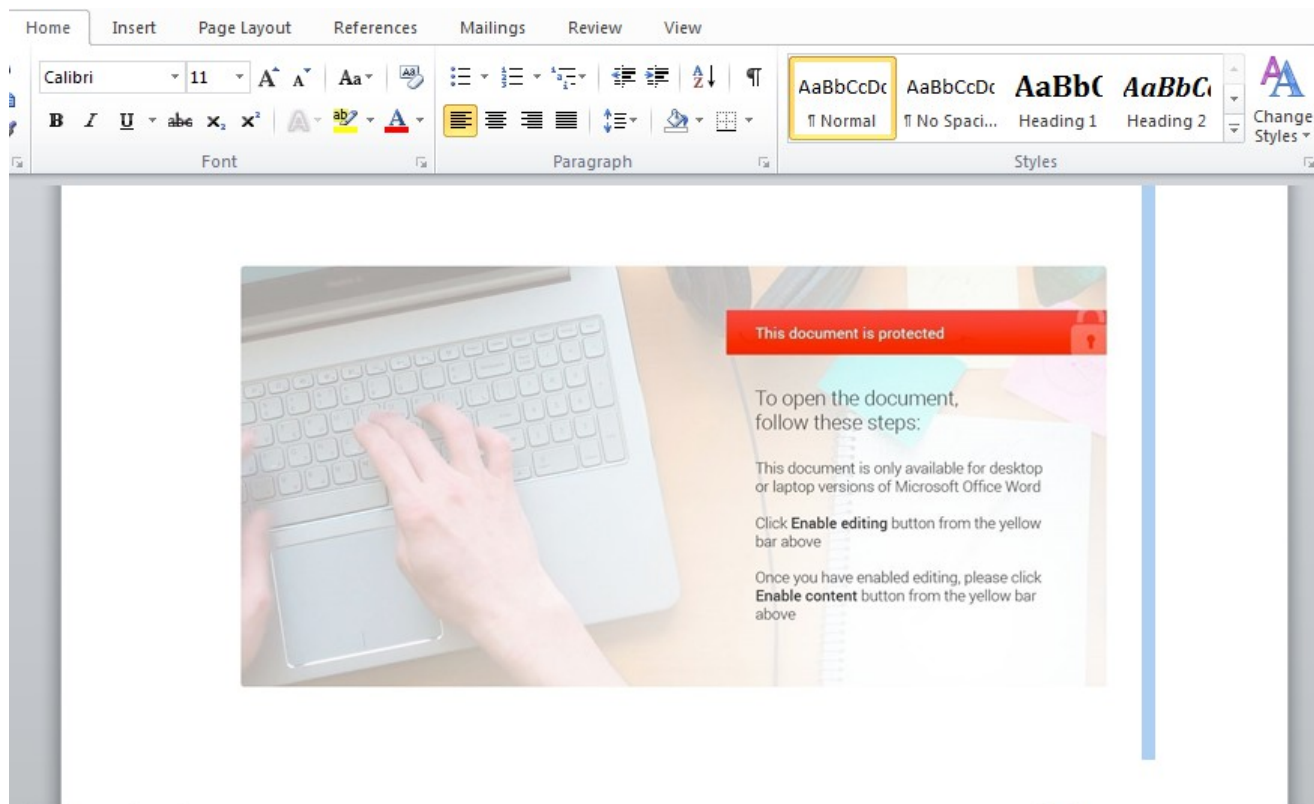
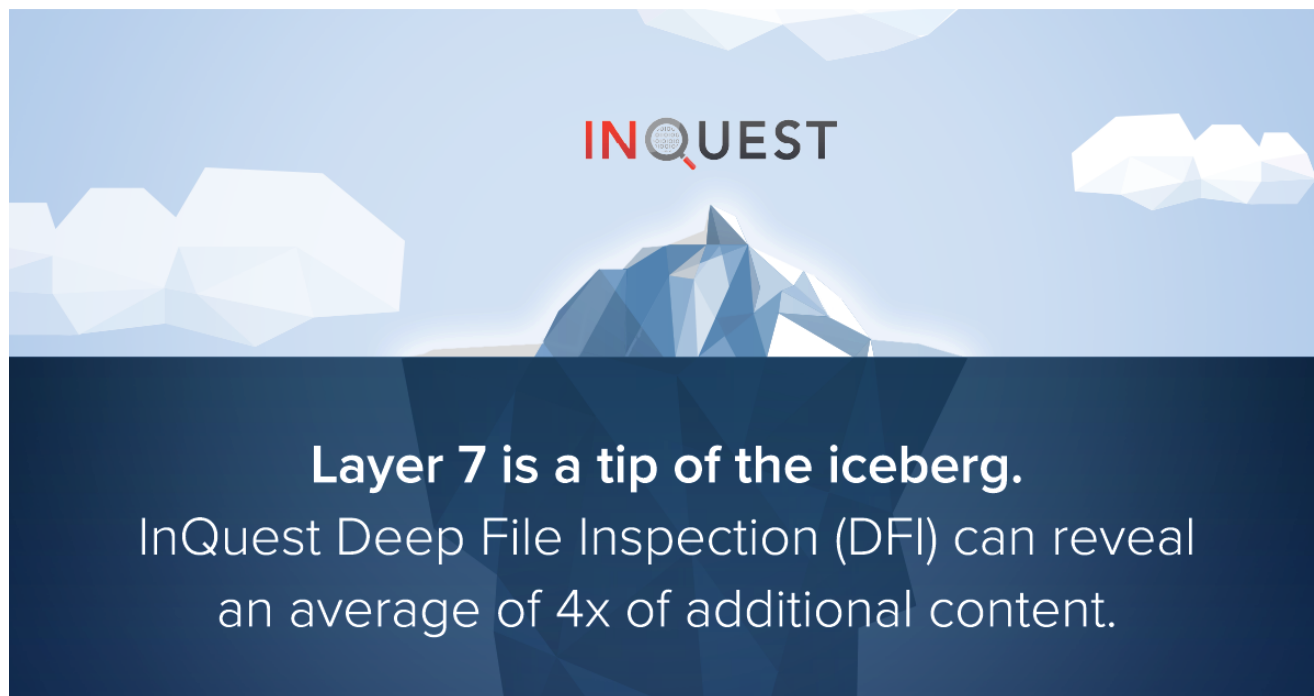


# Unearthing Hancitor Infrastructure

[inquest.net/blog/2021/04/16/unearthing-hancitor-infrastructure](https://inquest.net/blog/2021/04/16/unearthing-hancitor-infrastructure)

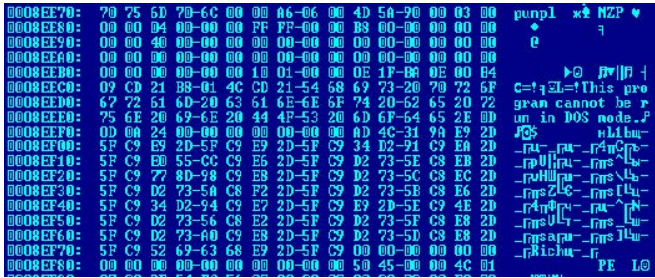


It's no secret that today, targeted attacks and phishing attacks are the primary means of spreading malware. The purpose of which is to collect user data, theft banking data, and espionage. Threat Actors are constantly working to improve the tools they use. In this article,

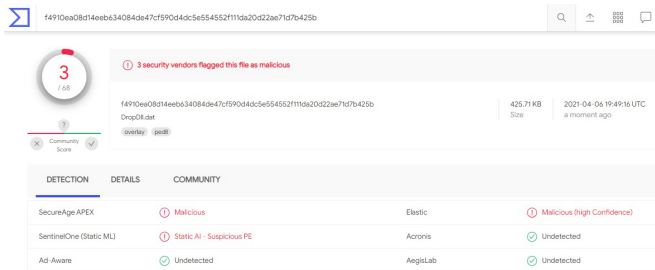
I will try to show you how the Hancitor group is improving their toolbox.

Looking at this malicious document MD5: [de80e1d7d9f5b1c64ec9f8d4f5063989](#)

As in previous versions of Hancitor, the add-on also contains an executable library.

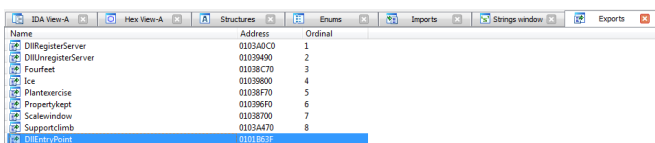


DLL MD5: [a4838dd31c672122441bebcf7e9d277](#) the developers of the malicious code have heavily modified the executable library. DLL is very heavily packaged, and the malicious code is hidden from the analysis. The first analysis of the sample had a meager detection rate on VirusTotal.

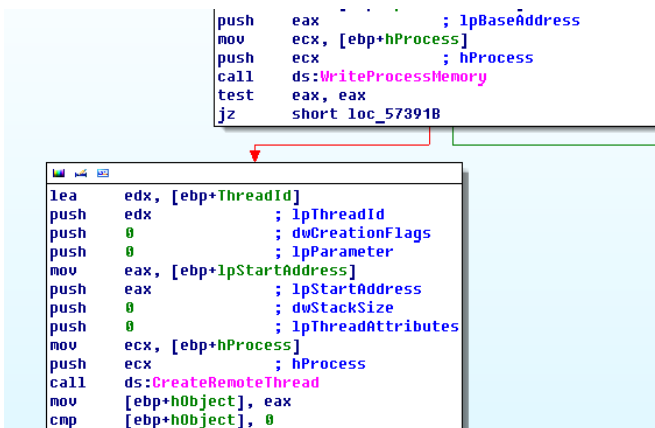


The library is unpacked using a sequential call of the exported functions. The payload of this campaign is contained in the unpacked library.

MD5: [BB948C6B1F60213D8A8C176A5CA2EDBB](#)



The malicious program writes itself to the svchost.exe address space and runs a remote thread.



Decrypting the code reveals the C2 address.

```

00572D9C | . FF15 10405700 CALL DUORD PTR DS:[&ADUAPI32.CryptDecrypt] ADUAPI32.CryptDecrypt
00572D9D | . 85C0 TEST EAX,EAX
00572D9E | . 75 04 JNZ SHORT UnpackF1.00572D9A
00572D9F | . EB 08 JMP SHORT UnpackF1.00572D9A
00572DA0 | . 00 JZ SHORT UnpackF1.00572D9A
EAX=00000001

```

Address	Hex dump	ASCII	0006D9F0
0037C640	30 35 30 34 5F 6B 68 72 6E 37 00 00 00 00 00 00	0504_khrn7.....	0006D9F4
0037C650	68 74 74 70 3A 2F 2F 64 69 76 65 6C 65 72 65 76	http://dntel.ru	0006D9F8
0037C660	6F 6C 2E 63 6F 6D 2F 38 2F 66 6F 72 75 6D 2E 70	ol.com/8/forum.p	0006D9FC
0037C670	68 70 7C 68 74 74 70 3A 2F 2F 70 6F 6C 69 6F 6E	http://pelion	0006E000
0037C680	61 6C 6C 61 73 2E 72 25 2F 38 2F 66 6F 72 75 6D	allac.ru/8/forum	0006E004
0037C690	2E 70 69 70 7C 68 74 74 70 3A 2F 2F 63 61 6D 65	.php/http://caen	0006E008
0037C6A0	74 61 74 65 6C 65 62 2E 72 75 2F 38 2F 66 6F 72	tateleb.ru/8/foe	0006E00C
0037C6B0	75 6D 2E 70 68 70 7C 00 00 00 00 00 00 00 00 00	un.php!.....	0006E010
0037C6C0	AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA		0006E014

At the beginning of the unpacked data, we see the identifier of the malicious campaign: **.0504\_khrn7**

```

.rdata:005741E8 00000008 C 0.0.0.0
.rdata:005741F0 00000008 C ncdeleb
.rdata:005741F8 0000003F C GUID=%8u&BUILD=%s&INFO=%s&EXT=%s&SP=%s&TYPE=1&WIN=%d.%d(64)
.rdata:00574238 0000003F C GUID=%8u&BUILD=%s&INFO=%s&EXT=%s&SP=%s&TYPE=1&WIN=%d.%d(32)
.rdata:00574278 0000000D C LoadLibraryA
.rdata:00574288 0000000F C LoadLibraryExA

```

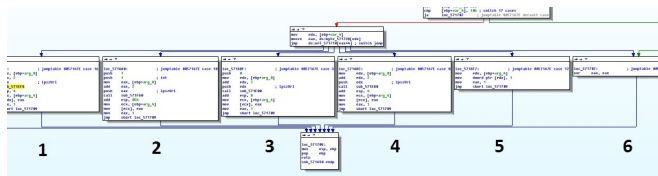
After collecting data from the compromised system, the program sends the data to a remote server using a specific mask. After transferring data to the server, the program waits for 100 minutes for a remote command.

```

loc_57195A: ; dwMilliseconds
push 60000
call ds:Sleep
call Control_Response_C2
push 60000 ; dwMilliseconds
call ds:Sleep
jmp loc_5718B2

```

Based on the data received, the threat actor decides how to further execute the malicious code. He has the ability to execute 6 commands.



### Sequencing

1. Download the executable file and run it as a DLL library.
2. Launches the svhost.exe, then downloads an executable file and writes it to the svhost.exe address space.
3. Download the executable file and run it as a code in the self addr. space.
4. Download the executable file and run it as a code in the self addr. space.
5. The program goes into a further sleep (100min) mode.
6. The program is terminated.

Target executable file that is executed:

[http://tren0.ru/6jhuy675rt\[.\]exe](http://tren0.ru/6jhuy675rt[.]exe)

MD5:77be0dd6570301acac3634801676b5d7

## IOC

[http://divelerevol.com/8/forum\[.\]php](http://divelerevol.com/8/forum[.]php)

[http://polionallas.ru/8/forum\[.\]php](http://polionallas.ru/8/forum[.]php)

[http://cametateleb.ru/8/forum\[.\]php](http://cametateleb.ru/8/forum[.]php)

## Bio

Dmitry Melikov is a malware researcher that has a passion for reverse engineering and information security.

[LinkedIn](#)

[Twitter](#)

---

## Tags

[guest malware-analysis labs](#)

## Get The InQuest Insider

---

Find us on [Twitter](#) for frequent updates, follow our [Blog](#) for bi-weekly technical write-ups, or subscribe here to receive our monthly newsletter, The InQuest Insider. We curate and provide you with the latest news stories, field notes about innovative malware, novel research / analysis / threat hunting tools, security tips and more.