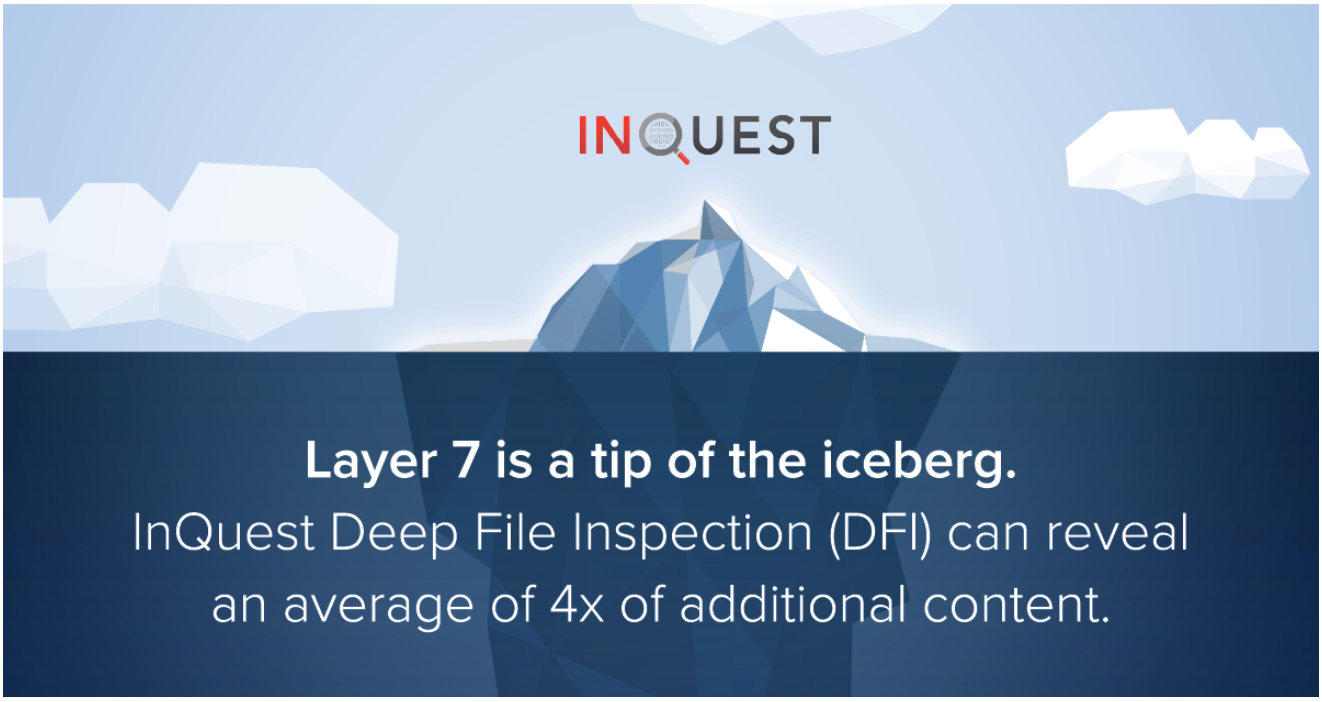
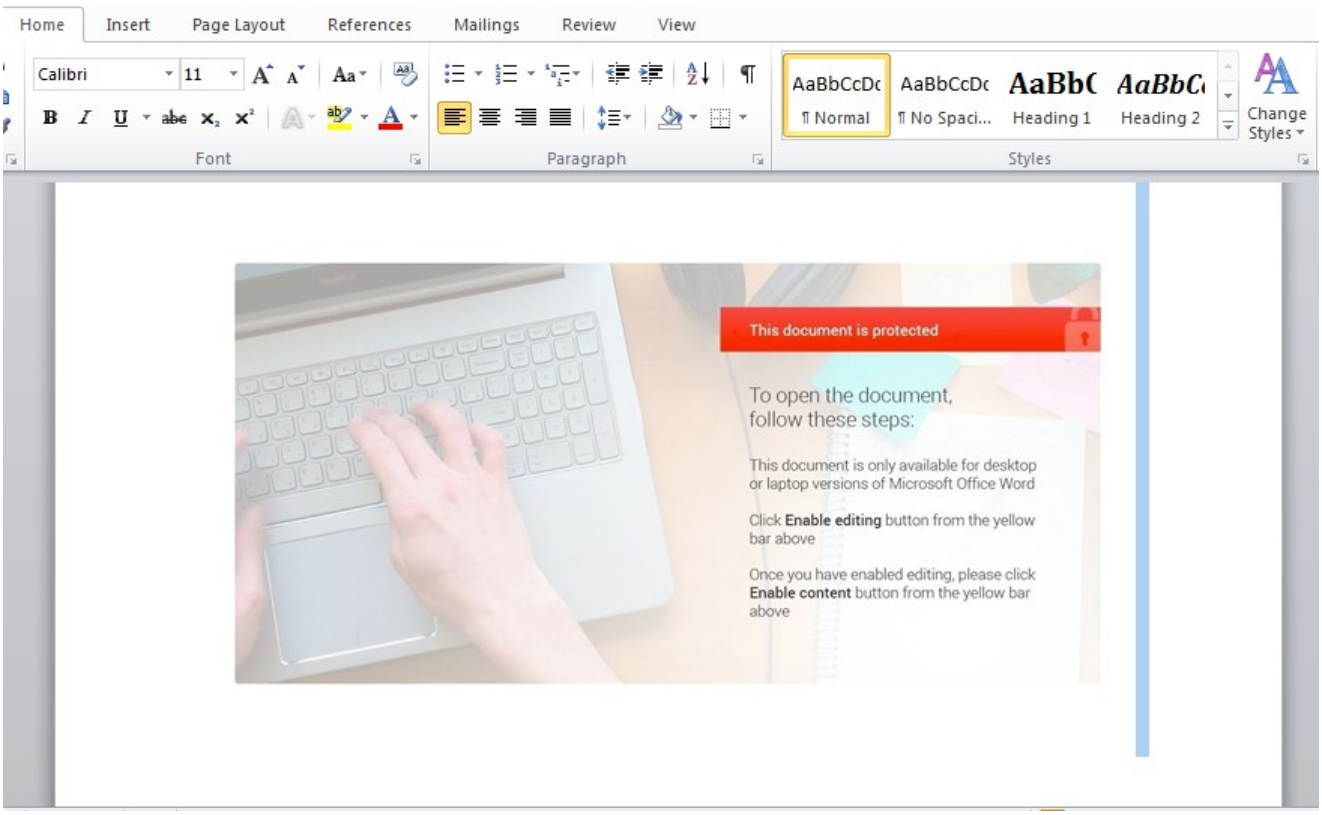
Unearthing Hancitor Infrastructure

inquest.net/blog/2021/04/16/unearthing-hancitor-infrastructure



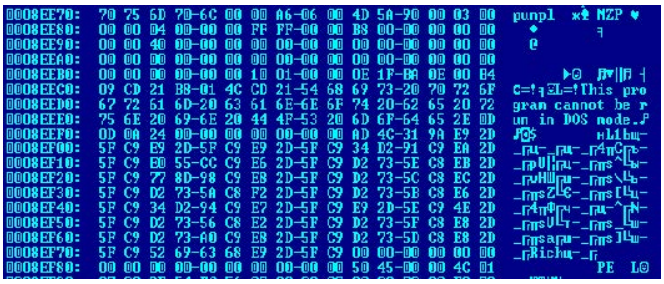


It's no secret that today, targeted attacks and phishing attacks are the primary means of spreading malware. The purpose of which is to collect user data, theft banking data, and espionage. Threat Actors are constantly working to improve the tools they use. In this article,

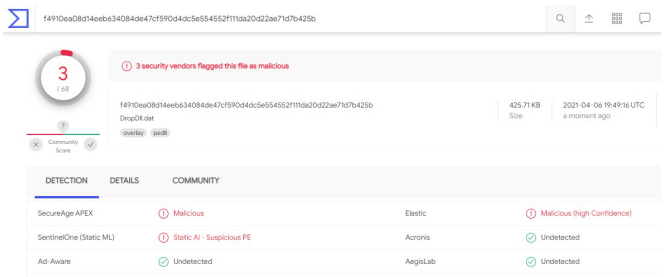
I will try to show you how the Hanictor group is improving their toolbox.

Looking at this malicous document MD5: de80e1d7d9f5b1c64ec9f8d4f5063989

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

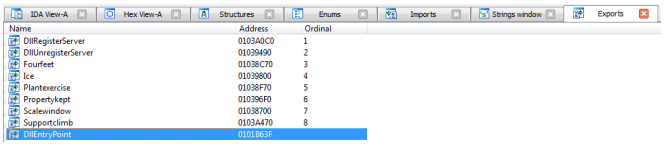


DLL MD5: a4838dd31c672122441bebcbf7e9d277 the developers of the malicious code have heavily modified the executable library. DLL is very heavily packaged, and the malicious code is hidden from the analysis. The first analysis of the sample had a meager detection rate on VirusTotal.



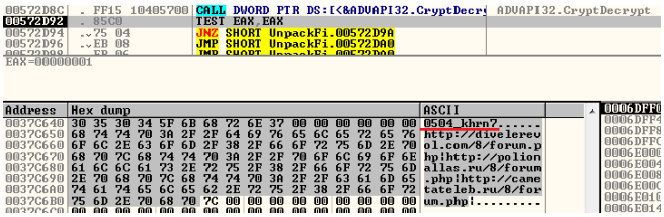
The library is unpacked using a sequential call of the exported functions. The payload of this campaign is contained in the unpacked library.

MD5: BB948C6B1F60213D8A8C176A5CA2EDBB

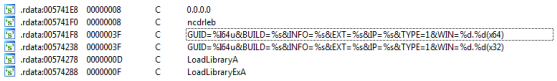


The malicious program writes itself to the svchost.exe address space and runs a remote thread.

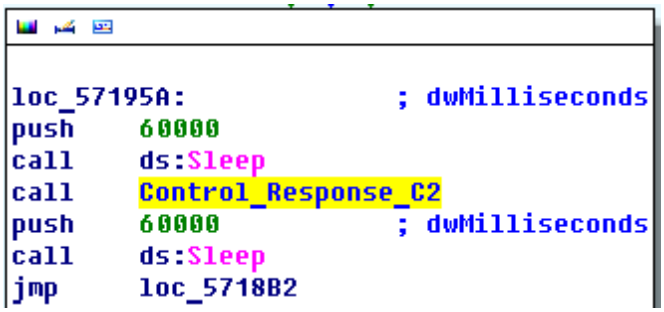
Decrypting the code reveals the C2 address.



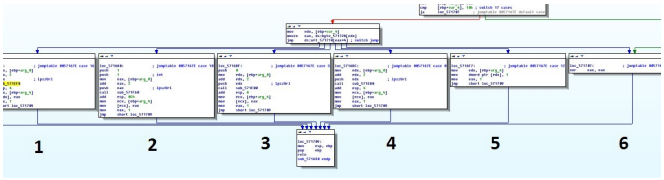
At the beginning of the unpacked data, we see the identifier of the malicious campaign:
.0504_khrn7



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.



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 adrr. space.
4. Download the executable file and run it as a code in the self adrr. 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
MD5:77be0dd6570301acac3634801676b5d7

IOC
http://divelerevol.com/8/forum[.]php
http://polionallas.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