Mrgod

3 min read · Draft · Listen

NOVA CTF 2023 (Forensics)

CHALLENGE : NOVA_VIRUS

CATEGORY : FORENSICS

CHALLENGE DESCRIPTION:

The player has been recruited as an agent by the Impossible Mission Force (IMF) to investigate a virus that has infected a top-secret government computer system. The virus is causing havoc within the system, and the player must find the source of the infection and extract the hidden flag.

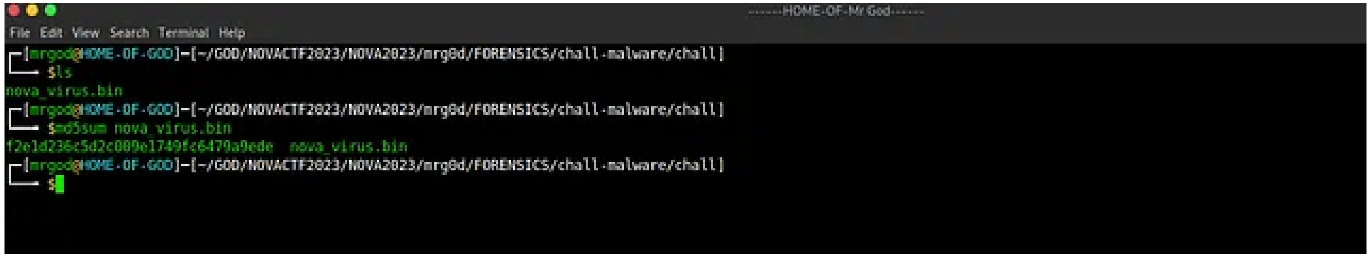
Given File : nova_virus.bin

You've got yourself a mission here! Let's dive right in and see what kind of adventure we can have.

So, you want to identify the hash of a file called nova_virus.bin? Well, that's easy peasy lemon squeezy! Just use the command

```
$md5sum nova_virus.bin
```

and voila, you've got your hash!



------HOME-OF-Mr God------
File Edit View Search Terminal Help

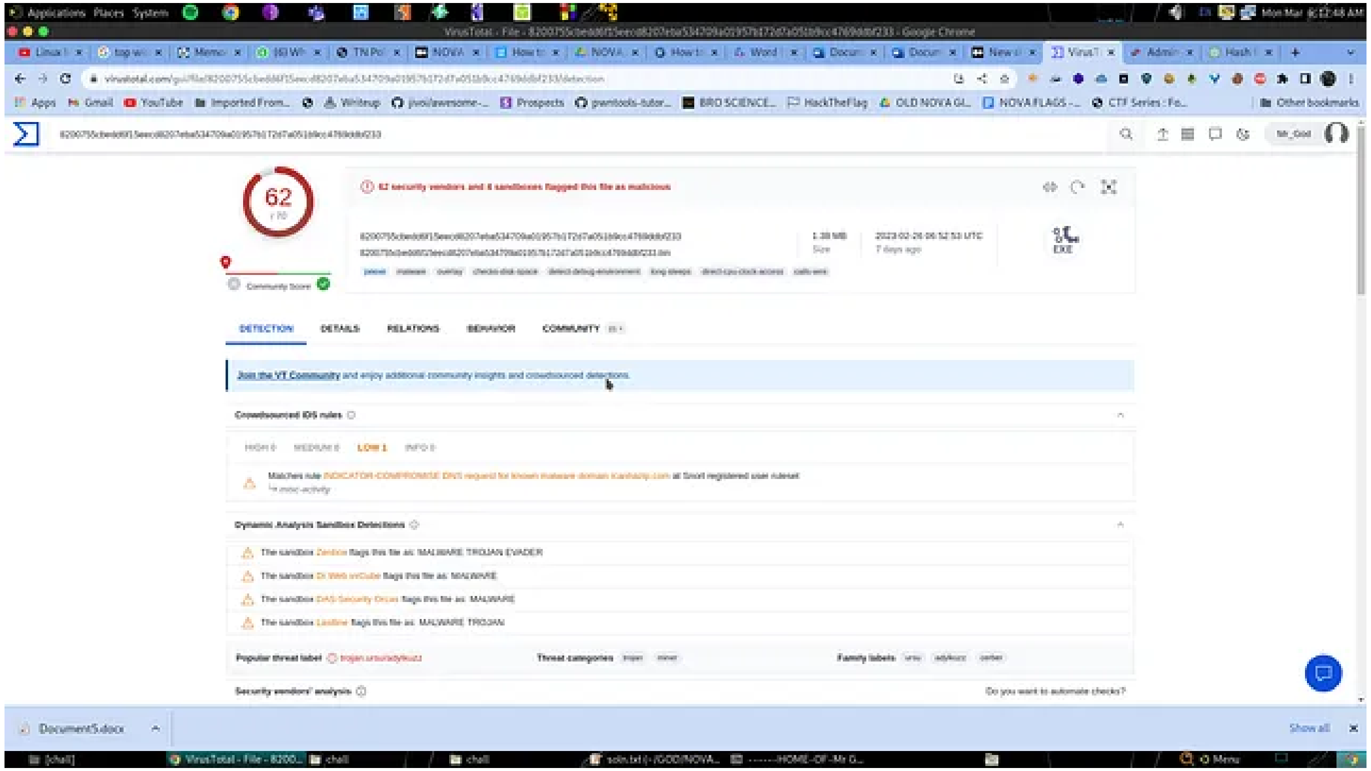
```
┌─[mrgod@HOME-OF-GOD]─[~/GOD/NOVACTF2023/NOVA2023/mrg0d/FORENSICS/chall-malware/chall]
└──╼ $ls
nova_virus.bin
┌─[mrgod@HOME-OF-GOD]─[~/GOD/NOVACTF2023/NOVA2023/mrg0d/FORENSICS/chall-malware/chall]
└──╼ $md5sum nova_virus.bin
f2e1d236c5d2c009e1749fc6479a9ede  nova_virus.bin
┌─[mrgod@HOME-OF-GOD]─[~/GOD/NOVACTF2023/NOVA2023/mrg0d/FORENSICS/chall-malware/chall]
└──╼ $
```

Hash

The hash is **f2e1d236c5d2c009e1749fc6479a9ede.**

Now, the next step is to check for this hash on VirusTotal. But wait, there's more! If you check the community section, you'll see a post by someone named **mr_god**. He's even given you a drive link! What a helpful guy.

Drive Link : **https://drive.google.com/file/d/1Y3q2-iylvgutR6QYhN-YWhhvEWLgvC0U/view?usp=share_link**



62 security vendors and 4 sandboxes flagged this file as malicious

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Crowdsourced IDS rules

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE TROJAN EVADER

The sandbox Dr.Web vxCube flags this file as: MALWARE

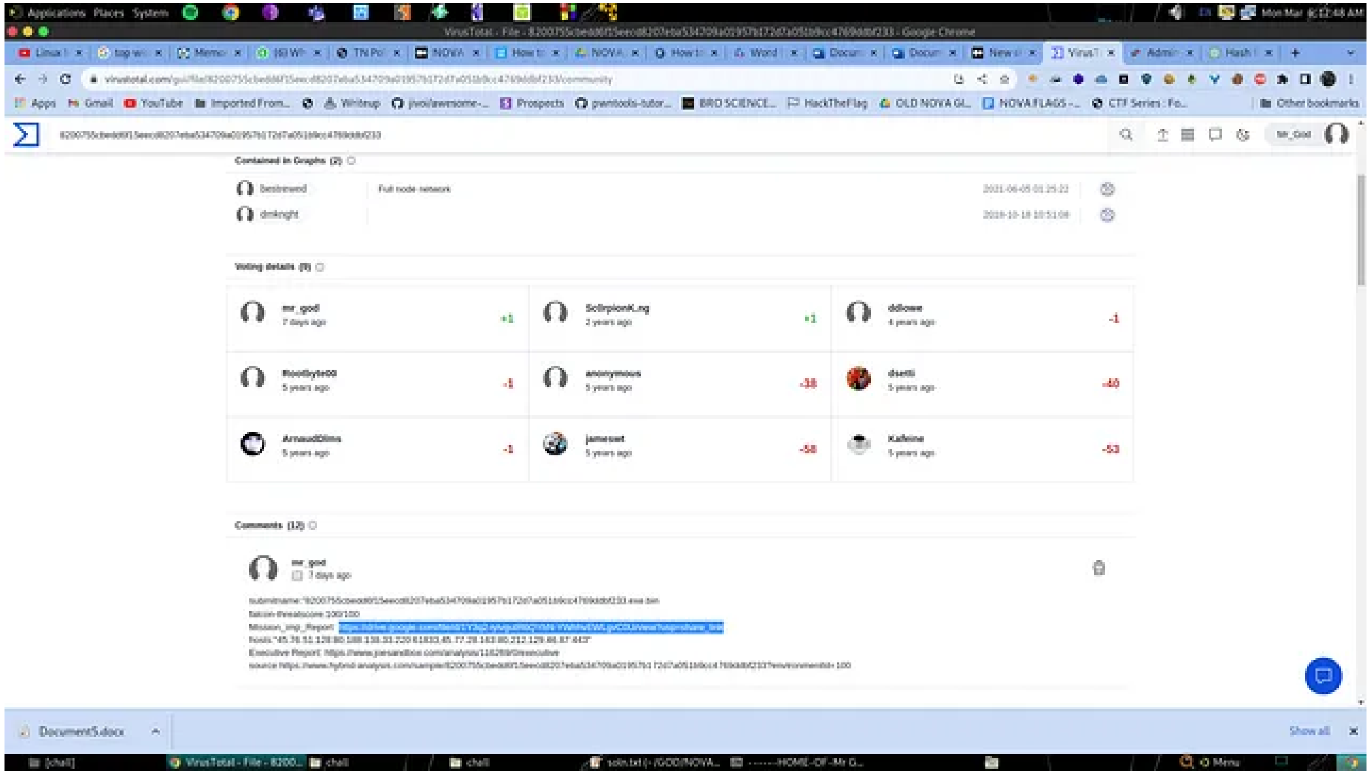
The sandbox DAS-Security Orcas flags this file as: MALWARE

The sandbox Lastline flags this file as: MALWARE TROJAN

Security vendors' analysis

Do you want to automate checks?

Virustotal



Contained in Graphs (2)

bestrewed	Full node network	2021-06-05 01:25:22
dmknght		2018-10-18 10:51:08

Voting details (9)

mr_god 7 days ago +1	ScIrpionK_ng 2 years ago +1	ddlowe 4 years ago -1
floodbyte00 5 years ago -1	anonymous 5 years ago -38	dsetti 5 years ago -40
ArnaudDlms 5 years ago -1	jameset 5 years ago -58	Kafeine 5 years ago -53

Comments (12)

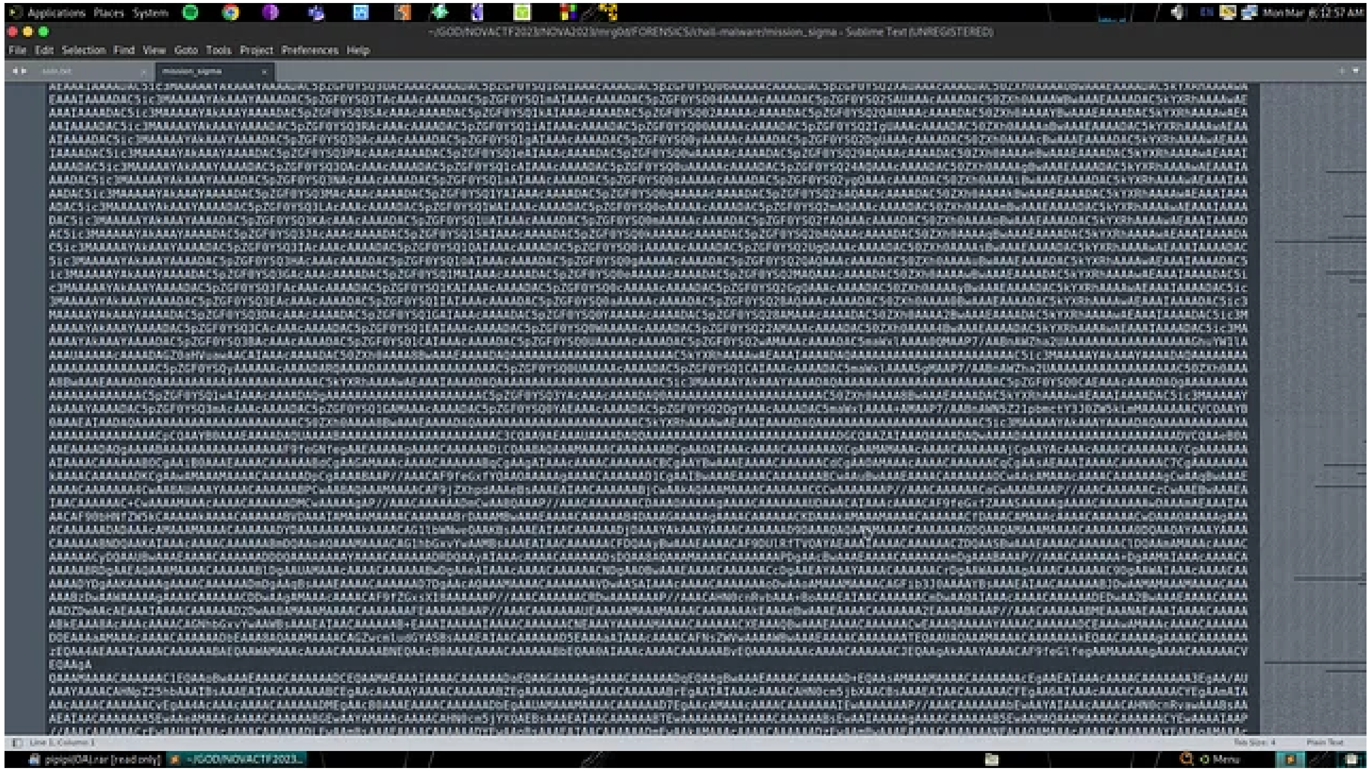
mr_god
7 days ago

```
submitname:"[illegible].exe.bin
falcon-threatscore 100/100
Mission_img_Report: [illegible]
hosts:"45.76.51.120:80 [illegible]"
Executive Report: https://www.joesandbox.com/analysis/[illegible]/executive
source:https://www.hybrid-analysis.com/sample/[illegible]?environmentId=100
```

The guy..!

Wait ..! who is that guy?

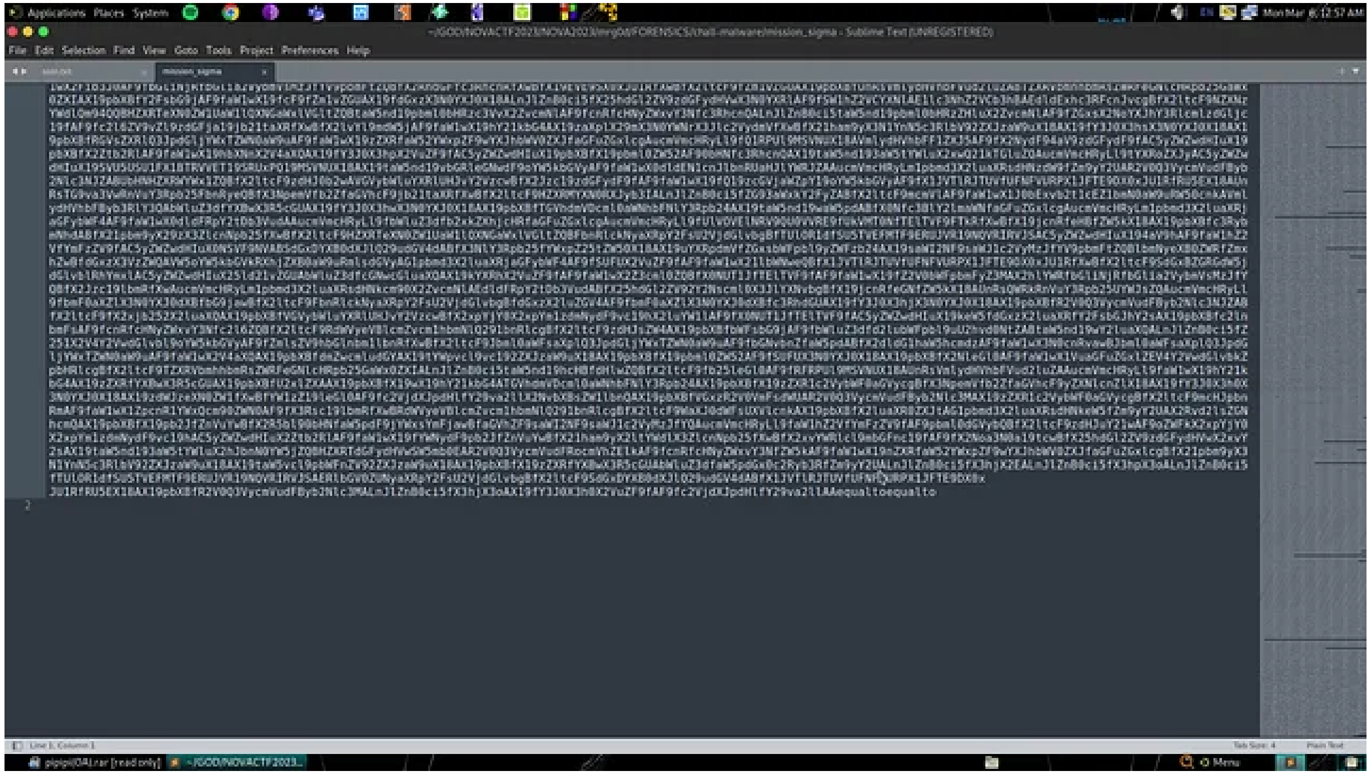
So, you click on the link and download a file called **mission_sigma.** But what's this? It's just a bunch of gibberish.


Applications Places System
~/GOD/NOVACTF2023/NOVA2023/mrgod/FORENSICS/chall-malware/mission_sigma - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
mission_sigma
Mon Mar 6 12:57 AM

eeeeeeeee....!!!

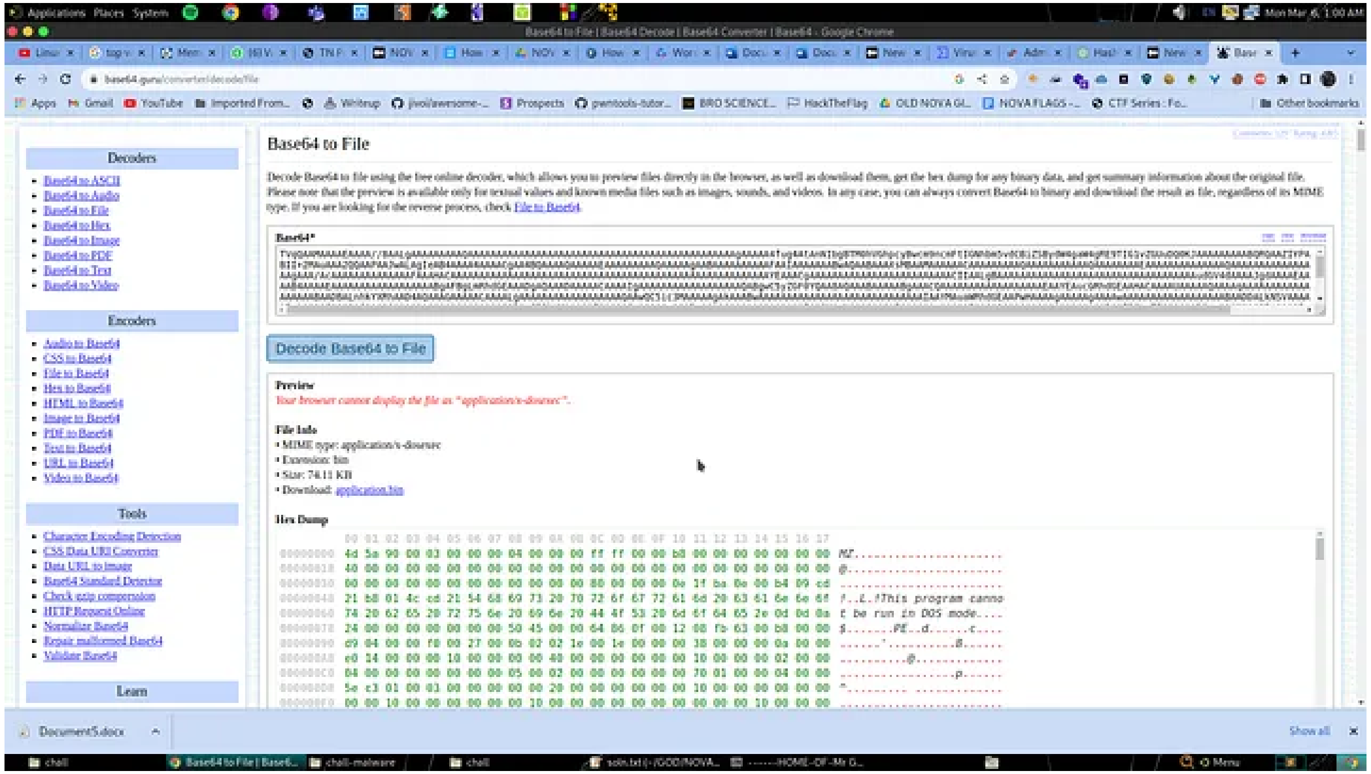
Don't panic! That gibberish is actually base64 encoded content.

But when i try to convert it into a file , it throws an error....!!After i noticed..!


Applications Places System
File Edit Selection Find View Goto Tools Project Preferences Help
mission_sigma

equaltoequalto?

change that **equaltoequalto ~ ==**



Base64 to File

Decode Base64 to file using the free online decoder, which allows you to preview files directly in the browser, as well as download them, get the hex dump for any binary data, and get summary information about the original file. Please note that the preview is available only for textual values and known media files such as images, sounds, and videos. In any case, you can always convert Base64 to binary and download the result as file, regardless of its MIME type. If you are looking for the reverse process, check File to Base64.

Base64*

[illegible]

Preview

Your browser cannot display the file as "application/x-dosexec".

File Info
- MIME type: application/x-dosexec
- Extension: bin
- Size: 74.11 KB
- Download: application.bin

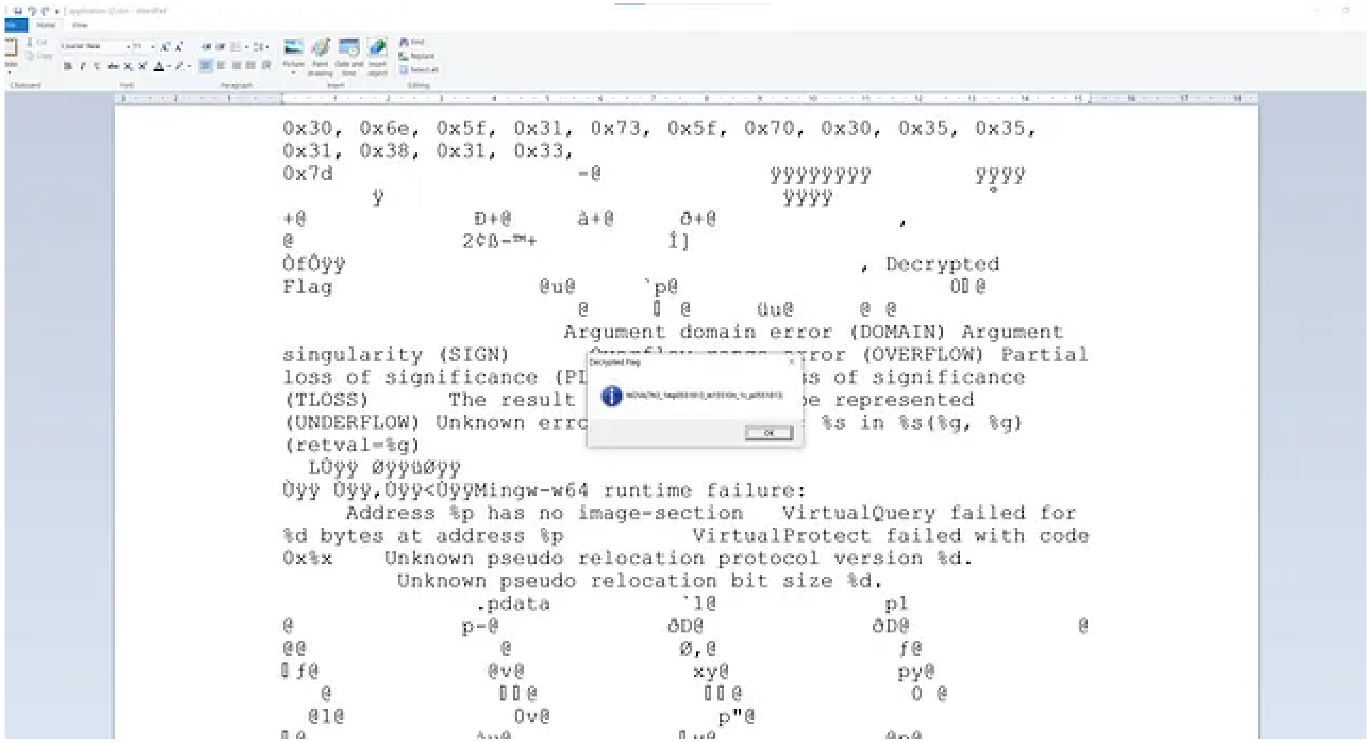
Hex Dump

```
         00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00  MZ......................
00000018 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @.......................
00000030 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd  ........................
00000048 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f  !..L.!This program canno
00000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a  t be run in DOS mode....
00000078 24 00 00 00 00 00 00 00 50 45 00 00 64 86 0f 00 12 00 fb 63 00 b8 00 00  $.......PE..d.......c...
00000090 d9 04 00 00 f0 00 27 00 0b 02 02 1e 00 1e 00 00 00 38 00 00 00 0a 00 00  ......'..........8......
000000A8 e0 14 00 00 00 10 00 00 00 00 40 00 00 00 00 00 00 10 00 00 00 02 00 00  ..........@.............
000000C0 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 70 01 00 00 04 00 00  .................p......
000000D8 5e c3 01 00 03 00 00 00 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00  ^.......................
000000F0 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00  ........................
```

decoded file

Now, it’s time to decode that content. Just use your favorite base64 decoder and you’ll get a file. And what’s in that file, you ask? An .exe file, of course!

Execute that bad boy on your Windows machine and BAM! You’ve got yourself a flag!



```
0x30, 0x6e, 0x5f, 0x31, 0x73, 0x5f, 0x70, 0x30, 0x35, 0x35,
0x31, 0x38, 0x31, 0x33,
0x7d                   -@              ÿÿÿÿÿÿÿÿ        ÿÿÿÿ
       ÿ                                ÿÿÿÿ
+@           Ð+@     à+@     ð+@                 ,
@           2¢ß-™+          Î]
ÒfÔÿÿ                                        , Decrypted
Flag                  @u@      `p@                    Ò@
                       @      @     Ùu@      @ @
                      Argument domain error (DOMAIN) Argument
singularity (SIGN)         ...rror (OVERFLOW) Partial
loss of significance (PL                  ss of significance
(TLOSS)      The result                  be represented
(UNDERFLOW) Unknown erro                 %s in %s(%g, %g)
(retval=%g)
  LÒÿÿ øÿÿùøÿÿ
Ùÿÿ Ùÿÿ,Ùÿÿ<ÙÿÿMingw-w64 runtime failure:
     Address %p has no image-section   VirtualQuery failed for
%d bytes at address %p          VirtualProtect failed with code
0x%x    Unknown pseudo relocation protocol version %d.
         Unknown pseudo relocation bit size %d.
               .pdata          `1@            pl
@             p-@            ðD@            ðD@            @
@@              @             Ø,@             f@
 f@             @v@            xy@             py@
   @              @            @              0 @
  @1@              Ov@             p"@
```

Our Flag...!!!

The flag is **NOVA{7h3_1mp0551813_m15510n_15_p0551813}.**

Phew! What an adventure! Who knew identifying a file hash could be so exciting?