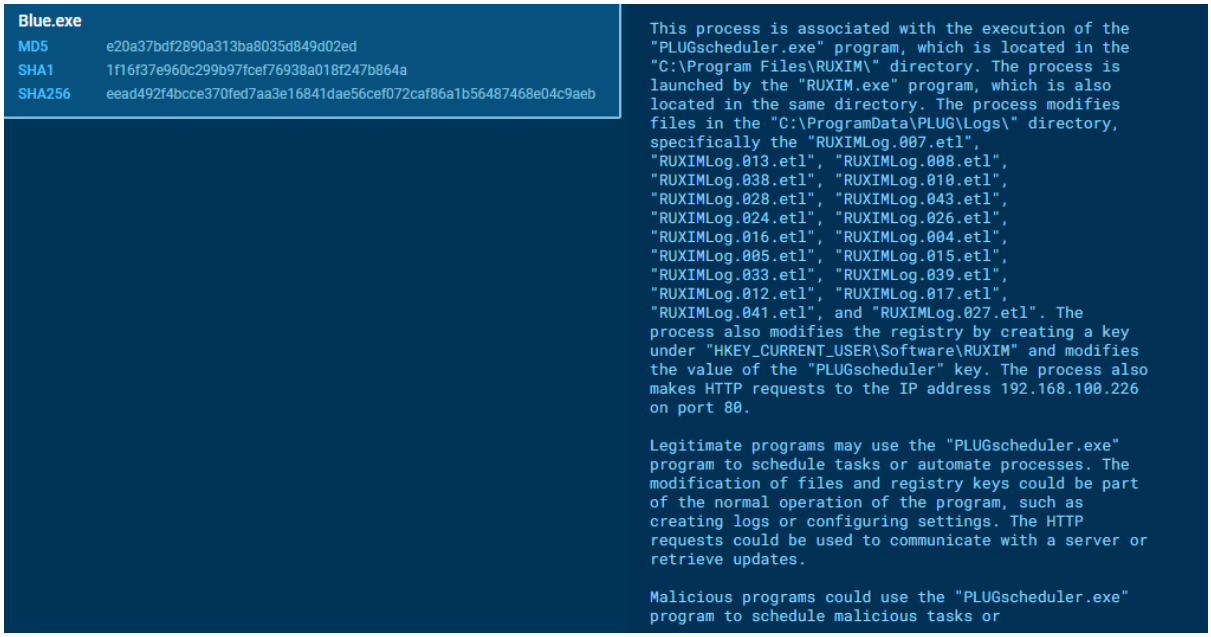
Malware – Blue

First of all, Im not good at dynamic analysis. So when there are malware challenge, I can only hope to decrypt whatever I saw in bunch of tools. Some of the tools im using is IDAPRO, any.run and Virus Total. This takes A LOT of my time as Im not good at web so im more focus on other things.

You see how many task I've run? Then I saw that any.run have a restart button. So there should be more than this. Like tripled.

All of the file that I can extract I gave to ChatGPT hoping there is flag plaintext. But nope



Any.run AI summary also doesn't yield anything useful.

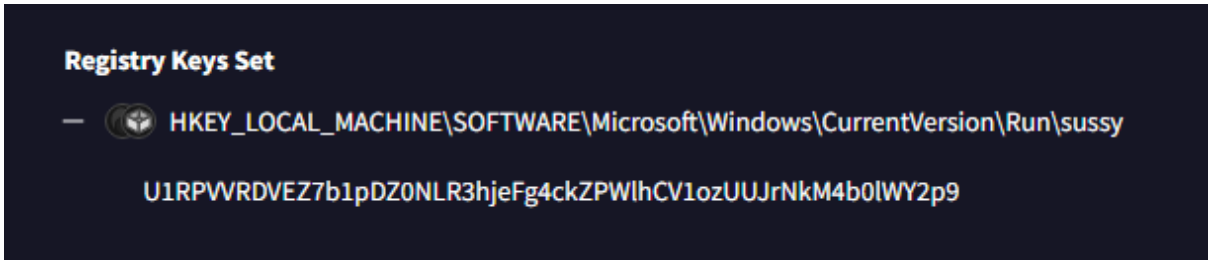
So for like 1 day and half, I cant get anything in any.run. or im too noob. Pls give me tips @John

I did use IDAPro. But the thing is, the malware is obfuscated. The only thing I know that unobfuscate is just UPX. So, I tried UPX -d and go to IDApro again. But it still says its obfuscated. I don't remember where it said that maybe chatgpt because in Chatgpt there is Malware Analysis malware, but I use it for one hour only and its useless. So, the string in IDApro is too many and I'm too noob at searching from thousands of no name functions.

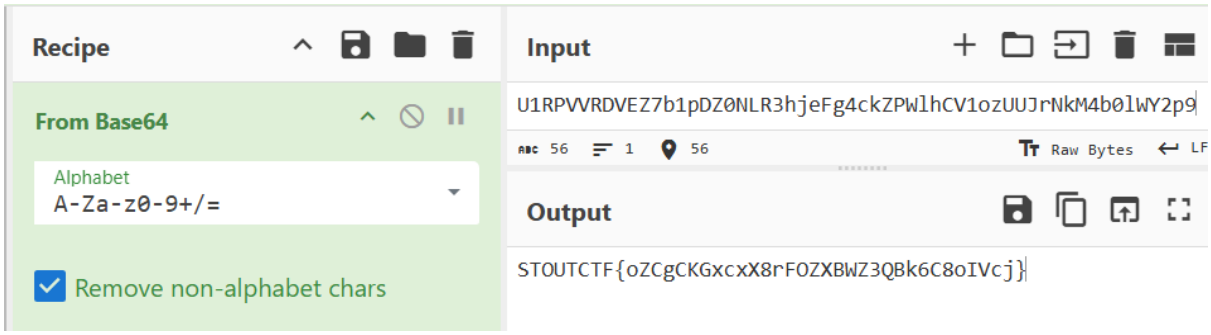
Then after I got substitute teacher's flag, and flag hoarding it (sorry h4rmony) I focused on malware again. I installed new VM and tried to run in it, but it kept crashing. You know how long I tried? Freaking 10 hours. But its okay, in the meantime, I do my writeup while installing and uninstalling the VM and submitting flags that Im hoarding. Then after finished doing my writeup and submitting flags (except the last web chall I cant get it).

THE BEST PART (malware part 2)

Same timestamp as submitting flag and doing writeup, and while trying to "failed dynamic" analysis of the malware, I export virustotal analysis and feed to chatgpt (expand all the report and screenshotting) multiple times I got something. When screenshotting behaviour tab, under Registry keys set there are base64 encoding that give flag OMG



ChatGPT decoded it but its gone. So here is the cyberchef screenshot



That’s all from me, just a noob guy using chatgpt if I don’t know anything about it.

Imma do the last web challenge now and I’ll update if I get it. Don’t know if I can cause the whole day im looking at the screen.

*update: I got it