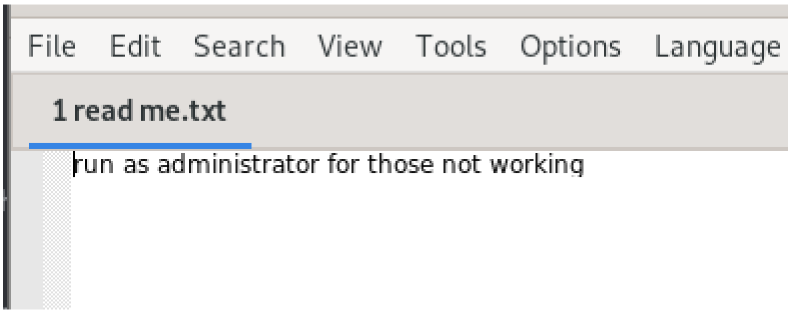
My Second Family.

> (I don't even have my first dude)

Now.



run as administrator for those not working

As soon as I saw this- I knew it was going to be good.

A'ight so after unzipping the .zip, we get 7 items.
5 DLL's,1 exe and *that* readme.txt file.

- game.dll
- msvcp140.dll
- quit.dll
- sqlit4.dll
- start.dll
- My Second Family Game Start.exe
- readme.txt

Now, I started with Ghidra on the exe to see what the actual makeup of the file was.
....
after strings. I like `strings`
Aaaand I was disappointed.

> Node.js `<nexe~sentinel>`

So-
I.
yeah. Not a cool C# virus I thought it would be.
Tho this time, unlike Takolya the obfuscator used was different.

> Read File1Js here.

...and we found another, Js file to uhh. Investigate (from that api.*/Inject.js), array index 73.
So this was a 2-stage malware? Also notice that they use webhooks to post the creds which- conveniently has their guildId that we can report to Discord.
So ig time for the second Js file to investigate (AND we didn't even touch the DLL's yet. This one's interesting.)

> Read File2Js here.

Uh. About the- dlls.
Strings show that every one of them just had a bunch of SQL statements and sqlite4 stored the creds (but Inject.js file never really used it soo...?)

This report is **incomplete** as I don't have time rn to go through the entire second Js file. I will do that sometimes later
`<inb4 never>`