

Forum:[Hack Forums](#)

Thread: [Malware Analysis Blog\(Formbook info stealer analysis\)](#)

decessum - May 5, 2024, 6:56 pm

Hi, I created a blog to write down some of my research and track my learning within the realm of malware analysis. If you guys wanna check it out that would be awesome, I am mainly going to try to post a new analysis every week. I am just getting into the world of malware analysis so if you see any errors or anything just hit me up with the email linked in the About section of the website, I am always looking for suggestions or etc.

I recently analyzed the Formbook malware and found some pretty cool stuff so let me know what ya think! spoiler I found emails all linked to this domain within the embedded executable:

myhydropowered(dot)com

Link to malware analysis blog main page: [cyber-forensics\(dot\)blog/](#)

Link to malware analysis blog formbook analysis:
[cyber-forensics\(dot\)blog/2024/05/06/formbook-analysis/](#)

Thanks.

Bastille - May 5, 2024, 10:21 pm

Wow nice work man ! Be sure that I'll check every malware analysis you do, feel free to share them on HF.

I'm not into malware analysis but I know few things, I mostly use VirusTotal and I'm not familiar yet with other tools (such as the ones you mentioned in the blog). Could be nice to make a thread with every useful tool and their purposes :)

Do you mind if I move your thread in the White Hat section ? I think it could fit better there

How did you learn malware analysis, self-taught ? school ?