

# Forum:[Hack Forums](#)

Thread: [Community Alert | KGB Crypter / Dictator Scamming](#)

**SIM-5486627** - August 8, 2024, 12:45 pm

Hello,

I would like to do a community alert about @Dictator  
And wdkiller.com (KGB Crypter) on the 1055\$ private plan.

1. The plan is clearly not private (all customers that purchase that plan will use the same stub, the same shellcode loader...)
2. He doesn't signs the EXE file and it is not AIO since he's doing DLL hijacking
3. He re-use same stub for everyone
4. Stub being "FUD" for 20days is already 40/70 after crypting (because he's using that same stub and exec method for each customers)
5. Crypt isn't unique (since he's doing DLL hijacking, he has to put some DLL to make the shellcode exec, he keep the same DLL everytime for every crypts on every users, that leads that some retards did a VT check and made the shellcode loader detected scantime) - Also on virustotal i could see other .zip file with the dll shellcode loader that's how i could discover it was shared & shitty (so the DLL shellcode loader was already detected before my crypt)
6. "Stubs are handmade coded for each request, exclusive service. Takes 12 hours to the administrator work on your stub." - He made instant deliver so it's kinda fake
7. "You can request custom features like: startup, rootkit, persistence" - I never saw these features, only startup and fake error
8. "With this you can bypass Chrome, Edge, Firefox, Google Drive, and all kind of "trusted" warnings." - Obviously detected by chrome since 40/70 DLL inside the zip file

+ He's not answering for a week...

Video with all proofs and where i showcase how bullshit it is (it's more easy to understand than my shitty text): <https://youtu.be/VJdeowXzK3Y>

**Tentco** - August 9, 2024, 2:10 am

One thing I'm confused about that in 1k package he claims to personally sign your payload crypt with an EV Cert but I saw dll-sideload in your case.

**SIM-5486627** - August 9, 2024, 6:18 am

(Aug 9, 2024 02:10 AM)Tentco Wrote: [\[CITE\]](#) One thing I'm confused about that in 1k package he claims to personally sign your payload crypt with an EV Cert but I saw dll-sideload in your case.

+