

Forum:[Hack Forums](#)

Thread: [Why is a public stub bad?](#)

·CHESTER· - June 8, 2025, 9:38 am

There are sellers who sell public stubs or shared stubs. Is this bad because multiple people are using the same file, so if one gets caught, everyone else goes down with them?

Why not inject a bunch of random code and do random control flow (e.g. if statement vs for loop) for each stub randomly? Or are modern AI-driven AV engines too good at detecting this such that it wouldn't make any difference?

CryptDaddi - June 8, 2025, 9:47 am

(Jun 8, 2025 09:38 AM)ChesterMolestor Wrote: [\[CITE\]](#) There are sellers who sell public stubs or shared stubs. Is this bad because multiple people are using the same file, so if one gets caught, everyone else goes down with them?

Why not inject a bunch of random code and do random control flow (e.g. if statement vs for loop) for each stub randomly? Or are modern AI-driven AV engines too good at detecting this such that it wouldn't make any difference?

AV's often use signature based detection. If a stub becomes public or is used by many people, AVs can easily extract a static pattern from it and flag all future uses.

Modern AI/ML based AVs go beyond signatures, so simple random code or random control flow wont help.

·CHESTER· - June 8, 2025, 9:49 am

(Jun 8, 2025 09:47 AM)CryptDaddi Wrote: [\[CITE\]](#) AV's often use signature based detection. If a stub becomes public or is used by many people, AVs can easily extract a static pattern from it and flag all future uses.

Modern AI/ML based AVs go beyond signatures, so simple random code or random control flow wont help.

What's to stop Microsoft from buying every public stub subscription (most are \$60 to \$100) for several months? So it would be nothing for them to buy and instantly add it to their signature library.

CryptDaddi - June 8, 2025, 9:52 am

(Jun 8, 2025 09:49 AM)ChesterMolestor Wrote: [\[CITE\]](#) What's to stop Microsoft from buying every public stub subscription (most are \$60 to \$100) for several months? So it would be nothing for them to buy and instantly add it to their signature library.

Yeah, they probably do that already. Buying public stubs is cheap for them, and once they have it, they can add signatures fast. That's why public or shared stubs get burned quickly.

DramaKing - June 8, 2025, 3:21 pm

(Jun 8, 2025 09:49 AM)ChesterMolestor Wrote: [\[CITE\]](#) What's to stop Microsoft from buying every public stub subscription (most are \$60 to \$100) for several months? So it would be nothing for them to buy and instantly add it to their signature library.

Psh. Infiltrate marketplaces such as this or Telegram channels and buy malware for analysis? WD will submit every non-whitelisted, unsigned executable to Microsoft for analysis.

Also, you don't see anyone advertising their service as featuring public stubs. Some sellers might even advertise private stubs but actually sell public ones.

•CHESTER• - June 8, 2025, 8:27 pm

(Jun 8, 2025 03:21 PM)DramaKing Wrote: [\[CITE\]](#) Also, you don't see anyone advertising their service as featuring public stubs. Some sellers might even advertise private stubs but actually sell public ones.

I don't know about that. Lots of sellers say their stub is public or shared.

•CHESTER• - June 13, 2025, 10:45 am

(Jun 8, 2025 10:10 AM)MarlboroMan Wrote: [\[CITE\]](#) This is the most valuable answer. This is also why a lot of services fail.

But aren't you also selling public stubs?

•CHESTER• - June 14, 2025, 7:47 am

(Jun 13, 2025 10:49 AM)MarlboroMan Wrote: [\[CITE\]](#) I don't sell stubs.

Doesn't the crypter you are selling use a public or shared stub?

Voidlight - June 14, 2025, 10:47 am

(Jun 14, 2025 07:53 AM)MarlboroMan Wrote: [\[CITE\]](#) It doesn't use A stub, period.

can you elaborate on how your crypter does not use a builder/stub architecture?