

Forum:[Hack Forums](#)

Thread: [Bypass AntiVirus](#)

mnt007 - August 3, 2023, 7:44 pm

I made small troijan using ProcessHollowing Technique.
but it had detected AntiVirus - Defender.
I think there is a problem in Process Hollowing.
Anyone know a good way to bypass windows defender?

DramaKing - August 3, 2023, 9:04 pm

(Aug 3, 2023 07:44 PM)mnt007 Wrote: [\[CITE\]](#) I made small troijan using Process Hollowing Technique.

but it had detected AntiVirus - Defender.
I think there is a problem in Process Hollowing.
Anyone know a good way to bypass windows defender?
The problem is that you injected malware into the process. If you didn't create it yourself, its signature is likely know to AV. You should disable Defender, then download the Trojan.

mnt007 - August 4, 2023, 12:56 am

(Aug 3, 2023 09:04 PM)DramaKing Wrote: [\[CITE\]](#) The problem is that you injected malware into the process. If you didn't create it yourself, its signature is likely know to AV. You should disable Defender, then download the Trojan.

I made it myself. I want to know about AV's detection techniques.
My troijan wasn't detected by Defender with pattern.
I obfuscated it's code for bypassing AV, but ...

DramaKing - August 4, 2023, 9:08 am

(Aug 4, 2023 12:56 AM)mnt007 Wrote: [\[CITE\]](#) I made it myself. I want to know about AV's detection techniques.

My troijan wasn't detected by Defender with pattern.
I obfuscated it's code for bypassing AV, but ...
Okay, then Defender is catching it with behavioral/heuristic detection. You need to patch AMSI or, as I said, disable Defender / add an exception. The standard version has no defense shields like other AV. You just need to be an administrator.