

Forum: [Hack Forums](#)

Thread: [Question about runtime encryption](#)

HighFive - October 20, 2019, 1:24 pm

I am trying to learn how the whole process of crypting works and code a crypter. So by far my crypter is working only scantime. I have a stub that contains encrypted virus. It is not detected by my anti-virus, but when I run it in sanbox it gets instant detected and deleted. Stub is loading resource file(encrypted virus) then decrypt it and run it in memory. For what I have read, I thought that when I run decrypted exe in memory it should prevent from detection on executing. I am testing it with some darkcomet server and anti-virus detects it exactly as DarkComet malware. So it is not like av is reconizing some type of malware/crypter behavior in stub but instantly when I trying load decrypted exe to memory, it gets detected.

My question is, am I missing any other methods of encryption/manipulation? Or maybe I should just try finding different method of loading file to memory?

misterfugazi - October 20, 2019, 2:30 pm

Runtime encryption does not exist. It is a myth.

I recommending learning how to work with payloads that evade AV and opening meterpreter shells and running code remotely.

smutnagab - October 20, 2019, 2:43 pm

The issue at hand is dynamic memory scanning which most traditional AV products will include as part of their real-time protection.

You have a few options:

1. Change the code so it is not picked up by hash checksum/generic signature scanning.
2. A layer of emulation which can circumvent the memory scanner which is getting on your nerves.
3. Exploit AV products explicitly.