

Forum:[Hack Forums](#)

Thread: [Who can tell me how anti virus software works?](#)

boruto6677 - August 18, 2020, 8:05 am

I really want to know how anti-virus software works, I have looked at some information on wikipedia but I think it is not very complete. Can someone tell me how anti-virus software works? And how does stub and crypter work so that the antivirus can't detect the payload?

devlightz - August 18, 2020, 8:09 am

I'm not cyber security guy but I think the basic idea is an Anti virus decompiles and scans the code of files and applications and looks for known malicious code. A crypter/obfuscator takes your code and makes it almost unreadable so that these malicious code blocks arent recognizable by the anti virus software. Someone please correct me if I'm wrong but I'm pretty sure this is the basic idea of both types of software.

The Amazing Sinner - August 18, 2020, 8:11 am

Signature-based detection detects by comparing a virus signature (a binary pattern of known viruses) against files being scanned. Heuristic-based detection detects behavior in and patterns of code that indicates a virus may be present.

If you need any help encrypting/recoding a stub let me know.
Shoot me a PM.

boruto6677 - August 18, 2020, 5:46 pm

(Aug 18, 2020 08:09 AM)devlightz Wrote: [\[CITE\]](#) I'm not cyber security guy but I think the basic idea is an Anti virus decompiles and scans the code of files and applications and looks for known malicious code. A crypter/obfuscator takes your code and makes it almost unreadable so that these malicious code blocks arent recognizable by the anti virus software. Someone please correct me if I'm wrong but I'm pretty sure this is the basic idea of both types of software.

(Aug 18, 2020 08:11 AM)TheSinner Wrote: [\[CITE\]](#) Signature-based detection detects by comparing a virus signature (a binary pattern of known viruses) against files being scanned. Heuristic-based detection detects behavior in and patterns of code that indicates a virus may be present.

If you need any help encrypting/recoding a stub let me know.
Shoot me a PM.
Thanks!!