

Introduction To Payload Encryption

Payload Encryption

Payload encryption in malware is a technique used by attackers to hide the malicious code contained in a malicious file. Attackers use various encryption algorithms to conceal the malicious code, making it more difficult for security solutions to detect the malicious activity of the file. Encryption also helps the malware to remain hidden and undetected on the user's system for longer periods. Encrypting parts of the malware will almost always be necessary against modern security solutions.

Encryption Pros and Cons

Encryption can help evade signature-based detection when using signed code and payloads, but it may not be effective against other forms of detection, such as runtime and heuristic analysis.

It is important to note that the more data that's encrypted within a file, the higher its entropy. Having a file with a high entropy score can cause security solutions to flag the file or at the very least consider it suspicious and place additional scrutiny on it. Decreasing a file's entropy will be discussed in future modules.

Encryption Types

The upcoming modules will go through three of the most widely used encryption algorithms in malware development:

- XOR
- AES
- RC4

[Previous](#)[Modules](#)[Undo](#)[Next](#)