Stealth

Malek Mohammad

Information Security Consultant

https://github.com/malek-mohammad
www.linkedin.com/in/malekmohammad

Detection

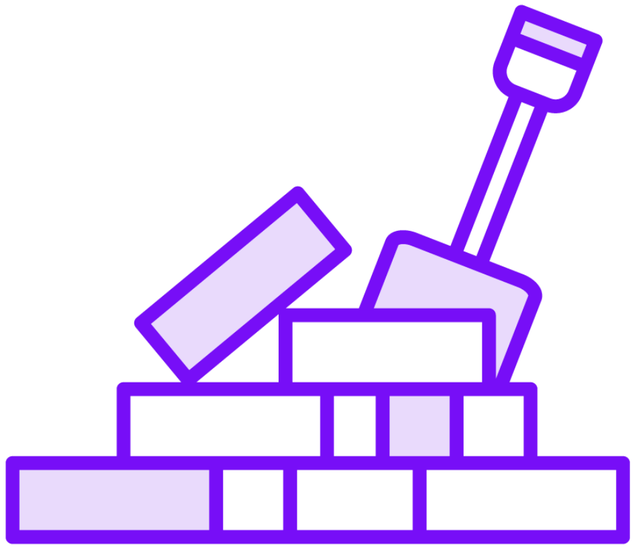
Risk of being detected

Detection by security applications

Detection by users

Techniques for stealth

Obfuscation



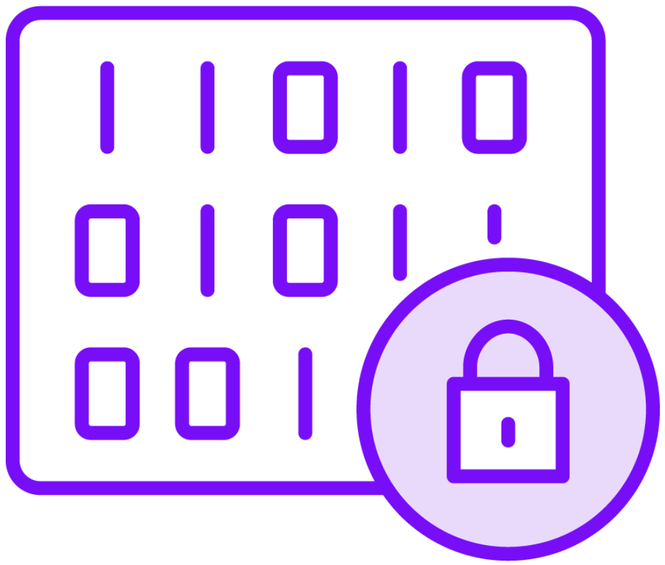
Rename variables

Rename functions

Add unneeded code

Use complex structures

Other Techniques



Use base64 encoding

Random characters

Use eval to execute

Encryption with a key

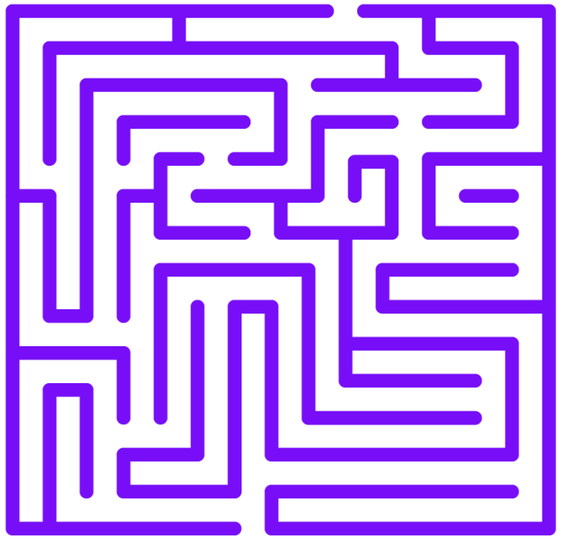
Combine techniques

Stealth by Encoding

Encode to hide

Turns data into ASCII

Stealth by Obfuscation



Difficult to understand

Names with no meaning

Unnecessary code

Complex logic

Stealth by Encryption

Encryption protects

No access without a key

Use encryption tools

Encrypt parts of the script

Closure

Sensed the strength of bash

Practice is key

Real world scenarios

Check the communities

Thanks for attending