

Evading Detection in Memory



William Hardy
Security Engineer



Module Overview

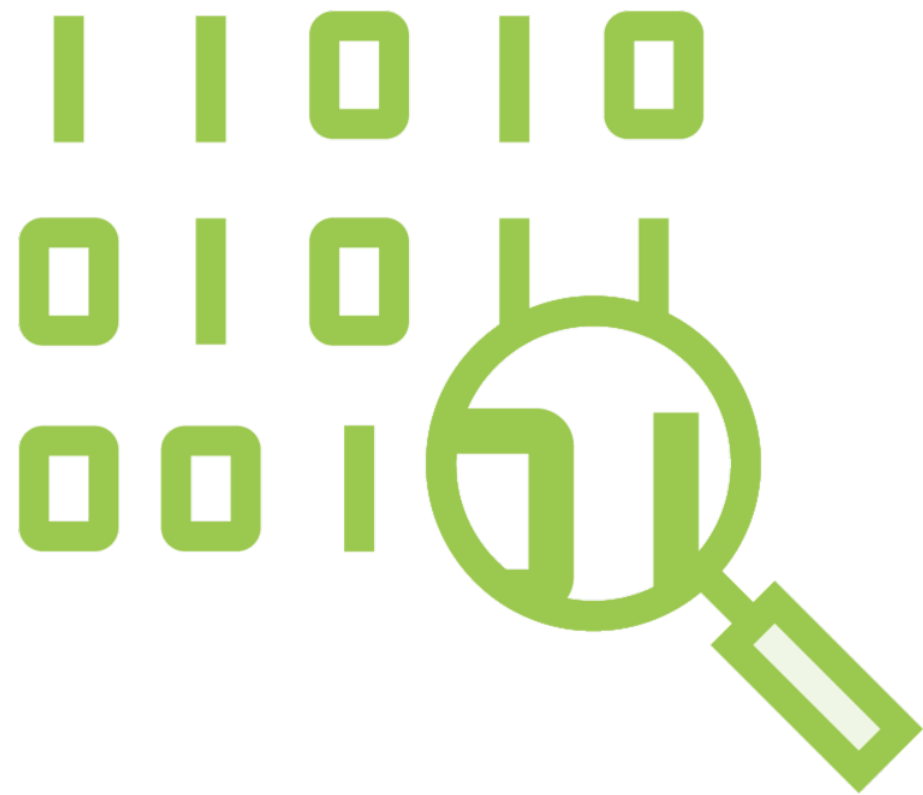


Evading in-memory signatures

Demo



Evading in-memory Signatures



Signatures are also used in memory to detect code after it has been decoded or decrypted



We can evade them by modifying the code and artifacts that reside in memory

Evading in-memory Signatures



Identifying good signature candidates

Automating the code refactoring

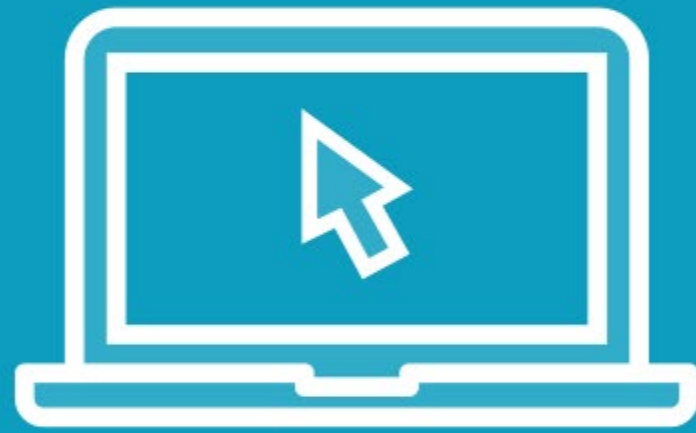
Manually performing the code refactoring

Using shared forks of the project on GitHub

Reverse engineering the antivirus



Demo



Modifying the Payload
Modifying Extensions

