Técnicas de inyección de procesos

La técnica de inyección de procesos consiste en inyectar trozos de códigos en procesos que están en ejecución.

Dicha técnica es utilizada por el malware, se oculta la ejecución de código y no es detectada por los antivirus porque se inyecta código en procesos conocidos.

Algunos casos en los que se puede inyectar, cuando un proceso llama a funciones de un API, cuando un procesos llama a una DLL, cuando un proceso carga más memoria, etc.

Algunas pruebas de concepto

Inyección de mapeo (la inyección de mapeo es una técnica de inyección de proceso que evita el uso de syscall monitorizado común VirtualAllocEx y WriteProcessMemory)

- https://github.com/antonioCoco/Mapping-Injection

Cargar en memoria y ejecutar un payload de ejecución de comandos arbitrarios en PowerShell

- https://www.jesusninoc.com/2017/02/16/cargar-en-memoria-y-ejecutar-un-payload-de-ejecucion-de-comandos-arbitrarios-en-powershell/

Analizar con Cheat Engine un payload de ejecución de comandos arbitrarios para ejecutar PowerShell

- https://www.jesusninoc.com/2017/03/20/analizar-con-cheat-engine-un-payload-de-ejecucion-de-comandos-arbitrarios-para-ejecutar-powershell/

Utilizar el payload de ejecución de comandos arbitrarios para ejecutar PowerShell

- https://www.jesusninoc.com/2017/02/11/utilizar-el-payload-de-ejecucion-de-comandos-arbitrarios-para-ejecutar-powershell/

Analizar un payload de ejecución de comandos arbitrarios para ejecutar PowerShell

- https://www.jesusninoc.com/2017/02/12/analizar-un-payload-de-ejecucion-de-comandos-arbitrarios-para-ejecutar-powershell/

Utilizar una DLL compilada con Microsoft Visual C# en PowerShell

- https://www.jesusninoc.com/04/17/utilizar-una-dll-compilada-con-microsoft-visual-c-en-powershell/