

Table of Contents

Table of Contents.....	2
Introduction.....	3
MapMemoryHandlers.....	4
Structure Components.....	6
Filter for File Handle.....	9
NtDuplicateObject:.....	11
NtQueryObject:.....	11
Filter Register Keys.....	15
Parameters.....	18
Steps in FindRegistryKeyHandle.....	18
FilterProcesses.....	19
Filter User Process Tokens.....	27
Filter Threads.....	28
RWX Finder.....	35
Process Injection with random RWX Memory Spaces.....	38
This code are doing the following things:.....	41
Free Loader Injector.....	42
Proof of Concept.....	52
Exercise.....	53
Conclusions.....	54