

Table of Contents

Table of Contents.....	2
Introduction.....	6
How Security Products Work.....	8
Import Address Table Obfuscation.....	10
Red Team (Offensive) Use of the IAT.....	10
Blue Team (Defensive) Use of the IAT.....	10
Windows Defender Killer.....	15
Unhook Antivirus Hooks with an NTDLL Fresh Copy.....	21
1. Function Hooks.....	21
2. Behavior Analysis.....	22
3. Decision Making.....	22
ETW Patcher.....	36
Patching AV Hooks.....	41
Network Evasion.....	46
AntiDebugging Evasion.....	55
Exercise.....	61
Conclusions.....	63