

SKRÓCONY SPIS TREŚCI

Przedmowa Rodriga Rubia Branco	xxi
Podziękowania	xxv
Skróty	xxvii
Wprowadzenie	xxxi
Część I: Rootkity	1
Rozdział 1: Czym jest rootkit: studium przypadku TDL3	3
Rozdział 2: Rootkit Festi: najbardziej zaawansowany bot spamowy i DDoS	15
Rozdział 3: Obserwowanie infekcji rootkitami	41
Część II: Bootkity	55
Rozdział 4: Ewolucja bootkitu	57
Rozdział 5: Podstawy procesu rozruchu systemu operacyjnego	65
Rozdział 6: Zabezpieczenia procesu rozruchu	79
Rozdział 7: Techniki infekcji bootkitów	95
Rozdział 8: Statyczna analiza bootkitu przy użyciu IDA Pro	107
Rozdział 9: Dynamiczna analiza bootkitu: emulacja i wirtualizacja	129
Rozdział 10: Ewolucja technik infekowania MBR i VBR: Olmasco	149
Rozdział 11: Bootkity IPL: Rovix i Carberp	165
Rozdział 12: Gapz: zaawansowana infekcja VBR	197
Rozdział 13: Rozwój ransomware MBR	231
Rozdział 14: Rozruch UEFI a proces rozruchowy MBR/VBR	259
Rozdział 15: Współczesne bootkity UEFI	283
Rozdział 16: Podatności oprogramowania układowego UEFI	317