

SPIS TREŚCI

O autorach	XXI
Przedmowa	XXIII
Podziękowania	XXVII
Wprowadzenie	XXIX
Rozdział 0 Elementarz analizy malware	1
CZĘŚĆ 1 ANALIZA PODSTAWOWA	7
Rozdział 1 Podstawowe techniki statyczne.	9
Rozdział 2 Analiza malware na maszynach wirtualnych.	29
Rozdział 3 Podstawowa analiza dynamiczna.	39
CZĘŚĆ 2 ZAAWANSOWANA ANALIZA STATYCZNA	63
Rozdział 4 Kurs błyskawiczny asemblera x86	65
Rozdział 5 IDA Pro	85
Rozdział 6 Rozpoznawanie w asemblerze konstrukcji języka C	107
Rozdział 7 Analizowanie malware w systemie Windows	133
CZĘŚĆ 3 ZAAWANSOWANA ANALIZA DYNAMICZNA	163
Rozdział 8 Debugowanie	165
Rozdział 9 OllyDbg	177
Rozdział 10 Debugowanie jądra za pomocą WinDbg	201
CZĘŚĆ 4 FUNKCJONALNOŚCI MALWARE	225
Rozdział 11 Zachowanie malware	227
Rozdział 12 Ukryte uruchamianie malware	249
Rozdział 13 Szyfrowanie danych	263
Rozdział 14 Sygnatury sieciowe dotyczące malware	291

CZĘŚĆ 5	ZAPOBIEGANIE INŻYNIERII ODWROTNEJ	321
Rozdział 15	Zapobieganie deasemblacji	323
Rozdział 16	Zapobieganie debugowaniu	347
Rozdział 17	Techniki wykrywania maszyny wirtualnej	365
Rozdział 18	Pakowanie i rozpakowywanie	379
CZĘŚĆ 6	TEMATY SPECJALNE	399
Rozdział 19	Analizowanie shellcode	401
Rozdział 20	Analizowanie C++	421
Rozdział 21	64-bitowe malware	435
DODATEK A	WAŻNE FUNKCJE SYSTEMU WINDOWS	445
DODATEK B	NARZĘDZIA DO ANALIZY MALWARE	457
DODATEK C	ROZWIĄZANIA ĆWICZEŃ LABORATORYJNYCH	469
INDEKS		723