

SZCZEGÓŁOWY SPIS TREŚCI

O AUTORACH	XXI
O recenzencie technicznym	XXII
O współpracujących autorach.	XXII
PRZEDMOWA	XXIII
PODZIĘKOWANIA	XXVII
Indywidualne podziękowania	XXVII
WPROWADZENIE	XXIX
Czym jest analiza malware?	XXX
Wymagania wstępne	XXX
Nauka w praktyce	XXXI
Co znajduje się w książce?	XXXII
0	
ELEMENTARZ ANALIZY MALWARE	1
Cel analizy malware	1
Techniki analizy złośliwego oprogramowania.	2
Podstawowa analiza statyczna	2
Podstawowa analiza dynamiczna.	2
Zaawansowana analiza statyczna	3
Zaawansowana analiza dynamiczna.	3
Rodzaje złośliwego oprogramowania	3
Ogólne zasady analizy malware.	5
CZĘŚĆ 1 ANALIZA PODSTAWOWA	7
1	
PODSTAWOWE TECHNIKI STATYCZNE.	9
Skanowanie antywirusowe – przydatny pierwszy krok	10
Haszowanie – odcisk palca malware	10
Znajdowanie łańcuchów	11
Pakowanie i obfuskacja przez malware	13
Spakowane pliki	13
Wykrywanie spakowanych programów za pomocą PEiD.	14

Format plików Portable Executable	15
Dołączane biblioteki i funkcje	15
Dołączanie statyczne, w czasie wykonywania i dynamiczne	15
Eksplorowanie funkcji dołączanych dynamicznie za pomocą Dependency Walker	16
Importowane funkcje	18
Eksportowane funkcje	18
Analiza statyczna w praktyce	18
PotentialKeylogger.exe – rozpakowany plik wykonywalny	19
PackedProgram.exe – ślepy zaułek	21
Nagłówki i sekcje plików PE	21
Badanie plików PE za pomocą PEview	22
Podgląd sekcji zasobów za pomocą Resource Hackera	25
Korzystanie z innych narzędzi dla plików PE	26
Podsumowanie nagłówka Pe	26
Podsumowanie	26
2	
ANALIZA MALWARE NA MASZYNACH WIRTUALNYCH	29
Struktura maszyny wirtualnej	30
Tworzenie maszyny do analizy malware	31
Konfigurowanie VMware	31
Korzystanie z maszyny do analizy malware	34
Podłączanie malware do internetu	34
Podłączanie i odłączanie urządzeń peryferyjnych	34
Wykonywanie migawek	35
Przesyłanie plików z maszyny wirtualnej	36
Ryzyka związane z wykorzystaniem VMware do analizy malware	36
Nagrywanie/odtworzenie – komputer na biegu wstecznym	37
Podsumowanie	37
3	
PODSTAWOWA ANALIZA DYNAMICZNA	39
Piaskownice – podejście tanie i szybkie	40
Użycie piaskownicy dla malware	40
Wady piaskownic	41
Uruchamianie malware	42
Monitorowanie za pomocą Process Monitora	43
Interfejs narzędzia procmon	44
Filtrowanie w procmon	45
Wyświetlanie procesów za pomocą Process Explorera	47
Interfejs Process Explorera	47
Korzystanie z opcji weryfikacji	48
Porównywanie łańcuchów	49
Korzystanie z Dependency Walker	49
Analiza złośliwych dokumentów	50
Porównywanie migawek rejestru za pomocą Regshota	50
Udawanie sieci	51
Korzystanie z ApateDNS	51

Monitorowanie za pomocą Netcat	52
Analizowanie pakietów za pomocą Wiresharka	53
Korzystanie z INetSim	55
Podstawowe narzędzia analizy dynamicznej w praktyce	56
Podsumowanie	60
CZĘŚĆ 2 ZAAWANSOWANA ANALIZA STATYCZNA	63
4	
KURS BŁYSKAWICZNY ASEMBLERA X86	65
Poziomy abstrakcji	66
Inżynieria odwrotna	67
Architektura x86	68
Pamięć główna	68
Instrukcje	69
Kody operacji i kolejność bajtów	70
Operandy	70
Rejestry	70
Proste instrukcje	73
Stos	76
Instrukcje warunkowe	79
Rozgałęzienia	79
Instrukcje rep	80
Metoda main w C i offsety	82
Więcej informacji – podręczniki architektury Intel x86	84
Podsumowanie	84
5	
IDA PRO	85
Ładowanie pliku wykonywalnego	86
Interfejs IDA Pro.	87
Tryby okna deasemblacji	87
Okna przydatne do analizy.	89
Powrót do widoku domyślnego.	90
Nawigacja w IDA Pro.	90
Korzystanie z odsyłaczy.	93
Odsyłacze w kodzie	93
Odsyłacze do danych	94
Analizowanie funkcji.	94
Korzystanie z grafów.	96
Dostosowywanie zdeasembrowanego kodu	97
Zmianianie nazw lokalizacji	97
Komentarze	98
Formatowanie operandów.	99
Używanie nazwanych stałych	99
Przeddefiniowywanie kodu i danych	101
Rozszerzanie IDA za pomocą wtyczek.	102
Korzystanie ze skryptów IDC.	102

Korzystanie z IDAPython	103
Korzystanie z komercyjnych wtyczek	104
Podsumowanie	104

6

ROZPOZNAWANIE W ASEMLERZE KONSTRUKCJI JĘZYKA C 107

Zmienne globalne a lokalne	108
Deasemblacja operacji arytmetycznych	110
Rozpoznawanie instrukcji if	111
Graficzna analiza funkcji za pomocą IDA Pro.	112
Rozpoznawanie zagnieżdżonych instrukcji if	112
Rozpoznawanie pętli	114
Wykrywanie pętli for.	114
Wykrywanie pętli while	116
Konwencje wywołań funkcji	117
cdecl.	118
stdcall	118
fastcall.	118
Odkładanie vs. kopiowanie.	118
Analizowanie instrukcji switch	120
Styl if.	120
Deasemblacja tablic	124
Identyfikowanie struktur	126
Analizowanie odniesień na liście powiązanej	129
Podsumowanie	131

7

ANALIZOWANIE MALWARE W SYSTEMIE WINDOWS. 133

Windows API.	134
Typy i notacja węgierska	134
Uchwyty	135
Funkcje systemu plików.	135
Pliki specjalne	136
Rejestr systemu Windows	137
Klucze główne rejestru	138
Regedit	138
Programy uruchamiane automatycznie.	138
Typowe funkcje dotyczące rejestru	139
Analiza kodu rejestru w praktyce.	140
Tworzenie skryptów dotyczących rejestru przy użyciu plików .reg.	141
Sieciowe API.	141
Gniazda kompatybilne z BSD	141
Sieć – strona klienta i serwera	142
WinINet API	143
Śledzenie działającego malware	143
Biblioteki DLL	143
Procesy	145
Wątki	147

Koordynacja międzyprocesowa z użyciem muteksów	149
Usługi	150
Component Object Model	152
Wyjątki – gdy coś pójdzie nie tak	155
Tryb użytkownika a tryb jądra	156
Native API	157
Podsumowanie	159

CZĘŚĆ 3 ZAAWANSOWANA ANALIZA DYNAMICZNA 163

8 **DEBUGOWANIE** 165

Debugery kodu źródłowego i debugery asemblera	166
Debugowanie w trybie jądra i w trybie użytkownika	166
Korzystanie z debuggera	167
Praca krokowa	167
Step-over vs. step-into	168
Wstrzymywanie wykonywania za pomocą punktów przerwania	169
Wyjątki	174
Wyjątki pierwszej i drugiej szansy	174
Typowe wyjątki	174
Modyfikowanie wykonania za pomocą debuggera	175
Modyfikowanie wykonywania programu w praktyce	175
Podsumowanie	176

9 **OLLYDBG** 177

Ładowanie malware	178
Otwieranie pliku wykonywalnego	178
Dołączanie do uruchomionego procesu	179
Interfejs OllyDbg	179
Mapa pamięci	180
Rebasing	181
Wyświetlanie wątków i stosów	183
Wykonywanie kodu	184
Punkty przerwania	185
Programowe punkty przerwania	185
Warunkowe punkty przerwania	186
Sprzętowe punkty przerwania	188
Pamięciowe punkty przerwania	188
Ładowanie plików DLL	188
Śledzenie	190
Standardowa historia śledzenia	190
Stos wywołań	190
Śledzenie wykonania	190
Śledzenie w Poison Ivy	191
Obsługa wyjątków	192
Poprawki w kodzie	192

Analizowanie shellcode	194
Narzędzia pomocnicze	194
Wtyczki	195
OllyDump	195
Hide Debugger	196
Command Line	196
Bookmarks	197
Debugowanie z użyciem skryptów	197
Podsumowanie	198

10

DEBUGOWANIE JĄDRA ZA POMOCĄ WINDBG	201
Sterowniki i kod w jądrze	201
Konfigurowanie debugowania jądra	203
Korzystanie z WinDbg	206
Odczytywanie pamięci	206
Korzystanie z operatorów arytmetycznych	206
Ustawianie punktów przerwania	207
Lista modułów	207
Microsoftowe symbole	208
Wyszukiwanie symboli	208
Wyświetlanie informacji o strukturze	209
Konfigurowanie windowsowych symboli	210
Debugowanie jądra w praktyce	211
Spojrzenie na kod w przestrzeni użytkownika	211
Spojrzenie na kod w trybie jądra	212
Znajdowanie obiektów sterowników	215
Rootkity	217
Analiza rootkitów w praktyce	218
Przerwania	221
Ładowanie sterowników	222
Problemy z jądrem w Windows Vista, Windows 7 i w wersjach x64	222
Podsumowanie	223

CZĘŚĆ 4 FUNKCJONALNOŚCI MALWARE 225

11

ZACHOWANIE MALWARE	227
Downloaderzy i launchery	227
Backdoory	228
Połączenie zwrotne	228
Narzędzia administracji zdalnej	229
Botnety	230
Porównanie RAT i botnetów	230
Złodzieje danych uwierzytelniających	230
Przechwytywanie poprzez GINA	231
Zrzucanie skrótów	232
Rejestrowanie naciśnięć klawiszy	234

Mechanizmy trwałości	237
Rejestr systemu Windows	237
Systemowe pliki binarne z wprowadzonym trojanem.	239
Przejmowanie kolejności ładowania bibliotek DLL.	240
Eskalacja uprawnień	241
Użycie SeDebugPrivilege.	242
Tuszując swoje ślady – rootkity w trybie użytkownika.	243
IAT hooking	244
Inline hooking.	244
Podsumowanie	246
12	
UKRYTE URUCHAMIANIE MALWARE.	249
Launchery	249
Iniekcja do procesu	250
Iniekcja DLL	250
Bezpośrednia iniekcja	253
Podmiana procesu	253
Iniekcja hooków	255
Hooki lokalne i zdalne.	256
Keyloggery korzystające z hooków	256
Użycie SetWindowsHookEx	256
Wybieranie za cel ataku określonego wątku.	257
Detours	258
Iniekcja APC	258
Iniekcja APC z przestrzeni użytkownika.	259
Iniekcja APC z przestrzeni jądra	260
Podsumowanie	261
13	
SZYFROWANIE DANYCH	263
Cel analizy algorytmów szyfrowania.	263
Proste szyfrowanie	264
Szyfr Cezara	264
XOR	264
Inne proste metody szyfrowania	270
Base64.	270
Typowe algorytmy kryptograficzne	274
Rozpoznawanie łańcuchów i importów.	275
Wyszukiwanie stałych kryptograficznych.	275
Wyszukiwanie treści o wysokiej entropii	277
Niestandardowe szyfrowanie	279
Identyfikowanie niestandardowego szyfrowania.	279
Zalety niestandardowego szyfrowania dla atakującego	281
Deszyfrowanie	282
Samodeszyfracja	282
Ręczne tworzenie funkcji deszyfrujących.	282
Użycie instrumentacji do generycznego deszyfrowania	284
Podsumowanie	287

14		
SYGNATURY SIECIOWE DOTYCZĄCE MALWARE		291
Przeciwdziałania dotyczące sieci		291
Obserwacja złośliwego oprogramowania w jego naturalnym środowisku		292
Wskaźniki szkodliwej aktywności		293
OPSEC = Operations security		293
Bezpieczne, online'owe badanie atakującego		294
Taktyki pośrednie		294
Uzyskiwanie adresu IP i informacji o domenie		294
Przeciwdziałania oparte na zawartości ruchu sieciowego		296
Wykrywanie włamań za pomocą Snorta		296
Głębsze spojrzenie		298
Łączenie technik analizy dynamicznej i statycznej		301
Niebezpieczeństwo nadmiernej analizy		302
Ukrywanie się przed wzrokiem		302
Zrozumienie otaczającego kodu		306
Znalezienie kodu odpowiedzialnego za komunikację sieciową		307
Poznananie źródeł zawartości ruchu sieciowego		308
Dane wpisane na stałe a dane efemeryczne		308
Identyfikacja i wykorzystanie etapów szyfrowania		309
Tworzenie sygnatury		311
Analizowanie reguł parsowania		312
Wybieranie wielu elementów		314
Zrozumienie perspektywy atakującego		315
Podsumowanie		316
CZĘŚĆ 5 ZAPOBIEGANIE INŻYNIERII ODWROTNEJ		321
15		
ZAPOBIEGANIE DEASEMBLACJI		323
O co chodzi w zapobieganiu deasemblacji		324
Pokonać algorytmy deasemblacji		325
Deasemblacja liniowa		325
Deasemblacja śledząca przepływ programu		327
Techniki zapobiegania deasemblacji		330
Instrukcje skoku z tym samym celem		330
Instrukcja skoku ze stałym warunkiem		331
Niemożliwa deasemblacja		332
Wstawianie instrukcji NOP w IDA Pro		335
Zaciemnianie kontroli przepływu wykonania		336
Problem ze wskaźnikiem funkcji		336
Dodawanie brakujących odsyłaczy w kodzie w IDA Pro		337
Nadużywanie wskaźnika powrotu		337
Niewłaściwe wykorzystanie strukturalnej obsługi wyjątków		339
Zapobieganie analizie ramek stosu		342
Podsumowanie		344

16		
ZAPOBIEGANIE DEBUGOWANIU		347
Wykrywanie debuggera w systemie Windows		348
Użycie Windows API		348
Ręczne sprawdzanie struktur		349
Sprawdzanie śladów w systemie		352
Identyfikowanie zachowania debuggera		352
Skanowanie INT		353
Wyznaczanie sum kontrolnych kodu		353
Kontrole czasu		353
Zakłócanie funkcjonalności debuggera		355
Użycie wywołań zwrotnych TLS		355
Użycie wyjątków		357
Wstawianie przerw		358
Luki w debuggerach		359
Luki w nagłówku PE		359
Luka w OutputDebugString		361
Podsumowanie		361
17		
TECHNIKI WYKRYWANIA MASZYNY WIRTUALNEJ		365
Artefakty VMware		366
Omijanie wyszukiwania artefaktów VMware		368
Sprawdzanie artefaktów pamięci		369
Podatności w instrukcjach		369
Użycie jako anti-WM techniki Red Pill		370
Użycie techniki No Pill		371
Odpytywanie portu komunikacji we/wy		372
Użycie instrukcji str.		373
Instrukcje anti-VM architektury x86		373
Podświetlanie anti-VM w IDA Pro		373
Użycie ScoopyNG		375
Podkręcanie ustawień		375
Poza maszynę wirtualną		376
Podsumowanie		376
18		
PAKOWANIE I ROZPAKOWYWANIE		379
Anatomia pakera		380
Nakładka rozpakowująca		380
Ładowanie pliku wykonywalnego		380
Rozwiązywanie importów		381
Skok ogonowy		382
Ilustracja procesu rozpakowywania		382
Rozpoznawanie spakowanych programów		383
Wskaźniki spakowanego programu		383
Obliczanie entropii		383

Warianty rozpakowywania	384
Automatyczne rozpakowywanie	384
Rozpakowywanie ręczne	385
Przebudowa tabeli importów za pomocą narzędzia Import Reconstructor	386
Znajdowanie OEP.	387
Ręczna naprawa tabeli importów	392
Wskazówki i porady dotyczące popularnych pakerów	393
UPX	393
PECompact.	393
ASPack	394
Petite	394
WinUpack	394
Themida	396
Analizowanie bez pełnego rozpakowywania	396
Spakowane biblioteki DLL	397
Podsumowanie	398

CZĘŚĆ 6 TEMATY SPECJALNE 399

19

ANALIZOWANIE SHELLCODE	401
Ładowanie shellcode'u w celu analizy.	402
Kod niezależny od pozycji	402
Określanie miejsca wykonywania	403
Użycie call/pop	403
Użycie fnstenv.	405
Manualne rozwiązywanie symboli	407
Znajdowanie kernel32.dll w pamięci	407
Parsowanie danych o eksportach z PE.	409
Użycie zahaszowanych nazw eksportów	410
Kompletny przykład Hello World	412
Szyfrowanie shellcode'u	415
Ślizganie się po NOP-ach	416
Poszukiwanie shellcode'u	416
Podsumowanie	418

20

ANALIZOWANIE C++.	421
Programowanie obiektowe	421
Wskaźnik this	422
Przeciążanie i dekorowanie	424
Dziedziczenie i nadpisywanie funkcji	425
Funkcje wirtualne	426
Użycie vtable	428
Rozpoznawanie vtable	429
Tworzenie i niszczenie obiektów	430
Podsumowanie	431

21	
64-BITOWE MALWARE	435
Dlaczego 64-bitowe malware?	436
Różnice w architekturze x64	437
Różnice w konwencji wywołań i użyciu stosu w x64	438
Funkcje wywołujące i nie wywołujące innych funkcji	440
Prolog i epilog w kodzie 64-bitowym	440
64-bitowa obsługa wyjątków	441
Windows 32-bitowy w Windowsie 64-bitowym	441
Wskazówki dotyczące funkcjonalności 64-bitowego malware	442
Podsumowanie	443
DODATEK A	
WAŻNE FUNKCJE SYSTEMU WINDOWS	445
DODATEK B	
NARZĘDZIA DO ANALIZY MALWARE	457
DODATEK C	
ROZWIĄZANIA ĆWICZEŃ LABORATORYJNYCH	469
Laboratorium 1.1 – rozwiązania	469
Laboratorium 1.2 – rozwiązania	471
Laboratorium 1.3 – rozwiązania	472
Laboratorium 1.4 – rozwiązania	473
Laboratorium 3.1 – rozwiązania	474
Laboratorium 3.2 – rozwiązania	477
Laboratorium 3.3 – rozwiązania	482
Laboratorium 3.4 – rozwiązania	484
Laboratorium 5.1 – rozwiązania	485
Laboratorium 6.1 – rozwiązania	492
Laboratorium 6.2 – rozwiązania	494
Laboratorium 6.3 – rozwiązania	499
Laboratorium 6.4 – rozwiązania	502
Laboratorium 7.1 – rozwiązania	504
Laboratorium 7.2 – rozwiązania	509
Laboratorium 7.3 – rozwiązania	511
Laboratorium 9.1 – rozwiązania	521
Laboratorium 9.2 – rozwiązania	530
Laboratorium 9.3 – rozwiązania	535
Laboratorium 10.1 – rozwiązania	539
Laboratorium 10.2 – rozwiązania	545
Laboratorium 10.3 – rozwiązania	551
Laboratorium 11.1 – rozwiązania	557
Laboratorium 11.2 – rozwiązania	562
Laboratorium 11.3 – rozwiązania	571
Laboratorium 12.1 – rozwiązania	576
Laboratorium 12.2 – rozwiązania	581

Laboratorium 12.3 – rozwiązania	588
Laboratorium 12.4 – rozwiązania	590
Laboratorium 13.1 – rozwiązania	598
Laboratorium 13.2 – rozwiązania	602
Laboratorium 13.3 – rozwiązania	608
Laboratorium 14.1 – rozwiązania	617
Laboratorium 14.2 – rozwiązania	623
Laboratorium 14.3 – rozwiązania	628
Laboratorium 15.1 – rozwiązania	636
Laboratorium 15.2 – rozwiązania	637
Laboratorium 15.3 – rozwiązania	642
Laboratorium 16.1 – rozwiązania	646
Laboratorium 16.2 – rozwiązania	651
Laboratorium 16.3 – rozwiązania	655
Laboratorium 17.1 – rozwiązania	660
Laboratorium 17.2 – rozwiązania	663
Laboratorium 17.3 – rozwiązania	668
Laboratorium 18.1 – rozwiązania	675
Laboratorium 18.2 – rozwiązania	676
Laboratorium 18.3 – rozwiązania	677
Laboratorium 18.4 – rozwiązania	680
Laboratorium 18.5 – rozwiązania	682
Laboratorium 19.1 – rozwiązania	686
Laboratorium 19.2 – rozwiązania	689
Laboratorium 19.3 – rozwiązania	694
Laboratorium 20.1 – rozwiązania	703
Laboratorium 20.2 – rozwiązania	704
Laboratorium 20.3 – rozwiązania	707
Laboratorium 21.1 – rozwiązania	714
Laboratorium 21.2 – rozwiązania	719
INDEKS	723