

Spis treści

O książce	7
Wstęp	9
Wymagana wiedza, sprzęt i oprogramowanie	10
Języki programowania a złośliwe oprogramowanie	10
Rozdział 1. Architektura procesorów z rodziny 80x86	11
Organizacja pamięci	11
Rejestry procesora	12
Stos	13
Tryby pracy	14
Tryby adresowania	14
Budowa rozkazu	15
Zestawy instrukcji	16
Rozdział 2. Architektura systemów z rodziny Windows NT	17
Różnice pomiędzy systemami Windows 9x i Windows NT	17
Procesy i wątki	18
Procesy systemowe	18
Poziomy uprawnień	18
Usługi	20
Budowa pliku wykonywalnego	20
Kontrola konta użytkownika	21
Zabezpieczenie przed zmianami jądra Windows	22
Rozdział 3. Złośliwe oprogramowanie	23
Technika łączenia z innymi programami	24
Plan funkcjonalności	24
Ogólny algorytm działania	25
Implementacja	26
Inne stosowane techniki	46
Polimorfizm, oligomorfizm i metamorfizm	46
Technika wstrzyknięcia kodu do procesu	47
Technika RunPE	48
Utworzenie zdalnego wątku w procesie	56
Wstrzyknięcie biblioteki DLL	61
Techniki tworzenia podpięć (ang. hooking)	63

Podpięcia do Windows za pomocą SetWindowsHookEx	64
Podpięcia do funkcji za pomocą biblioteki Detours	70
Podpięcia do funkcji z biblioteki NTDLL.DLL	72
Zostawienie możliwości zdalnej kontroli	75
Zasada działania i pochodzenie nazwy	75
Opis wybranych funkcji gniazd Windows	75
Implementacja prostego programu Klient-Serwer	76
Techniki wykradania danych	80
Zastraszanie użytkownika	86
Bomba z zapalnikiem czasowym	86
Wsparcie z internetu, czyli Trojan Downloader	89
Zasada działania	89
Przykładowa implementacja	89
Techniki utrudniające wykrycie i analizę	90
Antyodpluskwanie	90
Antydisasemblacja	91
Antyemulacja	92
Dynamiczne wywoływanie funkcji	94
Zaciemnianie kodu	95
Fałszywe rozszerzenie pliku	96
Miejsca zachowania plików i autostart	97
Techniki rozprzestrzeniania	97
Infekowanie pamięci USB	97
Rozprzestrzenianie P2P	97
Technika Java-Drive-By	97
Tradycyjny wirus	99
Implementacja przykładowego wirusa	99
Rozdział 4. Obrona przed złośliwym oprogramowaniem	105
Zasady bezpiecznej pracy	105
Programy antywirusowe	106
Zapory ogniowe	106
Monitorowanie plików instalowanych w systemie za pomocą Sandboxie	106
Rozdział 5. Zakończenie	109
Wywiad z twórcą złośliwego oprogramowania	109
Dodatek A Skanery online i serwisy analizujące pliki	111
Dodatek B Podstawowe instrukcje języka Asembler	113
Dodatek C Biblioteka standardowa języka C	119
assert.h — Odpluskwanie (ang. Debugging)	119
ctype.h — Funkcje do typów znakowych	119
errno.h — Błędy	120
float.h — Liczby zmiennoprzecinkowe	121
iso646.h — Operacje logiczne i bitowe	121
limits.h — Rozmiary typów całkowitych	122
locale.h — Lokalizacja programów	123
math.h — Obliczenia matematyczne	123
setjmp.h — Skoki nielokalne	124
signal.h — Sygnały	124
stdarg.h — Argumenty	125
stddef.h — Definicje standardowe	125
stdio.h — Operacje wejścia/wyjścia	126

Funkcje	126
Stałe	128
Typy	128
stdlib.h — Narzędzia standardowe	128
Funkcje	128
string.h — Łańcuchy znaków	130
Funkcje	130
time.h — Czas	131
Funkcje	131
Dodatek D Bibliografia	132
Skorowidz	134

Książka powstała na podstawie obserwacji środowisk twórców złośliwego oprogramowania (głównie na zagranicznych forach internetowych) i po przeprowadzeniu wielu rozmów z autorami tych programów. Najwięcej wiedzy w tej dziedzinie zdobyłem w czasie studiów. To był początek mojej fascynacji bezpieczeństwem informatycznym i programowaniem. Pisałem i testowałem różne narzędzia na swoim komputerze i w sieci domowej. Nigdy jednak nie używałem swojej wiedzy i umiejętności w złych celach. Raczej cieszyło mnie, że pokonałem barierę systemu postawionego w celach testowych oraz gdy ludzie zgłaszali się do mnie, abym pomógł im zabezpieczyć komputer czy usunąć infekcję. Z całym szacunkiem do Ciebie, czytelniku, bo może nie to jest Twoim celem: jeżeli myślisz, że dzięki tej książce będziesz mógł się włamywać, niszczyć i okradać ludzi, pomyliłeś się. Nie po to powstała ta książka. Przytoczę tutaj słowa mojego znajomego księdza: „Szatan chce, żeby ludzie myśleli, że on nie istnieje, żeby nie wiedzieli, w jaki sposób działa, wtedy jest on łatwiej nim zawiądnąć”. Można to odnieść do złośliwego kodu: uświadom sobie, że on istnieje. Wiedz, że używa coraz ambitniejszych technik, i choć po części zrozum, w jaki sposób działa.

Cel i zakres

Celem książki jest zapoznanie czytelnika z technikami tworzenia złośliwego oprogramowania oraz sposobami obrony przed tym oprogramowaniem.

Materiały zawarte w tej książce służą jedynie celom edukacyjnym i badawczym. Autor nie ponosi odpowiedzialności za niewłaściwe wykorzystanie tych materiałów ani za ewentualne szkody, które prezentowane oprogramowanie może wyrządzić.

Książka opisuje podstawowe rodzaje złośliwego oprogramowania tworzone dla systemów Microsoft® Windows® z rodziny NT, gdyż te systemy są najczęstszym celem ataków; tekst zawiera też opisy różnych technik (nie tylko programistycznych) twórców *malware* (z ang. *złośliwe oprogramowanie*).