

Spis treści

O autorze	15
O recenzentach	16
Przedmowa	17

CZĘŚĆ 1. Działanie złośliwego oprogramowania — wstrzykiwanie, persystencja i techniki eskalacji przywilejów

ROZDZIAŁ 1	
Krótkie wprowadzenie do tworzenia złośliwego oprogramowania	25
Wymagania techniczne	25
Po co pisać złośliwe oprogramowanie?	26
Prosty przykład	26
Funkcje i działanie złośliwego oprogramowania	28
Typy złośliwego oprogramowania	28
Powłoki odwrotne	29
Praktyczny przykład: powłoka odwrotna	30
Praktyczny przykład: powłoka odwrotna dla Windows	31
Demonstracja	33
Używanie wewnętrznych funkcji Windows do tworzenia złośliwego oprogramowania	35
Praktyczny przykład	35
Analizowanie plików PE (EXE i DLL)	37
Praktyczny przykład	45
Sztuka oszukiwania systemu ofiary	46
Podsumowanie	48

ROZDZIAŁ 2

Różne metody wstrzykiwania złośliwego oprogramowania	49
Wymagania techniczne	49
Tradycyjne metody wstrzykiwania — kod i biblioteki DLL	50
Prosty przykład	50
Przykład wstrzykiwania kodu	53
Wstrzykiwanie bibliotek DLL	60
Przykład wstrzykiwania biblioteki DLL	61
Techniki uprowadzania	65
Uprowadzanie bibliotek DLL	67
Praktyczny przykład	68
Wstrzykiwanie kodu z użyciem asynchronicznych wywołań procedury	72
Praktyczny przykład wstrzykiwania APC	72
Praktyczny przykład wstrzykiwania APC za pośrednictwem NtTestAlert	77
Techniki podłączania się do wywołań API	77
Co to jest podłączanie się do wywołań API?	77
Praktyczny przykład	77
Podsumowanie	84

ROZDZIAŁ 3

Mechanizmy persystencji złośliwego oprogramowania	85
Wymagania techniczne	85
Klasyczna ścieżka — klucze Run w rejestrze	86
Prosty przykład	86
Wykorzystywanie kluczy rejestru używanych przez proces Winlogon	90
Praktyczny przykład	90
Wykorzystywanie kolejności wyszukiwania bibliotek DLL do utrwalenia złośliwego oprogramowania	96
Wykorzystywanie usług Windows do persystencji	101
Praktyczny przykład	101
W poszukiwaniu persystencji — badanie nieoczywistych furtek	110
Praktyczny przykład	110
Jak znajdować nowe sztuczki persystencyjne?	116
Podsumowanie	116

ROZDZIAŁ 4	
Escalacja przywilejów w zainfekowanych systemach	117
Wymagania techniczne	117
Manipulowanie tokenami dostępowymi	118
Tokeny Windows	118
Lokalny administrator	121
SeDebugPrivilege	122
Praktyczny przykład	123
Impersonacja	128
Kradzież haseł	128
Praktyczny przykład	129
Ingerowanie w kolejność wyszukiwania bibliotek DLL	
i ataki na łańcuch dostaw	133
Praktyczny przykład	133
Obchodzenie UAC	137
fodhelper.exe	137
Praktyczny przykład	139
Podsumowanie	143

CZĘŚĆ 2. Techniki unikania wykrycia

ROZDZIAŁ 5	
Sztuczki zapobiegające debugowaniu	147
Wymagania techniczne	147
Wykrywanie obecności debugera	147
Praktyczny przykład nr 1	148
Praktyczny przykład nr 2	150
Wykrywanie punktów przerwania	151
Praktyczny przykład	152
Identyfikowanie flag i artefaktów	154
Praktyczny przykład	155
ProcessDebugFlags	157
Praktyczny przykład	157
Podsumowanie	158

ROZDZIAŁ 6

Strategie zwalczania maszyn wirtualnych	160
Wymagania techniczne	160
Techniki wykrywania systemu plików	161
Wykrywanie maszyny wirtualnej VirtualBox	161
Praktyczny przykład	161
Demonstracja	162
Podejścia do wykrywania sprzętu	164
Sprawdzanie dysku twardego	164
Demonstracja	164
Techniki wykrywania sandboksów oparte na czasie	165
Prosty przykład	165
Identyfikowanie maszyn wirtualnych za pośrednictwem rejestru	167
Praktyczny przykład	168
Demonstracja	169
Podsumowanie	171

ROZDZIAŁ 7

Strategie zapobiegania dezasemblacji	172
Popularne techniki zapobiegania dezasemblacji	172
Praktyczny przykład	173
Wykorzystanie przepływu sterowania między funkcjami	176
Praktyczny przykład	177
Obfuskacja API i kodu asemblera	178
Praktyczny przykład	178
Doprowadzanie do awarii narzędzi analitycznych	181
Praktyczny przykład	181
Podsumowanie	182

ROZDZIAŁ 8

W labiryncie antywirusów — gra w kotka i myszkę	183
Wymagania techniczne	183
Mechanika antywirusów	184
Detekcja statyczna	184
Detekcja heurystyczna	184
Dynamiczna analiza heurystyczna	185
Analiza behawioralna	185

Zapobieganie detekcji statycznej	185
Praktyczny przykład	185
Zapobieganie analizie dynamicznej	192
Praktyczny przykład	193
Obchodzenie interfejsu skanowania złośliwego oprogramowania (AMSI)	194
Praktyczny przykład	194
Zaawansowane techniki unikania wykrycia	195
Wywołania systemowe	196
Identyfikator wywołania systemowego	196
Praktyczny przykład	196
Haki w trybie użytkownika	198
Bezpośrednie wywołania systemowe	199
Praktyczny przykład	199
Obchodzenie EDR	201
Praktyczny przykład	201
Podsumowanie	203

CZĘŚĆ 3. Matematyka i kryptografia w złośliwym oprogramowaniu

ROZDZIAŁ 9

Algorytmy haszowania	207
Wymagania techniczne	207
Rola algorytmów haszowania w złośliwym oprogramowaniu	208
Kryptograficzne funkcje skrótu	208
Haszowanie w analizie złośliwego oprogramowania	209
Przegląd typowych algorytmów haszowania	209
MD5	209
SHA-1	210
Bcrypt	212
Praktyczne użycie algorytmów haszowania w złośliwym oprogramowaniu	213
Haszowanie wywołań WinAPI	213
MurmurHash	219
Podsumowanie	222

ROZDZIAŁ 10	
Proste szyfry	223
Wymagania techniczne	223
Wprowadzenie do prostych szyfrów	224
Szyfr Cezara	224
Szyfr ROT13	224
Szyfr ROT47	224
Odszyfrowywanie złośliwego oprogramowania — praktyczna implementacja prostych szyfrów	225
Szyfr Cezara	226
ROT13	227
ROT47	229
Algorytm Base64	231
Base64 w praktyce	231
Podsumowanie	239
ROZDZIAŁ 11	
Kryptografia w złośliwym oprogramowaniu	240
Wymagania techniczne	240
Przegląd technik kryptograficznych używanych w złośliwym oprogramowaniu	240
Szyfrowanie zasobów — plików konfiguracyjnych	241
Praktyczny przykład	242
Zabezpieczanie komunikacji za pomocą kryptografii	248
Praktyczny przykład	248
Ochrona ładunku — kryptografia jako sposób na obfuskację	252
Praktyczny przykład	252
Podsumowanie	255
ROZDZIAŁ 12	
Zaawansowane algorytmy matematyczne i kodowanie niestandardowe	256
Wymagania techniczne	257
Przegląd zaawansowanych algorytmów matematycznych używanych w złośliwym oprogramowaniu	257
Tiny encryption algorithm (TEA)	257
A5/1	258

Algorytm Madrygi	258
Skipjack	258
Praktyczny przykład	258
Używanie liczb pierwszych i arytmetyki modularnej w złośliwym oprogramowaniu	261
Praktyczny przykład	261
Implementowanie niestandardowych technik kodowania	266
Praktyczny przykład	266
Kryptografia krzywych eliptycznych (ECC) a złośliwe oprogramowanie	269
Praktyczny przykład	270
Podsumowanie	272

CZĘŚĆ 4. Przykłady rzeczywistego złośliwego oprogramowania

ROZDZIAŁ 13

Klasyczne przykłady złośliwego oprogramowania	275
Historyczny przegląd klasycznego złośliwego oprogramowania	275
Wczesne złośliwe oprogramowanie	276
Lata 80. XX wieku – pierwsza dekada XXI wieku — era robaków i masowej propagacji	276
Złośliwe oprogramowanie w XXI w.	276
Współczesne trojany bankowe	277
Ewolucja ransomware’u	277
Analiza technik stosowanych przez klasyczne złośliwe oprogramowanie	278
Ewolucja i wpływ klasycznego złośliwego oprogramowania	281
Czego można się nauczyć z klasycznego złośliwego oprogramowania?	284
Praktyczny przykład	285
Podsumowanie	289

ROZDZIAŁ 14

APT i cyberprzestępczość	290
Wprowadzenie do zaawansowanych uporczywych zagrożeń	290
Narodziny APT — wczesne lata 2000.	291
Operacja Aurora (2009)	291

Stuxnet i początek ataków cybernetyczno-fizycznych (2010)	291
Wzrost zagrożeń ze strony państwowych grup APT — od 2015 roku do dziś	292
Obecny krajobraz zagrożeń i przyszłe wyzwania	292
Cechy zaawansowanych uporczywych zagrożeń	292
Ostawione przykłady zaawansowanych uporczywych zagrożeń	294
APT28 (Fancy Bear) — rosyjska grupa cyberszpiegowska	295
APT29 (Cozy Bear) — uporczywy intruz	295
Grupa Lazarus — wielowymiarowe zagrożenie	295
Grupa Equation — szpiegowskie ramię NSA	295
Tailored Access Operations — cyfrowy arsenał NSA	296
TTP używane przez APT	296
Persystencja z użyciem klucza Applnit_DLLs	296
Persystencja poprzez funkcje ułatwień dostępu	300
Persystencja przez alternatywne strumienie danych	305
Podsumowanie	308

ROZDZIAŁ 15

Wycieki kodu źródłowego złośliwego oprogramowania	309
Przegląd wycieków kodu źródłowego złośliwego oprogramowania	309
Trojan bankowy Zeus	310
Carberp	310
Carbanak	311
Inne słynne wycieki kodu źródłowego złośliwego oprogramowania	312
Wpływ wycieków kodu źródłowego na rozwój złośliwego oprogramowania	313
Zeus	313
Carberp	315
Carbanak	316
Praktyczny przykład	320
Znaczące wycieki kodu źródłowego złośliwego oprogramowania	324
Podsumowanie	327

ROZDZIAŁ 16

Ransomware i współczesne zagrożenia	328
Wprowadzenie do ransomware'u i współczesnych zagrożeń	328
Analiza technik używanych przez ransomware	330
Conti	330
Hello Kitty	339
Studia głośnych przypadków ransomware'u i współczesnych zagrożeń	343
Pierwsze studium przypadku — atak ransomware'u WannaCry	343
Drugie studium przypadku — atak ransomware'u NotPetya	343
Trzecie studium przypadku — ransomware GandCrab	344
Czwarte studium przypadku — ransomware Ryuk	344
Współczesne zagrożenia	345
Praktyczny przykład	347
Strategie łagodzenia skutków ataku i przywracania danych	349
Podsumowanie	350

Chcę też podziękować wszystkim pracownikom holdingu Kuzdream Technologies IT, nie zdolałam tu wymienić wszystkich, więc szczególnie dziękuję mojemu przyjacielowi Daurenowi Tulebaevowi, który zainspirował powstanie fundacji charytatywnej +1, Anyi Tsygarowej, a także Kokharowi Kashimovowi, Artamanowi Shaykhin, Madiyarowi Tuleuovowi, Gulmirze Kupeshiev, Valisowi Yerekeshowi, Alexeyowi i Artemowi Rychkom, Daurynowi Saltymowi, Saktynowi Tleuberdinowi, Timurovi Omarovowi, Marlenowi Muslimovowi, Alimowi Bektashowi, Kanatowi Zilenovowi i Ayanowi Sutybaldiemu.

Dziękuję też moim przyjaciołom Olzhasowi Sattyevowi i Yenlikowi Sattyevie.

Dziękuję wreszcie całemu zespołowi wydawnictwa Packt Publishing, bez którego to książka wyszłaby zupełnie inaczej, zwłaszcza Ashwin! Gowdatie, Neha Sharma i Rinalowi Nabeilo.