

# Spis treści

|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| <b>Słowem wstępu .....</b>                                            | <b>11</b> |
| <b>Rozdział 1. Hacking — wprowadzenie .....</b>                       | <b>15</b> |
| 1.1. Na czym polega działalność hakerów .....                         | 15        |
| 1.2. Subkultura hakerów .....                                         | 15        |
| 1.3. Wojna cybernetyczna .....                                        | 16        |
| <b>Rozdział 2. Pakiety MASM32 i MASM64 .....</b>                      | <b>17</b> |
| 2.1. Przygotowanie środowiska pracy MASM32 .....                      | 17        |
| 2.1.1. Program „Witaj, 32-bitowy świecie!” .....                      | 17        |
| 2.2. Przygotowanie środowiska pracy MASM64 .....                      | 18        |
| 2.2.1. Program „Witaj, 64-bitowy świecie!” .....                      | 21        |
| <b>Rozdział 3. Architektura procesorów z rodziny x86(-64) .....</b>   | <b>23</b> |
| 3.1. Organizacja pamięci .....                                        | 23        |
| 3.2. Rejestry procesora .....                                         | 26        |
| 3.3. Stos .....                                                       | 38        |
| 3.4. Tryby pracy .....                                                | 40        |
| 3.5. Tryby adresowania .....                                          | 41        |
| 3.6. Zestawy instrukcji .....                                         | 42        |
| 3.7. Format instrukcji procesora .....                                | 45        |
| 3.7.1. Rozkodowanie instrukcji .....                                  | 45        |
| <b>Rozdział 4. Architektura systemów z rodziny Windows NT .....</b>   | <b>49</b> |
| 4.1. Procesy i wątki .....                                            | 49        |
| 4.2. Poziomy uprawnień .....                                          | 52        |
| 4.3. Format plików wykonywalnych Portable Executable (PE/PE32+) ..... | 53        |
| 4.4. System plików .....                                              | 55        |
| 4.4.1. Wybrane funkcje Windows API do operacji na plikach .....       | 55        |

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| 4.5. Wiersz polecenia .....                                                          | 60 |
| 4.6. Windows PowerShell .....                                                        | 60 |
| 4.6.1. Przykład. Liczenie linii, słów i znaków w plikach w określonym katalogu ..... | 61 |

## **Rozdział 5. Asembler x86(-64) — instrukcje ogólnego przeznaczenia ..... 63**

|                                                       |    |
|-------------------------------------------------------|----|
| 5.1. Instrukcje transferu danych .....                | 63 |
| 5.1.1. Instrukcja MOV .....                           | 63 |
| 5.1.2. Instrukcje kopiowania warunkowego CMOVcc ..... | 64 |
| 5.1.3. Instrukcja XCHG .....                          | 66 |
| 5.1.4. Instrukcja BSWAP .....                         | 67 |
| 5.1.5. Instrukcja XADD .....                          | 68 |
| 5.1.6. Instrukcja CMPXCHG .....                       | 69 |
| 5.1.7. Instrukcje CMPXCHG8B/CMPXCHG16B .....          | 69 |
| 5.1.8. Instrukcja PUSH .....                          | 70 |
| 5.1.9. Instrukcja POP .....                           | 71 |
| 5.1.10. Instrukcje PUSHA/PUSHAD .....                 | 71 |
| 5.1.11. Instrukcje POPA/POPAD .....                   | 72 |
| 5.1.12. Instrukcje CWD/CDQ/CQO .....                  | 72 |
| 5.1.13. Instrukcje CBW/CWDE/CDQE .....                | 73 |
| 5.1.14. Instrukcja MOVSX/MOVSXD .....                 | 73 |
| 5.1.15. Instrukcja MOVZX .....                        | 74 |
| 5.2. Instrukcje arytmetyczne .....                    | 75 |
| 5.2.1. Instrukcja ADCX .....                          | 75 |
| 5.2.2. Instrukcja ADOX .....                          | 76 |
| 5.2.3. Instrukcja ADD .....                           | 76 |
| 5.2.4. Instrukcja ADC .....                           | 77 |
| 5.2.5. Instrukcja SUB .....                           | 77 |
| 5.2.6. Instrukcja SBB .....                           | 78 |
| 5.2.7. Instrukcja IMUL .....                          | 79 |
| 5.2.8. Instrukcja MUL .....                           | 79 |
| 5.2.9. Instrukcja IDIV .....                          | 80 |
| 5.2.10. Instrukcja DIV .....                          | 80 |
| 5.2.11. Instrukcja INC .....                          | 81 |
| 5.2.12. Instrukcja DEC .....                          | 81 |
| 5.2.13. Instrukcja NEG .....                          | 81 |
| 5.2.14. Instrukcja CMP .....                          | 82 |
| 5.3. Instrukcje logiczne .....                        | 82 |
| 5.3.1. Instrukcja AND .....                           | 82 |
| 5.3.2. Instrukcja OR .....                            | 82 |

|                                                       |     |
|-------------------------------------------------------|-----|
| 5.3.3. Instrukcja XOR .....                           | 83  |
| 5.3.4. Instrukcja NOT .....                           | 83  |
| 5.4. Instrukcje przesunięć i obrotów .....            | 84  |
| 5.4.1. Instrukcje SAL/SHL .....                       | 84  |
| 5.4.2. Instrukcja SAR .....                           | 85  |
| 5.4.3. Instrukcja SHR .....                           | 85  |
| 5.4.4. Instrukcja RCL .....                           | 86  |
| 5.4.5. Instrukcja RCR .....                           | 87  |
| 5.4.6. Instrukcja ROL .....                           | 88  |
| 5.4.7. Instrukcja ROR .....                           | 89  |
| 5.4.8. Instrukcja SHRD .....                          | 89  |
| 5.4.9. Instrukcja SHLD .....                          | 90  |
| 5.5. Instrukcje do operacji na bitach i bajtach ..... | 91  |
| 5.5.1. Instrukcja BT .....                            | 91  |
| 5.5.2. Instrukcja BTS .....                           | 92  |
| 5.5.3. Instrukcja BTR .....                           | 92  |
| 5.5.4. Instrukcja BTC .....                           | 92  |
| 5.5.5. Instrukcja BSF .....                           | 93  |
| 5.5.6. Instrukcja BSR .....                           | 93  |
| 5.5.7. Instrukcje SETcc .....                         | 94  |
| 5.5.8. Instrukcja TEST .....                          | 96  |
| 5.5.9. Instrukcja CRC32 .....                         | 96  |
| 5.5.10. Instrukcja POPCNT .....                       | 97  |
| 5.6. Instrukcje manipulacji bitowych .....            | 97  |
| 5.6.1. Instrukcja ANDN .....                          | 97  |
| 5.6.2. Instrukcja BEXTR .....                         | 97  |
| 5.6.3. Instrukcja BLSI .....                          | 98  |
| 5.6.4. Instrukcja BLSMSK .....                        | 98  |
| 5.6.5. Instrukcja BLSR .....                          | 99  |
| 5.6.6. Instrukcja BZHI .....                          | 99  |
| 5.6.7. Instrukcja LZCNT .....                         | 99  |
| 5.6.8. Instrukcja MULX .....                          | 100 |
| 5.6.9. Instrukcja PDEP .....                          | 100 |
| 5.6.10. Instrukcja PEXT .....                         | 101 |
| 5.6.11. Instrukcja RORX .....                         | 101 |
| 5.6.12. Instrukcje SARX, SHLX, SHRX .....             | 102 |
| 5.6.13. Instrukcja TZCNT .....                        | 102 |
| 5.7. Instrukcje kontroli przepływu .....              | 103 |
| 5.7.1. Instrukcja JMP .....                           | 103 |
| 5.7.2. Instrukcje Jcc .....                           | 103 |

|         |                                          |     |
|---------|------------------------------------------|-----|
| 5.7.3.  | Instrukcje LOOP/LOOPcc .....             | 105 |
| 5.7.4.  | Instrukcja CALL .....                    | 106 |
| 5.7.5.  | Instrukcja RET .....                     | 106 |
| 5.8.    | Instrukcje do operacji na napisach ..... | 106 |
| 5.8.1.  | Instrukcje MOVS* .....                   | 106 |
| 5.8.2.  | Instrukcje CMPS* .....                   | 107 |
| 5.8.3.  | Instrukcje LODS* .....                   | 108 |
| 5.8.4.  | Instrukcje STOS* .....                   | 109 |
| 5.8.5.  | Instrukcje SCAS* .....                   | 110 |
| 5.9.    | Instrukcje wejścia/wyjścia .....         | 111 |
| 5.9.1.  | Instrukcja IN .....                      | 111 |
| 5.9.2.  | Instrukcja OUT .....                     | 111 |
| 5.9.3.  | Instrukcje INS* .....                    | 111 |
| 5.9.4.  | Instrukcje OUTS* .....                   | 112 |
| 5.10.   | Instrukcje kontroli flag .....           | 112 |
| 5.11.   | Instrukcje różne .....                   | 113 |
| 5.11.1. | Instrukcja LEA .....                     | 113 |
| 5.11.2. | Instrukcja NOP .....                     | 113 |
| 5.11.3. | Instrukcja UD2 .....                     | 113 |
| 5.11.4. | Instrukcja CPUID .....                   | 114 |
| 5.11.5. | Instrukcja MOVBE .....                   | 114 |

## **Rozdział 6. Asembler x86(-64) — zrozumieć język wirusów ..... 115**

|         |                                                              |     |
|---------|--------------------------------------------------------------|-----|
| 6.1.    | Struktura programu MASM64 .....                              | 115 |
| 6.2.    | Zmienne i stałe .....                                        | 115 |
| 6.2.1.  | Stałe .....                                                  | 116 |
| 6.2.2.  | Zmienne o rozmiarze bajta lub ciągu bajtów .....             | 116 |
| 6.2.3.  | Zmienne o rozmiarze słowa (ang. word) .....                  | 116 |
| 6.2.4.  | Zmienne o rozmiarze podwójnego słowa (ang. doubleword) ..... | 116 |
| 6.2.5.  | Zmienne o rozmiarze poczwórnego słowa (ang. quadword) .....  | 117 |
| 6.2.6.  | Zmienne o rozmiarze 6 bajtów .....                           | 117 |
| 6.2.7.  | Zmienne o rozmiarze 10 bajtów .....                          | 117 |
| 6.2.8.  | Zmienne o rozmiarze 16 bajtów .....                          | 117 |
| 6.2.9.  | Zmienne do przechowywania liczb zmiennoprzecinkowych .....   | 117 |
| 6.2.10. | Zmienne używane przy instrukcjach rozszerzeń MMX i SSE ..... | 118 |
| 6.3.    | Adresowanie argumentów .....                                 | 118 |
| 6.3.1.  | Operator offset .....                                        | 118 |
| 6.3.2.  | Instrukcja LEA .....                                         | 119 |
| 6.3.3.  | Dereferencja (operator [ ]) .....                            | 119 |

|                                                 |     |
|-------------------------------------------------|-----|
| 6.4. Wywoływanie funkcji Windows API .....      | 120 |
| 6.5. Program not-virus.CDJoke.Win64 .....       | 121 |
| 6.6. Program not-virus.MonitorOFF.Win64 .....   | 122 |
| 6.7. Program TrojanBanker.AsmKlip.Win64 .....   | 124 |
| 6.8. Program BitcoinStealer.AsmKlip.Win64 ..... | 128 |

## **Rozdział 7. Backdoor — tylne drzwi do systemu ..... 135**

|                                                            |     |
|------------------------------------------------------------|-----|
| 7.1. Backdoor w języku C# dla pulpitu Windows .....        | 136 |
| 7.1.1. Panel kontrolny .....                               | 136 |
| 7.1.2. Program infekujący .....                            | 140 |
| 7.1.3. Podsumowanie .....                                  | 146 |
| 7.2. Hybrydowy backdoor w 7 kilobajtach .....              | 147 |
| 7.2.1. Połączenie odwrotne (ang. reverse connection) ..... | 147 |
| 7.2.2. Panel kontrolny .....                               | 148 |
| 7.2.3. Program infekujący .....                            | 155 |

## **Rozdział 8. Wirus komputerowy — infekcja plików ..... 163**

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| 8.1. Informacje ogólne .....                                                              | 163 |
| 8.2. Infekcja plików wykonywalnych .....                                                  | 164 |
| 8.2.1. Dołączanie kodu wirusa do pliku wykonywalnego .....                                | 168 |
| 8.2.2. Tworzenie „ładunku”, którym będą infekowane pliki .....                            | 172 |
| 8.2.3. Payload Detonator — aplikacja do testowania kodu typu payload<br>i shellcode ..... | 175 |

## **Rozdział 9. File Binder — złośliwy kod „doklejony” do pliku ..... 177**

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| 9.1. Ukrywanie plików w zasobach programu .....                     | 177 |
| 9.2. Implementacja podstawowej funkcjonalności aplikacji Stub ..... | 178 |

## **Rozdział 10. Keylogger — monitoring działań w systemie ..... 185**

|                                                               |     |
|---------------------------------------------------------------|-----|
| 10.1. Funkcja SetWindowsHookEx .....                          | 185 |
| 10.2. Monitorowanie wciskanych klawiszy w 4 kilobajtach ..... | 187 |
| 10.3. Pobieranie nazwy aktywnego okna .....                   | 193 |
| 10.4. Przesyłanie raportów .....                              | 195 |

## **Rozdział 11. Ransomware — szantażowanie użytkownika ..... 199**

|                                                               |     |
|---------------------------------------------------------------|-----|
| 11.1. Ogólna zasada działania .....                           | 199 |
| 11.2. Atak WannaCry — paraliż ponad 200 tys. komputerów ..... | 199 |
| 11.3. Każdy może stworzyć ransomware .....                    | 201 |

**Rozdział 12. Koń trojański — zdalne sterowanie zainfekowanym komputerem ... 205**

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| 12.1. Trochę historii .....                                                           | 205 |
| 12.1.1. Najpopularniejsze konie trojańskie z lat 1990 – 2010 stworzone w Polsce ..... | 205 |
| 12.2. Pobieranie informacji o systemie .....                                          | 208 |
| 12.3. Zdalny menedżer plików .....                                                    | 209 |
| 12.3.1. Listowanie, usuwanie i uruchamianie plików .....                              | 210 |
| 12.3.2. Przesyłanie plików przez gniazdo .....                                        | 211 |
| 12.4. Podgląd kamery internetowej .....                                               | 213 |
| 12.5. Zrzuty ekranu (ang. screenshots) .....                                          | 216 |
| 12.6. Dodatkowe funkcjonalności .....                                                 | 217 |

**Rozdział 13. Pozostałe zagrożenia ..... 219**

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| 13.1. Adware — niechciane reklamy .....                                         | 219 |
| 13.2. Bakteria komputerowa — replikacja aż do wyczerpania zasobów .....         | 220 |
| 13.3. Bomba logiczna — uruchamianie złośliwego kodu po spełnieniu warunku ..... | 220 |
| 13.4. Botnet — sieć komputerów zombie .....                                     | 222 |
| 13.5. Chargeware — ukryte opłaty i niejasny regulamin .....                     | 222 |
| 13.6. Exploit — użycie błędu w oprogramowaniu .....                             | 223 |
| 13.7. Form Grabber — przechwytywanie danych z formularzy .....                  | 224 |
| 13.8. Hoax — fałszywy alarm .....                                               | 225 |
| 13.9. Robak — rozprzestrzenianie infekcji bez nosiciela .....                   | 225 |
| 13.10. Rootkit — intruz ukryty w systemie .....                                 | 225 |
| 13.11. Stealer — wykradanie poufnych informacji .....                           | 226 |

**Rozdział 14. Bezpieczeństwo systemów Microsoft Windows ..... 229**

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| 14.1. Program antywirusowy .....                                     | 229 |
| 14.2. Zapora ogniowa (ang. firewall) .....                           | 230 |
| 14.3. Maszyna wirtualna .....                                        | 231 |
| 14.4. Konfiguracja systemu Windows zwiększająca bezpieczeństwo ..... | 233 |
| 14.5. Podstawowe narzędzia systemowe .....                           | 234 |
| 14.6. Bezpieczeństwo danych .....                                    | 235 |
| 14.6.1. VPN — wirtualna sieć prywatna .....                          | 235 |
| 14.6.2. Projekt Tor i przeglądarka Tor Browser .....                 | 235 |
| 14.6.3. GNU Privacy Guard .....                                      | 236 |
| 14.6.4. Komunikacja Off-The-Record (OTR) .....                       | 237 |
| 14.6.5. Szyfrowanie nośników z danymi .....                          | 238 |
| 14.6.6. Zdjęcia i metadane EXIF .....                                | 239 |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| 14.7. Bezpieczeństwo haseł .....                                  | 241 |
| 14.7.1. Tworzenie bezpiecznego hasła .....                        | 241 |
| 14.7.2. Łamanie haseł do archiwum RAR, ZIP i innych .....         | 242 |
| 14.7.3. Łamanie haseł do portali internetowych .....              | 242 |
| 14.7.4. Phishing — „Hasel się nie łamie, hasła się wykrada” ..... | 243 |

## **Rozdział 15. Bezpieczeństwo oprogramowania — wprowadzenie .....**

|                                                                         |     |
|-------------------------------------------------------------------------|-----|
| 15.1. Inżynieria odwrotna kodu (ang. Reverse Code Engineering) .....    | 245 |
| 15.2. Subkultura crackerów .....                                        | 246 |
| 15.3. Rodzaje zabezpieczeń w programach .....                           | 247 |
| 15.4. Przegląd przydatnych narzędzi .....                               | 248 |
| 15.5. Legalny cracking — aplikacje typu CrackMe .....                   | 249 |
| 15.5.1. Programowanie aplikacji typu CrackMe .....                      | 249 |
| 15.5.2. Analiza i łamanie wcześniej utworzonego CrackMe .....           | 250 |
| 15.5.3. Tworzenie aplikacji usuwającej zabezpieczenie, tzw. crack ..... | 250 |
| 15.5.4. Dalsza nauka .....                                              | 252 |
| 15.6. Podstawowe zasady analizy złośliwego oprogramowania .....         | 252 |

## **Rozdział 16. Z pamiętnika hakera .....**

|                                                          |     |
|----------------------------------------------------------|-----|
| 16.1. „Skryptowy dzieciak” czy polityczny żołnierz ..... | 255 |
| 16.2. W schizofrenii się nie kradnie .....               | 256 |
| Podsumowując .....                                       | 258 |

## **Rozdział 17. Zakończenie .....**

|                          |     |
|--------------------------|-----|
| 17.1. Podsumowanie ..... | 259 |
|--------------------------|-----|

## **Dodatek A Najczęściej używane funkcje logiczne .....**

## **Dodatek B Leksykon pojęć używanych przez hakerów .....**

## **Dodatek C Aplikacja kopiująca samą siebie do systemu — kod źródłowy (MASM64) .....**

## **Dodatek D Ochrona klucza w rejestrze przed manualnym usunięciem — kod źródłowy (MASM64) .....**

## **Dodatek E Opóźnione uruchomienie (ang. delayed start) — kod źródłowy (MASM64) .....**

## **Skorowidz .....**