

Wirusy komputerowe i ochrona antywirusowa

Praca licencjacka
Uniwersytet Śląski

Wstęp 4

Rozdział 1. Zagrożenia i programy złośliwe 6

1.1. Wirusy 7

1.2. Konie trojańskie 7

1.3. Robaki 7

1.4. Bomby logiczne 8

1.5. Króliki (bakterie) 9

1.6. Tylne wejścia (Backdoors) 9

1.7. Exploit 9

1.8. Dialery 9

1.9. Spyware 10

1.10. Spam 10

1.11. Hoaxy 10

Rozdział 2. Historia i rozwój wirusów komputerowych 12

Rozdział 3. Wirusy komputerowe 21

3.1. Budowa wirusów komputerowych 22

3.2. Parametry wirusów komputerowych 22

3.3. Działanie wirusów komputerowych 24

3.4. Infekcja 25

3.5. Objawy i skutki zakażenia 26

3.6. Drogi propagacji wirusów 27

3.6.1. Niebezpieczne oprogramowanie. 29

3.7. Rozprzestrzenianie się 31

3.8. Co nie grozi zarażeniem 31

3.9. Tworzenie wirusów 33

3.9.1. Kto pisze wirusy komputerowe 33

3.9.2. Języki programowania 33

3.9.3. Generatory wirusów 34

Rozdział 4. Rodzaje wirusów komputerowych 38

4.1. Wirusy plikowe 38

4.1.1. Wirusy plików wsadowych BAT 39

4.1.2. Wirusy drażące 40

4.2. Wirusy sektora startowego 41

4.3. Makrowirusy 42

4.4. Wirusy skryptowe 43

4.5. Wirusy tablicy alokacji plików 43

4.6. Wirusy towarzyszące 44

4.7. Wirusy sprzęgające 45

4.8. Wirusy hybrydowe 45

4.9. Wirusy Intended 46

4.10. Wirusy „zoologiczne” 46

4.11. Retrowirusy 46

Rozdział 5. Podział wirusów ze względu na sposób działania po uruchomieniu 47

5.1. Wirusy nierezydentne 47

5.2. Wirusy rezydentne 48

5.2.1. Szybkie infekторы 50

5.2.2. Wolne infekторы 51

5.3. Wirusy hybrydowe 51

Rozdział 6. Techniki wykorzystywane przez wirusy 52

6.1. Przejmowanie przerwań 52

6.2. Technika stealth 53

6.3. Szyfrowanie 54

6.4. Wirusy polimorficzne 56

6.4.1. MtE Mutation Engine 58

6.5. Wirusy opancerzone 60

6.6. Modyfikacja CMOS-a 61

6.7. Optymalizacje kodu 62

6.8. Infekcja wewnątrzplikowa 62

6.9. Technika EP0 63

6.10. Ukrywanie przed programami antywirusowymi 63

6.11. Ukrywanie rozszerzeń plików 64

- 6.12. Infekcja plików tworzonych przez archiwizatory 64
- 6.13. Hiperinfekcja 65
- 6.14. Dostosowanie wyglądu zewnętrznego 65

Rozdział 7. Wirusy systemu Linux 67

- 7.1. Wirus Bliss 69

Rozdział 8. Najnowsze pomysły 71

- 8.1. Wirusy NTFS 71
- 8.2. Wirusy w JPEG 72
- 8.3. Wirusy dźwiękowe 74
- 8.4. Wirusy w urządzeniach mobilnych 75

Rozdział 9. Aspekt prawny wirusów komputerowych 81

Rozdział 10. Postępowanie antywirusowe 84

Rozdział 11. Rodzaje programów antywirusowych 86

- 11.1. Monitory 86
- 11.2. Skanery 86
- 11.3. Programy zliczające sumy kontrolne 87
- 11.4. Programy autoweryfikujące 87
- 11.5. Szczepionki 87

Rozdział 12. Techniki używane przez programy antywirusowe 88

- 12.1. Skaniny 88
- 12.2. Heurystyczne wyszukiwanie wirusów 88
- 12.3. Tryb krokowy 88
- 12.4. Emulacja procesora 89
- 12.5. Przynęty 89
- 12.6. Odświeżanie programów systemowych w sektorach 89
- 12.7. Blokowanie programów używających trybu krokowego 90
- 12.8. Pobieranie wielkości pamięci operacyjnej 90
- 12.9. Kwarantanna 90

Rozdział 13. Oprogramowanie antywirusowe 91

- 13.1. Symantec Norton AntiVirus 2005 92
- 13.2. Mks_vir 2005 93
- 13.3. AntiVirenKit 2005 Professional 95

13.4. Panda Titanium Antivirus 2005 96

13.5. Kaspersky Anti-Virus Personal 5.0 97

Zakończenie 100

Literatura 101

Wstęp

Postępująca informatyzacja życia społecznego, gospodarczego i prywatnego sprawiła, że systemy komputerowe stały się jednym z kluczowych elementów funkcjonowania współczesnego świata. Komputery oraz sieci teleinformatyczne są dziś nie tylko narzędziem pracy, nauki i komunikacji, ale również podstawą działania administracji publicznej, instytucji finansowych, przedsiębiorstw oraz infrastruktury krytycznej państwa. Wraz z dynamicznym rozwojem technologii informacyjnych rośnie jednak skala zagrożeń związanych z ich wykorzystywaniem. Jednym z najpoważniejszych i najbardziej złożonych problemów w obszarze bezpieczeństwa informatycznego są wirusy komputerowe oraz szeroko pojęte programy złośliwe, których celem jest zakłócanie pracy systemów, niszczenie danych, kradzież informacji lub przejmowanie kontroli nad zasobami użytkownika.

Wirusy komputerowe, choć często kojarzone jedynie z drobnymi uciążliwościami, takimi jak spowolnienie działania komputera czy wyświetlanie niepożądanych komunikatów, w rzeczywistości mogą powodować bardzo poważne konsekwencje. Należą do nich m.in. utrata danych, naruszenie prywatności użytkowników, straty finansowe, a także zagrożenie dla ciągłości działania firm i instytucji. W skali globalnej skutki masowych infekcji mogą prowadzić do paraliżu sieci komputerowych, destabilizacji rynków oraz osłabienia zaufania do nowoczesnych technologii. Z tego względu problematyka wirusów komputerowych oraz metod ochrony przed nimi od wielu lat stanowi istotny obszar badań naukowych, analiz technicznych oraz regulacji prawnych.

Geneza wirusów komputerowych sięga początków rozwoju oprogramowania i systemów operacyjnych, kiedy to twórcy

programów zaczęli eksperymentować z kodem zdolnym do samopowielania i modyfikowania innych aplikacji. Początkowo były to często eksperymenty o charakterze edukacyjnym lub demonstracyjnym, niemające na celu wyrządzenia szkód. Z biegiem czasu, wraz ze wzrostem popularności komputerów osobistych oraz rozwojem sieci komputerowych, wirusy zaczęły ewoluować w coraz bardziej zaawansowane formy. Współczesne złośliwe oprogramowanie charakteryzuje się dużą złożonością techniczną, zdolnością do ukrywania swojej obecności oraz wykorzystywaniem luk w zabezpieczeniach systemów i aplikacji.

Równolegle z rozwojem zagrożeń następował rozwój metod ochrony antywirusowej. Programy antywirusowe, które początkowo opierały się głównie na prostym wykrywaniu znanych sygnatur wirusów, obecnie wykorzystują zaawansowane techniki heurystyczne, emulację środowiska uruchomieniowego, analizę zachowania programów oraz mechanizmy prewencyjne. Ochrona antywirusowa przestała być wyłącznie narzędziem reagującym na już istniejące zagrożenia, a stała się integralnym elementem strategii bezpieczeństwa informatycznego, obejmującej zarówno aspekty techniczne, jak i organizacyjne oraz prawne.

Celem niniejszej pracy licencjackiej jest kompleksowe omówienie problematyki wirusów komputerowych oraz metod ochrony antywirusowej. Praca ma na celu przedstawienie zarówno teoretycznych podstaw związanych z definicją i klasyfikacją złośliwego oprogramowania, jak i praktycznych aspektów jego działania, rozprzestrzeniania się oraz zwalczania. Szczególna uwaga została poświęcona ewolucji wirusów komputerowych, ich budowie, technikom infekcji oraz mechanizmom ukrywania się przed programami zabezpieczającymi. Równocześnie zaprezentowano rozwój i różnorodność narzędzi antywirusowych, a także stosowane przez nie techniki wykrywania i neutralizacji zagrożeń.

Zakres pracy obejmuje również analizę mniej oczywistych, lecz istotnych elementów zagrożeń informatycznych, takich jak konie trojańskie, robaki, spyware, hoaxy czy spam, które często

stanowią integralną część współczesnego krajobrazu cyberzagrożeń. Uwzględniono także aspekty prawne związane z tworzeniem i rozpowszechnianiem wirusów komputerowych, co pozwala spojrzeć na problem nie tylko z perspektywy technicznej, lecz również społecznej i prawnej. Istotnym elementem pracy jest ponadto omówienie najnowszych kierunków rozwoju złośliwego oprogramowania, w tym zagrożeń związanych z systemami plików, formatami multimedialnymi oraz urządzeniami mobilnymi.

Struktura pracy została zaprojektowana w sposób umożliwiający stopniowe pogłębianie wiedzy czytelnika. Początkowe rozdziały wprowadzają podstawowe pojęcia i klasyfikacje zagrożeń, następnie przedstawiona zostaje historia oraz techniczne aspekty działania wirusów komputerowych, by w dalszej części skupić się na metodach ochrony antywirusowej i przeglądzie wybranych rozwiązań programowych. Takie ujęcie tematu pozwala na całościowe zrozumienie problemu oraz ukazanie wzajemnych zależności pomiędzy rozwojem zagrożeń a ewolucją mechanizmów obronnych.

Praca adresowana jest zarówno do osób rozpoczynających swoją przygodę z zagadnieniami bezpieczeństwa informatycznego, jak i do czytelników posiadających podstawową wiedzę w tym zakresie, którzy pragną ją usystematyzować i poszerzyć. Autor ma nadzieję, że przedstawione treści przyczynią się do lepszego zrozumienia natury wirusów komputerowych oraz podkreślą znaczenie świadomego i odpowiedzialnego korzystania z technologii informacyjnych w dobie powszechnej cyfryzacji.

Jeśli chcesz zamówić pisanie pracy od podstaw, to zapraszamy na stronę [pisanie prac](#) - sprawdzony serwis