

Robaki i wirusy – mechanizmy ataków

Wprowadzenie.....6

Cel i zakres pracy.....7

1. Programy złośliwe.....9

1.1 Ogólna klasyfikacja zagrożeń.....9

1.2 Zagrożenia ze strony programów.....10

2. Krótka historia wirusów komputerowych.....12

3. Wirusy komputerowe.....14

3.1 Działanie wirusa komputerowego.....14

3.2 Tworzenie wirusów.....15

3.3 Struktura wirusa.....16

3.4 Języki programowania wykorzystywane do pisanie wirusów.....18

3.5 Najważniejsze kategorie wirusów.....19

3.5.1 Wirus pasożytniczy.....19

3.5.2 Wirus towarzyszący.....20

3.5.3 Wirus sektora ładowania.....21

3.5.4 Makrowirusy.....22

3.5.5 Tajny wirus.....22

3.5.6 Wirus poli i metamorficzny.....23

3.5.7 Fagi.....24

4. Klasyfikacja wirusów ze względu na sposób działania po

uruchomieniu.....25

- 4.1 Wirusy plikowe.....25
- 4.2 Wirusy nierezydentne.....25
- 4.3 Wirusy rezydentne.....26
 - 4.3.1 Szybkie infektory.....26
 - 4.3.2 Wolne infektory.....26

5. Wormy.....28

- 5.1 Worm sieciowy.....29
- 5.2 Rozprzestrzenianie się wormów.....29
 - 5.2.1 Wormy przenoszone przez sieć – wykorzystanie poczty elektronicznej.....30
- 5.3 Worm Internetu.....31
- 5.3 Robaki aktywne.....33

6. Intruzi jako zagrożenie bezpieczeństwa.....34

- 6.1 Intruzi.....34
- 6.2 Techniki właman.....35
- 6.3 Wykrywanie właman.....38

7. Inne zagrożenia ze strony programów.....41

- 7.1 Bakteria.....41
- 7.2 Bomba logiczna.....41
- 7.3 Boczne wejście.....42
- 7.4 Kon trojański.....42
 - 7.4.2 Rodzaje koni trojańskich.....47
 - 7.4.4.1 Trojany zartownisie.....48
 - 7.4.4.2 Trojany destrukcyjne.....48
 - 7.4.4.3 Konie wykradające hasła i poufne informacje.....48
 - 7.4.4.4 Kon trojański zdalnego dostępu.....49
- 7.5 Programy typu backdoor.....51

8. Zagrozenia wirusem komputerowym – obiekty atakowane.....53

- 8.1 Pliki wykonywalne COM.....53
- 8.2 Pliki EXE dla systemu DOS (stare EXE).....53
- 8.3 Pliki nowe EXE dla Windows (NE).....53
- 8.4 Pliki systemowe SYS.....54
- 8.5 Pliki wsadowe BAT.....54
- 8.6 Pliki DOC.....55
- 8.7 Pliki XLS.....56
- 8.8 Pliki ASM.....56
- 8.9 Sektory systemowe.....56
- 8.10 Główny rekord ładujący (MBR).....57
- 8.11 Rekord ładujący.....57
- 8.12 Jednostki Alokacji Plików (JAP).....58
- 8.13 Wirusy kombinowane.....59

9. Przenikanie wirusów do systemu komputerowego.....60

- 9.1 Sposoby przenikania wirusów.....60
- 9.2 Powstanie infekcji.....60
- 9.3 Nosniki wirusa.....62
 - 9.3.1 Dyski elastyczne.....62
 - 9.3.2 Wymienne dyski sztywne.....63
 - 9.3.3 Kasety z taśmy magnetycznej.....63
 - 9.3.4 Nosniki innego rodzaju.....63
 - 9.3.5 Sieci.....63
- 9.4 Drogi przenikania wirusów.....64
 - 9.4.1 Oprogramowanie pirackie.....64
 - 9.4.2 Biuletyny elektroniczne.....64
 - 9.4.3 Programy shareware.....65
 - 9.4.4 Programy publiczne.....65
 - 9.4.5 Rozproszone komputery osobiste.....65
 - 9.4.6 Dyskiety i CD-ROMy dołączane do czasopism komputerowych.....66
 - 9.4.7 Pracownicy firm serwisowych.....66

10. Metody zabezpieczen i walki z zakazeniem wirusowym.....67

10.1 Kontrolowanie dostepu do sieci.....67

10.1.1 Identyfikacja kanalów dostepu.....68

10.1.2 Scentralizowane sieciowe serwery plików.....68

10.1.3 Rozproszenie zaufania.....69

10.1.4 Przesylanie w sieciach z polaczeniami ogólnie dostepnymi.....70

10.2 Metody kontroli dostepu.....70

10.3 Usługi poczty elektronicznej.....71

11. Ochrona przed infekcja.....72

11.1 Przygotowanie na ewentualny atak.....73

11.2 Zapobieganie infekcjom wirusowym.....74

11.3 Wykrywanie wirusa.....74

11.4 Powstrzymanie wirusa.....76

11.5 Przywracanie sytuacji sprzed ataku wirusa.....77

12. Podstawowe narzedzia antywirusowe.....78

12.1 Programy podsuwane wirusom do zaatakowania w pierwszej kolejnosci.....78

12.2 Programy sledzace odwolania do systemu operacyjnego.....78

12.3 Programy obliczajace i sprawdzajace sumy kontrolne plików.....79

12.4 Programy detekcyjne.....79

12.5 Programy uodparniajace pliki przed zakazeniem.....79

12.6 Programy leczace, usuwajace wirusy z plików oraz dysków.....80

13. Wspólne elementy programów antywirusowych.....81

13.1 Skanery.....81

13.2 Monitory.....82

13.3 Szczepionki.....83

13.4 Programy autoweryfikujące.....83

13.5 Programy zliczające sumy kontrolne.....83

14. Techniki stosowane przez programy antywirusowe.....85

14.1 Skanowanie.....85

14.2 Heurystyczne wyszukiwanie wirusów.....85

14.3 Tryb krokowy.....85

14.4 Emulacja procesora.....86

14.5 Przynęty.....86

14.6 Pobieranie wielkości pamięci operacyjnej.....87

15. Ochrona przed poszczególnymi rodzajami wirusów.....88

15.1 Ochrona przed wirusami.....88

15.2 Ochrona przed robakami.....89

15.3 Ochrona przed koniami trojańskimi.....89

15.4 Ochrona przed furtkami pozostawionymi w systemie.....90

15.5 Ochrona przed bombami logicznymi.....90

16. Programy antywirusowe.....91

16.1 Skanery antywirusowe on-line.....91

16.2 Przegląd programów antywirusowych.....95

17. Przyszłość wirusów.....105

17.1 Wirusy dla różnych systemów.....105

17.2 Wirusy infekujące wewnątrzplikowo.....105

17.3 Wirusy zmienne genetycznie.....106

17.4 Wirusy infekujące nowe, nie infekowane dotychczas obiekty.....106

18. Charakterystyka wybranych wirusów.....107

18.1	Wirusy makrowe.....	107
18.1.1	Wirus makrowy Concept.....	107
18.1.2	Wirus Melissa.....	107
18.2	Wirusy rozruchowe.....	108
18.2.1	Wirus pakistanski, Brain.....	108
18.2.2	Wirus Michał Anioł.....	108
18.3	Wirusy systemu Windows.....	109
18.3.1	Wirus Boza.....	109
18.3.2	Wirus CIH (Czarnobyl).....	109
18.4	Wirusy linuxowe.....	110
18.4.1	Wirus Staog.....	110
18.4.2	Wirus Bliss.....	110
18.5	Wirusy pasożytnicze.....	111
18.5.1	Wirus Exorcist.....	111
18.6	Wirusy plikowe.....	112
18.6.1	Wirusy Stoned.....	112
18.7	Konie trojańskie.....	112
18.7.1	Trojanczyk NVP.....	112
18.7.2	Trojanczyk IconDance.....	112
18.7.3	Trojanczyk Feliz.....	113
18.7.4	Trojanczyk AOL4FREE.....	113
18.7.5	Kon trojański RegForm.....	114
18.7.6	Trojanczyk ProMail.....	114
18.7.7	Back Oriffice (B0).....	115
18.7.8	SubSeven.....	115
18.8	Robaki.....	116
18.8.1	Worm.Myparty.....	116
18.8.2	Worm.Kiray.....	117
18.8.3	Worm.Gigger.....	118
18.8.4	Robak Firkin.....	119
18.8.5	Robak Nimda.....	120

Podsumowanie.....122

Literatura.....123

