Metody włamań do systemów komputerowych

Wstęp

Bogusław Kluge, Karina Łuksza, Ewa Mąkosa

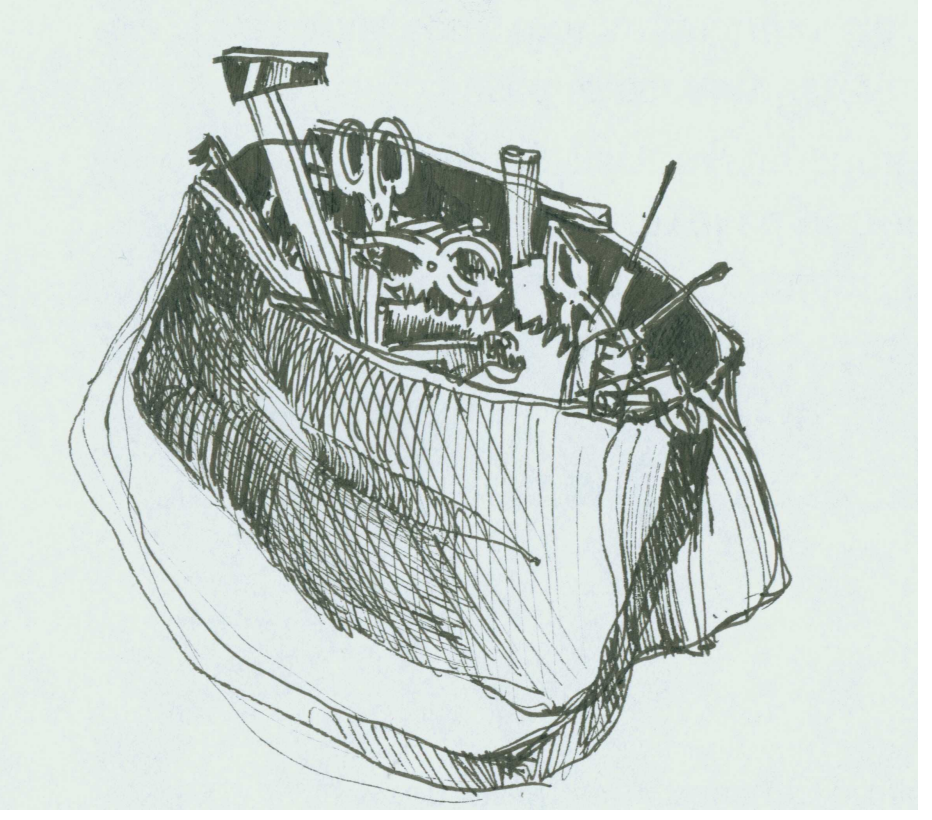
b.kluge@zodiac.mimuw.edu.pl, k.luksza@zodiac.mimuw.edu.pl,

e.makosa@zodiac.mimuw.edu.pl

Wstęp | Strategie ataku

Jakich metod używają hakerzy aby nas podejść? Zajrzyjmy do ich torby z narzędziami. Juz same nazwy sugerują dobrą zabawę:

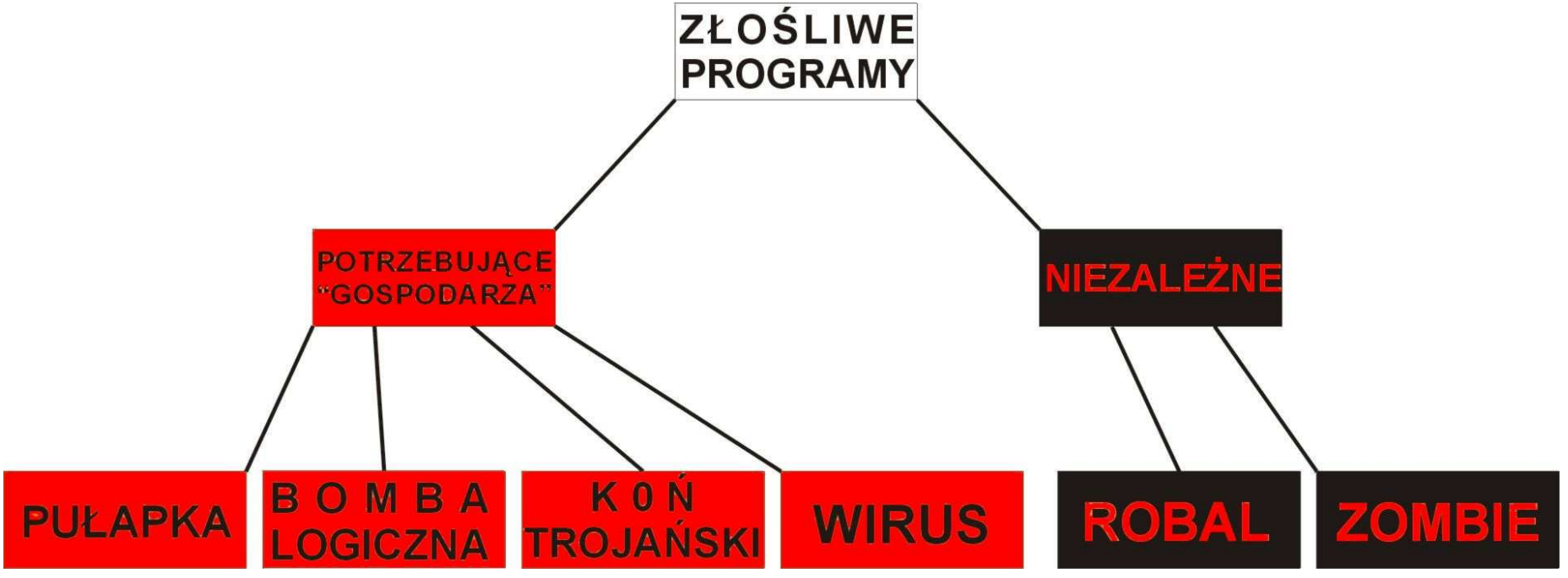
- wirusy
- robale
- bakterie
- konie trojańskie
- zombie
- bomby logiczne
- pułapki
- zrzucacze



- a przede wszystkim: błędy w aplikacjach..

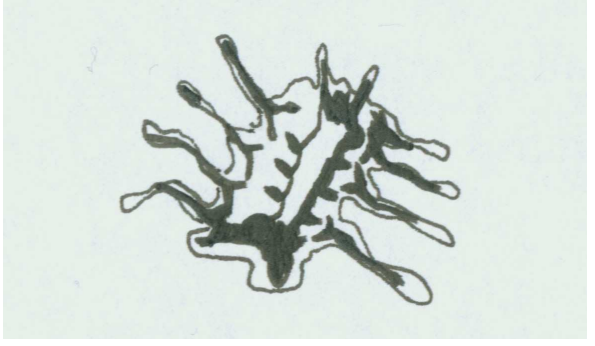
Wstęp | Podział

Złośliwe programy, ktore mogą nam zagrażać, możemy podzielić na takie, które potrzebują „gospodarza” (program, od którego zależą) oraz niezależne.



Wstęp | Wirus

„Unix. The world's first computer virus". *The Unix Haters Handbook.*



Program, który może "zarazić" inny program przekształcając go. Wirusy potrafią się również rozmnażać. Zakażone programy zarażają następne.. Można wyróżnić fazy życia wirusa:

- drzemanie: wirus jest bezczynny.
- propagacja: wirus rozprzestrzenia swoje kopie.
- aktywacja, spowodowana określonymi warunkami.
- wykonanie funkcji dla których jest przeznaczony.

Wstęp | Wirusy — klasyfikacja

- **pasożyt**: Dołącza się do plików wykonywalnych. Kiedy taki plik jest uruchamiany, pasożyt poszukuje następnych plików binarnych, aby je zarazić.
- **rezydent pamięci**: „Kwateruje się” w pamięci głównej podając się za program systemowy. Gdy mu się to uda, zaraża każdy wykonywany program.
- **boot sector**: Zaraża boot record. Rozprowadza się gdy system startuje z zakażonego dysku.
- **zamaskowany**: Ukrywa się przed rozpoznaniem przez oprogramowanie antywirusowe. Po wykonaniu pozostaje w pamięci. Stamtąd monitoruje i przechwytuje wywołania systemowe. Kiedy system próbuje otworzyć zainfekowany plik, zamaskowany wirus prezentuje jego “czystą” wersję.
- **polimorficzny**: Mutuje się z każdym zarażeniem — trudniejszy do rozpoznania jako jeden rodzaj wirusa.

Wstęp | Macro-wirusy

- wykorzystują makra
- Niektóre z makr, nazywane auto-wykonywalne, wykonują się w odpowiedzi na pewne wydarzenie, takie jak otworzenie pliku, rozpoczęcie aplikacji, czy nawet naciśnięcie pewnego przycisku.
- makro-wirus to kawałek replikującego się kodu wstawionego w auto-wykonywalne makro.
- gdy “jego” makro jest wykonywane, wirus kopiuje się do następnych plików, usuwa pliki itp.
- maj 2000: macro-wirus w Outlook’u (LOVELETTER)

Wstęp | Bakterie i „zrzucacze”

Nie należy mylić wirusów z **BAKTERIAMI**:

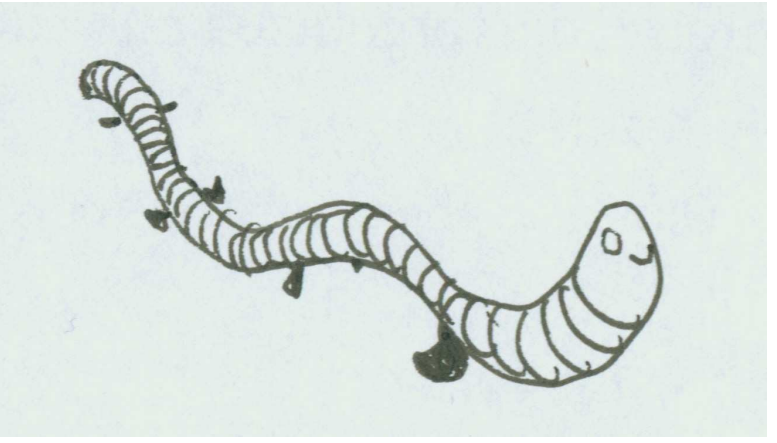
- Produkują własne kopie aby „zalać” system, wykorzystując całe jego zasoby, zarówno moc procesora jak i pamięć.
- Bakterie nie niszczą bezpośrednio żadnych plików.
- Ich jedynym celem jest replikowanie się.

Warto tu wspomnieć również o **„ZRZUCACZACH”** (jak inaczej przetłumaczyć „dropper”?)

- Program, który nie jest wirusem, ani nie jest nim zainfekowany.
- Jednak kiedy wykonywany, instaluje wirus w pamięci, dysku czy pliku.
- Napisany aby przenieść wirus.

Wstęp | Robale

ang. „worms”



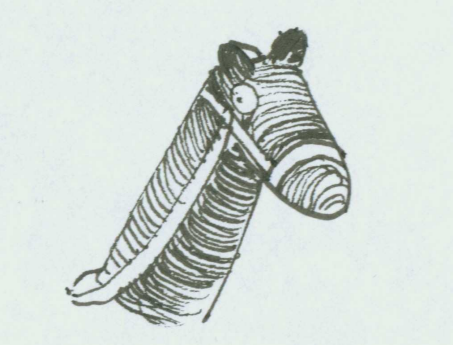
- Używają połączeń sieciowych do rozprzestrzeniania się, niekoniecznie po to, by modyfikować jakiekolwiek pliki na docelowych maszynach.
- Mogą przenosić oddzielny kod, a ten już może być bardziej niebezpieczny (np. wirus).

Wstęp | Zombie

- Program, który potajemnie przejmuje inny, podłączony do Internetu komputer, a następnie używa go do ataków. W ten sposób twórca zombie - właściwy haker jest trudny do ujęcia.

Wstęp | Koń trojański

Nazwa sloganowa: “trojan”.



- Kod dołączony do prawowitego programu, lub całkowicie go zastępujący.
- W sposób ukryty realizuje funkcje, nieznane użytkownikowi (i zapewne przez niego niepożądane). Oczywiste jest, iż funkcje te nie należą do „standardowych” funkcji programu.
- Program ten może być dowolny. „Trojana” da się zaszyć zarówno w programie logującym, jak i edytorze.

Wstęp | Bomba logiczna

ang. „logic bomb”

- Kod zaszyty, „uśpiony” w programie, uruchamiany tylko w specjalnych, sprzyjających warunkach.
- Uruchomiony, wykonuje funkcję, nie będącą żadną z funkcji programu, do którego bomba jest podłączona.
- Porównanie z bombą nasuwa się samo — ten program "eksploduje" na przykład gdy napotka określone pliki, bądź tylko wtedy, gdy uruchamia go pewien określony użytkownik.
- Zwykle podkładane przez programistów, którzy mają uprawniony dostęp do systemu.

Wstęp | Boczne drzwi

ang. „backdoors”

- Fragment kodu, który niezauważenie dla użytkownika wykonuje własne funkcje, zwykle z korzyścią dla autora programu.
- Znana jest sprawa programisty, który pisząc na zamówienie banku zapewnił sobie stały dochód — w obsługę transakcji wbudował odprowadzanie na swoje konto drobnej kwoty z zaokrągleń.
- Bardzo trudnym do wykrycia jest wykorzystanie kompilatora, który generuje standardowy kod wynikowy oraz boczne wejscie niezależne od kodu zródłowego.

Wstęp | Ale to nie wszystko

Wiele jest metod, sztuczek i strategii ataku, często wykorzystujących błędy systemu czy aplikacji, które nie tak łatwo dają się sklasyfikować. Oto te z metod, o których będziemy jeszcze chcieli opowiedzieć:

- Przepełnienie bufora.
- Dziwne łańcuchy formatujące.
- Sql injection.

Hakerzy mają jedną zaletę — nie sposób się przy nich nudzić...

Wstęp | Bibliografia

- http://www.cs.wright.edu/ pmateti/InternetSecurity/Lectures
- http://www.cs.umd.edu/ iftode/cs412/lectureNotes.htm (Wykład 14, Computer Security)
- Operating System Concepts, 6th Edition by Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, rozdziały 18 i 19 (po polsku: wydanie 5, rozdz. 19 i 20, dostępne w bibliotece)

Wstęp | Hakerzy ciągle pracują…