Robaki

Karina Łuksza k.luksza@zodiac.com.pl

Ewa Mąkosa e.makosa@zodiac.com.pl

Bogusław Kluge b.kluge@zodiac.com.pl

Ogólnie

Są to programy, które tworzą swoje własne kopie i przenoszą się za pomocą różnych połączeń sieciowych. W tym celu wykorzystują przede wszystkim dziury w atakowanych systemach i niefrasobliwość ich użytkowników.

W przeciwieństwie do wirusów nie potrzebują do rozmnażania się żadnego pliku nosiciela.

Budowa robaka

- Procedura instalacji w systemie
- Mechanizm dystrybucji
- Ciało robaka, czyli jego funkcje

Powstanie

Robaki stworzone zostały z myślą o wykonywaniu zdefiniowanych przez użytkownika zadań w środowisku rozproszonym.

Początkowo uznawano je za wydajny mechanizm przeprowadzania operacji sieciowych, ale wkrótce poważnym problemem okazało się zarządzanie nimi, a zwłaszcza kontrola ilości pracujących jednocześnie kopii programu.

Pierwsze robaki

- 1987 – pierwszy atak robaka *Christmas Tree Exec* na komputery mainframe IBM. Był to raczej koń trojański z umiejętnością powielania się.
- 1988 – *RTM* (autor Robert Tappan Morris) zaatakował przyłączone do Internetu systemy Sun i Dec Unix
- 1988 – *Father Christmas* w sieci DECnet, raportował o każdym udanym ataku.

- Większość robaków dedykowana jest na platformę Windows, ale są również robaki linuksowe (RedHat)
- Początkowo robaki pisane były w C++, teraz w językach wysokiego poziomu (Visual Basic, Delphi).
- Robaki w języku skryptowym
  - Robaki skryptowe zakodowane – wyglądają jak zwykłe pliki binarne, ale na ich końcu podłączona jest funkcja dekodująca. Po uruchomieniu robaka jest on najpierw rozkodowywany, a następnie wykonywany.

Kanały dystrybucji

- poczta elektroniczna
- IRC
- strony WWW
- Udostępnione zasoby komputera
- systemy wymiany komunikatów

Podmiana plików systemowych

Zapisanie kodu robaka pod nazwą jakiegoś często używanego programu i zachowanie oryginału pod inną nazwą. Przy uruchamianiu programu najpierw uruchamia się robak, który po wykonaniu się przekazuje sterowanie do prawidłowego programu.

Metoda wykorzystywana przez robaki typu EXE

Rejestracja jako program uruchamiany automatycznie podczas startu systemu

- Dodanie w rejestrze systemowym, w kluczu HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run ścieżki do programu.

Metoda wykorzystywana przez skrypty VBScript i Jscript, rozpowszechniane jako załączniki i pliki wykonywalne typu EXE.

- Umieszczenie kodu w katalogu *Autostart*.

Metoda stosowana przez robaki rozpowszechniające się za pomocą stron WWW i maili w formacie HTML oraz robaki atakujące komputer przez udostępnione zasoby.

Jest to zazwyczaj forma pośrednia. Docelowo program jest rejestrowany w rejestrze systemu.

Przechwytywanie plików

Kojarzenie rozszerzeń plików z robakiem. Gdy użytkownik próbuje uruchomić plik danego typu, system uruchamia robaka, gdzie wybrany plik jest parametrem wywołania.

Na początku wykonywany jest kod robaka, a następnie oryginalny program.

Opis

- Najczęściej stosowany sposób rozpowszechniania robaków internetowych, czyli podszywanie się pod ciekawy załącznik.
- Do przeprowadzenia wysyłki wykorzystuje najczęściej program Outlook lub Outlook Express.
- Na atakowanym komputerze robak wykona się niezależnie od odbierającego pocztę programu, jeśli tylko użytkownik otworzy załącznik.
- Schemat działania robaka:

1. Skopiowanie załącznika do katalogu systemowego
2. Instalacja w systemie
3. Funkcja rozpowszechniająca przesyłkę
   a) Uruchomienie Outlooka
   b) Odczytanie list adresowych
   c) Na każdy adres z każdej listy adresowej wysyłamy maila z zachęcającym do przeczytania tytułem, w załączniku którego dołączony jest kod robaka.
4. Ujawnienie działania

Outlook

- Domyślnie otwiera wszystkie załączniki bez pytania.

- Rejestruje się jako serwer OLE (mechanizm pozwalający na osadzanie obiektów pochodzących z różnych źródeł w jednym dokumencie, co pozwala na wykorzystanie możliwości oferowanych przez różne programy bez ich otwierania), co umożliwia przeprowadzenie automatycznej przesyłki przez robaki.

Netscape Mail

- Pyta użytkownika, co zrobić z załącznikiem. Domyślnie zapisuje go na dysk, a nie uruchamia.

- Nie rejestruje się jako serwer OLE

Opis

- Mniejszy zasięg niż dystrybucja poprzez e-mail
- **Zasada działania**: dodanie do pliku konfiguracyjnego skryptu, który będzie automatycznie wysyłał plik z kodem robaka do osób znajdujących się na kanale.
- Wejście nowej osoby na kanał wywołuje zdarzenie JOIN, które jest przez program przechwytywane. Do procedury obsługi zdarzenia dopisana zostaje próba wysłania robaka do osoby, której pseudonim uzyskaliśmy.
- mIRC i Pirch – programy wykorzystywane przez robaki

Problemy

- Domyślna konfiguracja programu mIRC powoduje ignorowanie odbierania wszystkich plików innych niż obrazki, pliki dźwiękowe i archiwa ZIP.
- Jeśli nawet użytkownik wyłączy powyższą blokadę, to i tak będzie ostrzegany o przesyłce i będzie musiał na nią zezwolić.
- Po przesłaniu robaka jest on zapisywany na dysku w wybranym katalogu (domyślnie do podkatalogu *download*). Dopiero gdy użytkownik wejdzie do katalogu *download* i do tego uruchomi przesłany plik – robaka, akcja się powiedzie.

Sposoby działania (Atak tylko poprzez przeglądarkę *Internet Explorer*)

1. Wykorzystanie plików HTML tylko do transportu robaków skryptowych.
   - W momencie oglądania strony wykona się skrypt, którego zadanie polega na zapisaniu kodu robaka w osobnym pliku i uruchomieniu go.
   - Takie robaki w celu rozpowszechniania mogą:
     - powielać się na wszystkich znalezionych w systemie dyskach (również zamapowane katalogi innego komputera)
     - dopisywać swój kod do znalezionych plików (wirusy). Po zainfekowaniu plików należących do drzewa serwera WWW, program może uruchomić się na każdym komputerze, na którym będzie przeglądany dany plik.
2. Całe ciało pliku HTML jest robakiem. Kod robaka jest zawarty pomiędzy znacznikami <script></script> i obudowany zawartością dokumentu HTML.
   - Różnica polega na sposobie odczytu własnej zawartości. Taki robak pobiera swój kod po prostu odczytując ciało dokumentu HTML.

Wada: Przy tworzeniu obiektu Scripting.FileSystemObject umożliwiającego wykonanie operacji na systemie plików przeglądarka wyświetli ostrzeżenie i zażąda zgody użytkownika na stworzenie tych obiektów.

3. (Tylko dla przeglądarek 4.0 – 5.0)
   - Metoda wykorzystuje klasę Scriptlet.TypeLib umożliwiającą wykonywanie zaawansowanych operacji systemowych takich jak np. tworzenie plików.
     - Dokument tworzy obiekt klasy Scriptlet.TypeLib. Dzięki niemu będzie mógł umieścić plik zawierający kod robaka w katalogu *Autostart*.
     - Przy następnym uruchomieniu komputera kod robaka się wykona.
   - Przeglądarki *Internet Explorer* powyżej wersji 5.5 zażądają zgody na utworzenie obiektu klasy Scriptlet.TypeLib.

Słabe strony przeglądarki *Internet Explorer*

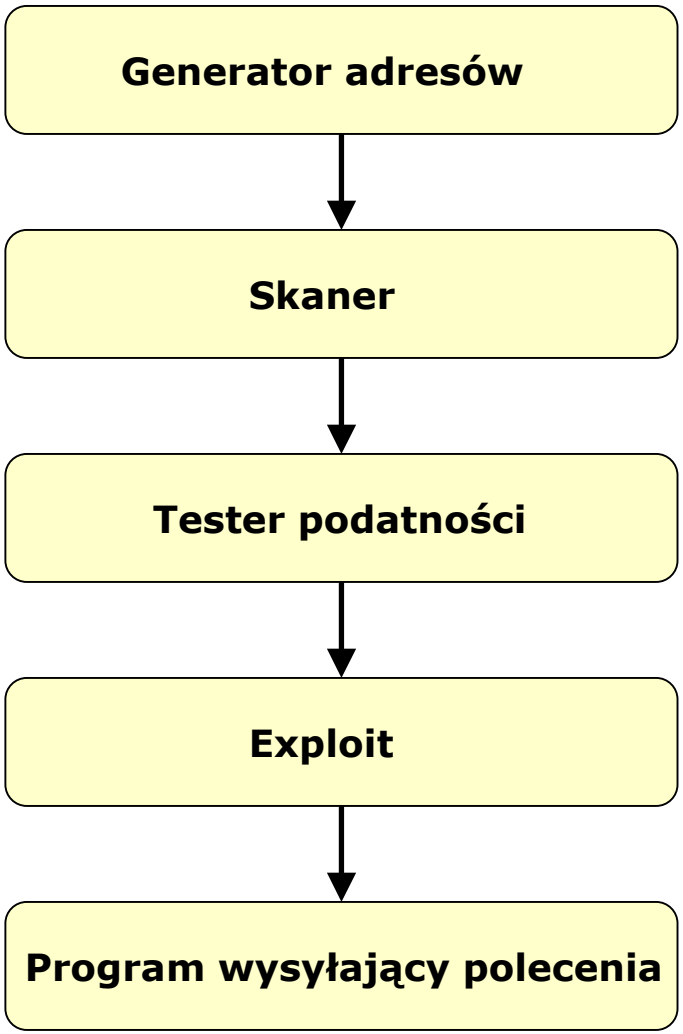
- Obsługa skryptów Jscript i VBScript, które mogą mieć dostęp do wszystkich elementów systemu za pomocą obiektów ActiveX. W przeciwieństwie do nich skrypty JavaScript operują jedynie na środowisku przeglądarki.
- Ogólnie umożliwia osadzanie na stronach obiektów ActiveX.
- Mocno zintegrowana z systemem Windows.

Wykorzystanie udostępnionych zasobów

Jeśli udostępniony został katalog systemowy komputera, to robak skopiuje się do Autostartu i zostanie uruchomiony przy następnym uruchamianiu systemu.

Programy wymiany komunikatów

Np. Netscape Messenger



Schemat ataku

1. Generowanie adresów IP – wybieramy jakąś metodę generowania adresów miejsc, do których chcemy się włamać.
2. Skaner – sprawdza, czy wygenerowane adresy reprezentują hosty w danej podsieci.
3. Tester podatności na atak – sprawdza, czy atak się powiedzie (czy cel jest podatny na sposób ataku – wyszukuje dziury)
4. Exploit – Dokonuje włamania, czyli wykorzystuje dziurę. Efektem ataku powinno być umieszczenie na atakowanym komputerze nasłuchującej powłoki.
5. Wysłanie komend do zdobytego hosta:
   - nasłuchująca powłoka na atakowanym komputerze powinna ściągnąć całego robaka i uruchomić go.
   - Wysyłamy kod robaka (ftp, lynx) pod wygenerowane adresy IP.
   - Uruchamiamy program, który wysyła polecenia odpakowania i uruchomienia robaka.

- Wykorzystywał luki w systemach bezpieczeństwa systemu UNIX i ułatwienia w dzieleniu zasobów sieci lokalnej.
- Składał się z dwóch części:
  - program haczący – po zainstalowaniu w atakowanym systemie łączył się z maszyną, z której pochodził i ściągał kopię robaka.
  - program główny – wyszukiwał następne maszyny łatwo dostępne z atakowanego komputera.
- Metody dystrybucji:
  - *rsh* – program umożliwiający łatwe wykonywanie zadań zdalnych. Określa specjalne pliki z wykazami par – nazwa komputera, nazwa rejestracyjna. Robak przeszukiwał te pliki i wynajdywał stanowiska, na których mógł się zdalnie zalogować bez podawania hasła.
  - *finger* – robak wykorzystywał błąd przepełnienia bufora i w wyniku czego był kierowany do procedury, która próbowała uruchomić shella.
  - *sendmail* – tu również wykorzystana została dziura, dzięki której robak mógł wywoływać polecenia wysyłające kopię programu haczącego i rozpoczynających jego wykonanie na atakowanym komputerze.
- Łamanie haseł – następny etap, czyli zyskiwanie dostępu do kolejnych kont. Robak wypróbowywał zestaw prawdopodobnych i popularnych haseł. Jeśli mu się udało to dalej przez *rsh*...

Ogólne zasady

- Nie otwierać nie oczekiwanych plików, zwłaszcza tych z rozszerzeniami VBS, SHS lub PIF, które prawie nigdy nie są używane przez normalne programy.
- Aktualizować oprogramowanie instalując patch'e, aby załatać nowo odkryte dziury.
- Do oglądania niepewnych stron nie używać przeglądarki *Internet Explorer.*
- Nie akceptować odbioru plików, które ktoś wysyła za pomocą systemu wymiany komunikatów lub IRC, jeśli takiego pliku się nie spodziewamy
- Nadać minimalne prawa do katalogów w systemach Windows NT/2000
- Nie udostępniać katalogu głównego ani katalogów systemowych

- Software 2.0, nr 9 (81) wrzesień 2001 – Jonathan Kaźmierczak „Skryptowe robaki internetowe”
- Software 2.0, nr 9 (93) wrzesień 2002 – Tomasz Potęga „Robaki sieciowe”
- Abraham Silberschatz, Peter B. Galvin „Podstawy systemów operacyjnych”