O analogiach pomiędzy bezpieczeństwem sieciowym a światem przyrody

Elżbieta Rzeszutko
Politechnika Warszawska

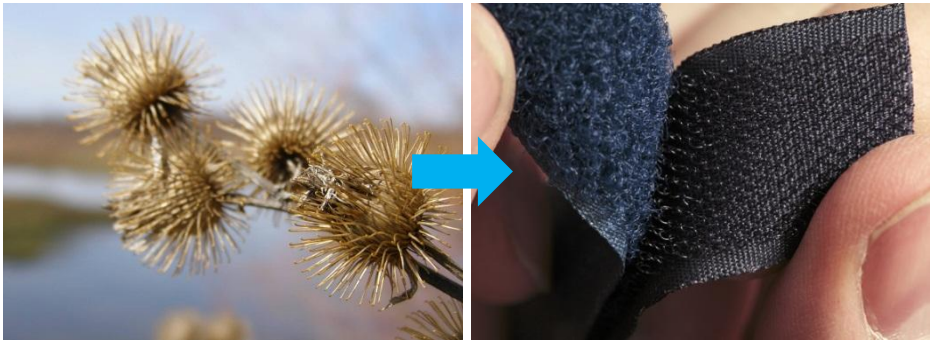
SCS 2014

27 listopada 2014

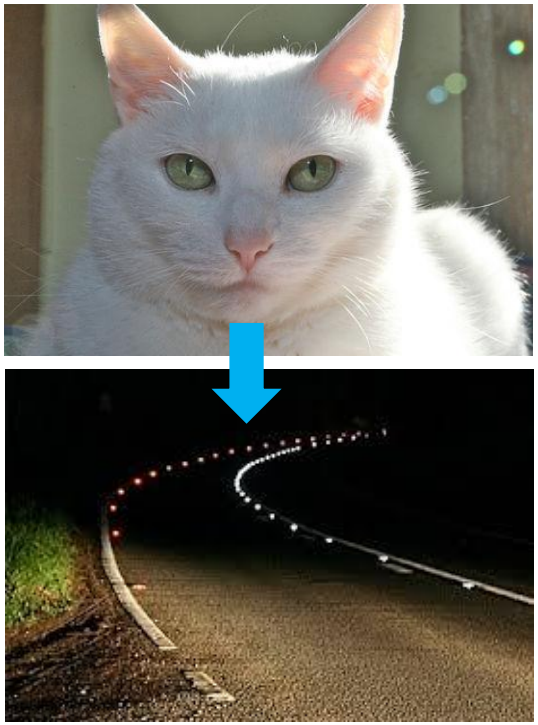
Inspiracja światem roślin i zwierząt (1/2)

- Od lat **obserwacja środowiska naturalnego** stanowi inspirację dla wynalazców i naukowców

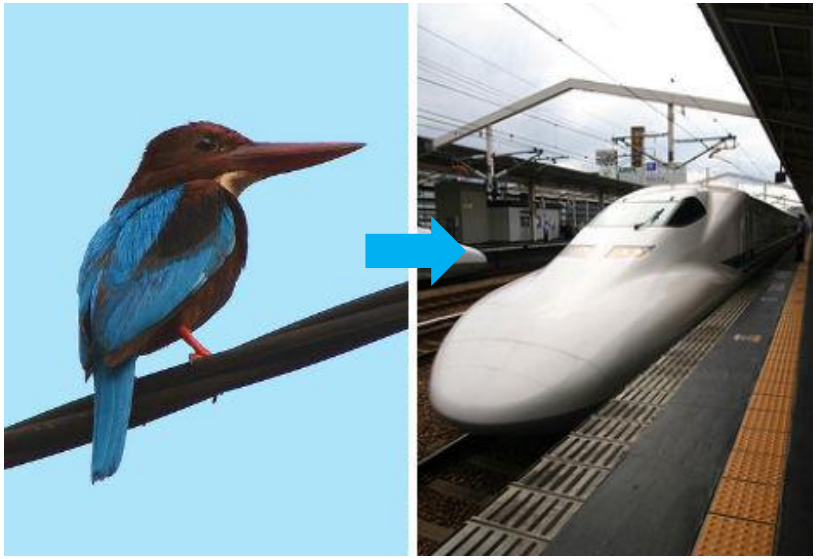
Zapięcie „na rzepy”



„Kocie oczy”

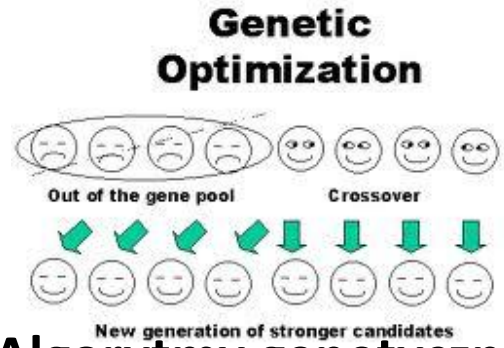


Kształ dziobu ultraszybkiego pociągu

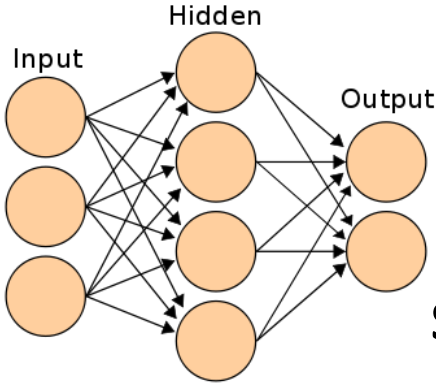


Inspiracja światem roślin i zwierząt (2/2)

- Opracowywane są zaawansowane techniki obliczeniowe oraz technologie sieciowe **inspirowane zjawiskami znanymi z natury**

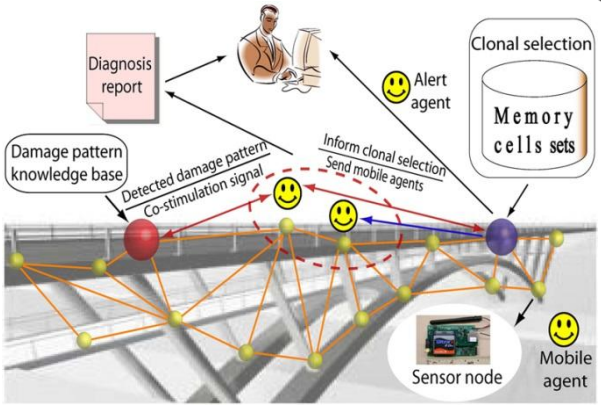


Algorytmy genetyczne



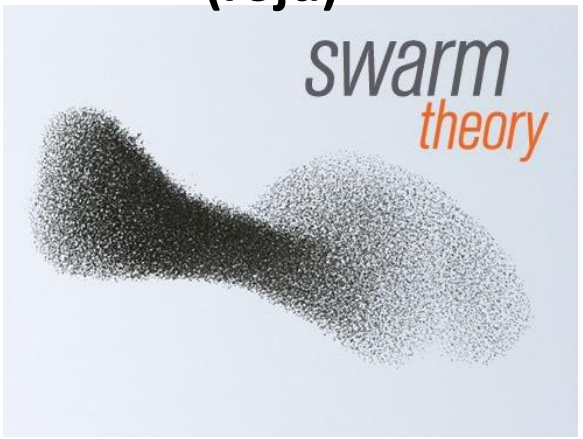
Sieci neuronowe

Sieci sensorowe



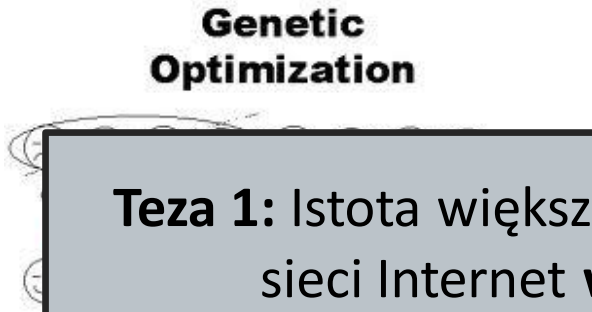
Sztuczne systemy immunologiczne

Systemy rozproszonej inteligencji (roju)



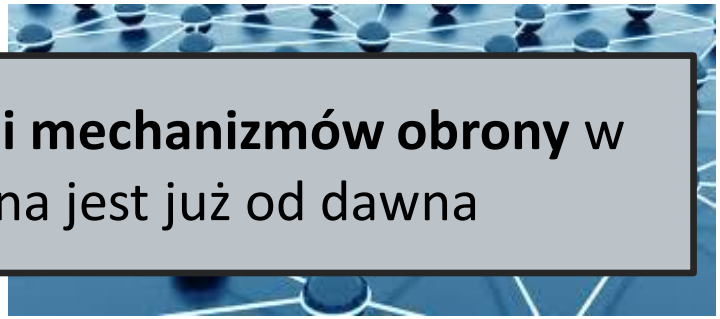
Inspiracja światem roślin i zwierząt (2/2)

- Opracowywane są zaawansowane techniki obliczeniowe oraz technologie sieciowe **inspirowane zjawiskami znanymi z natury**



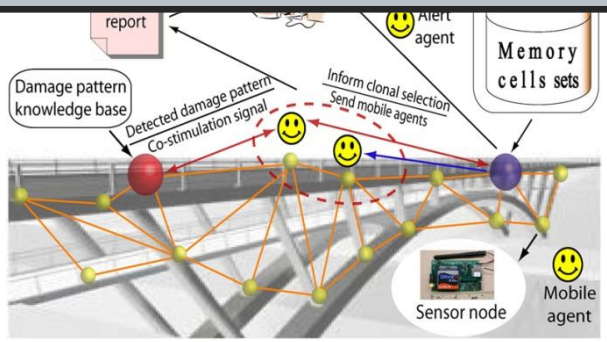
Algorytmy genetyczne

Sieci sensorowe

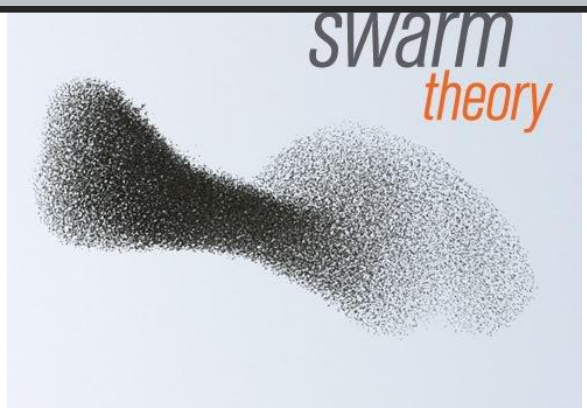


Teza 1: Istota większości **znanych ataków i mechanizmów obrony** w sieci Internet **w przyrodzie** spotykana jest już od dawna

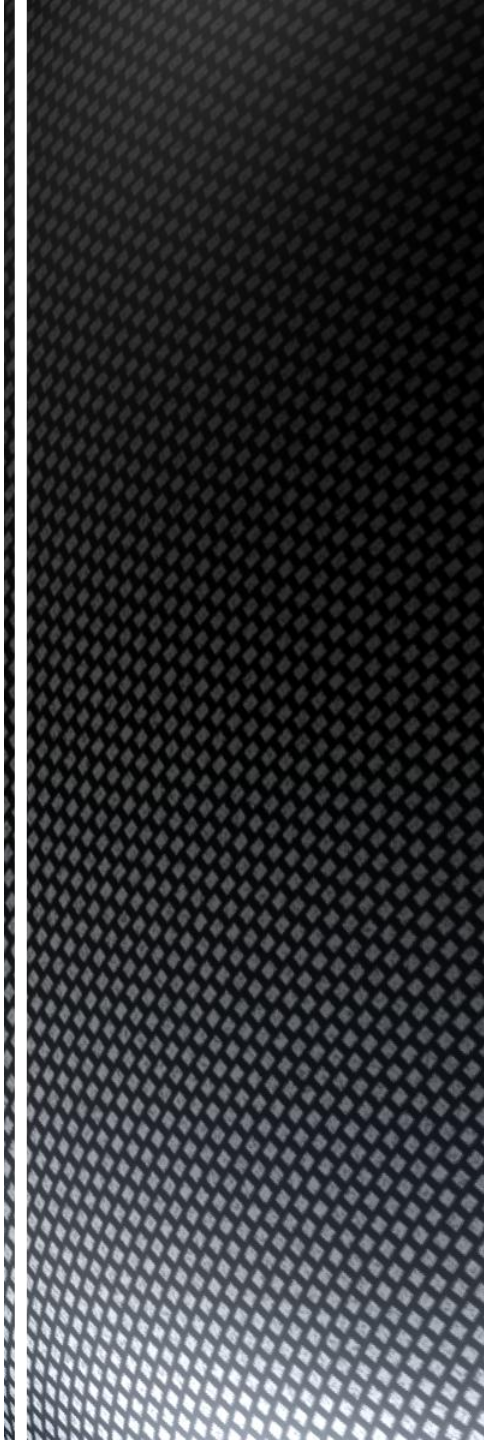
Teza 2: Zarówno w naturze jak i w Internecie obserwujemy **ewolucję technik ofensywnych** oraz odpowiadających im **technik defensywnych** (**wyścig zbrojeń**)



Sztuczne systemy immunologiczne



Techniki ofensywne



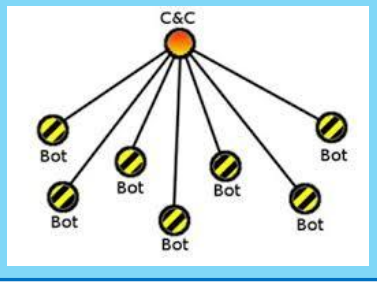
Etapy typowego ataku sieciowego w Internecie

Etap I:

Instalacja złośliwego oprogramowania

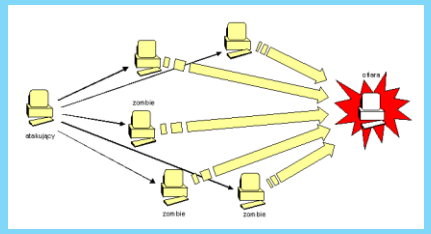
Etap II:

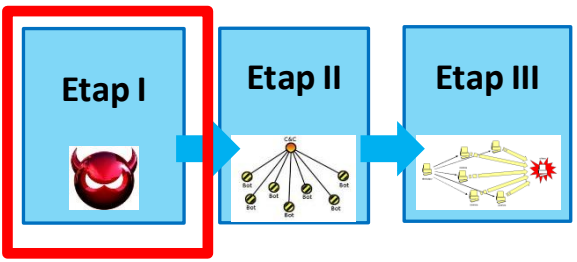
Formowanie sieci botnet



Etap III:

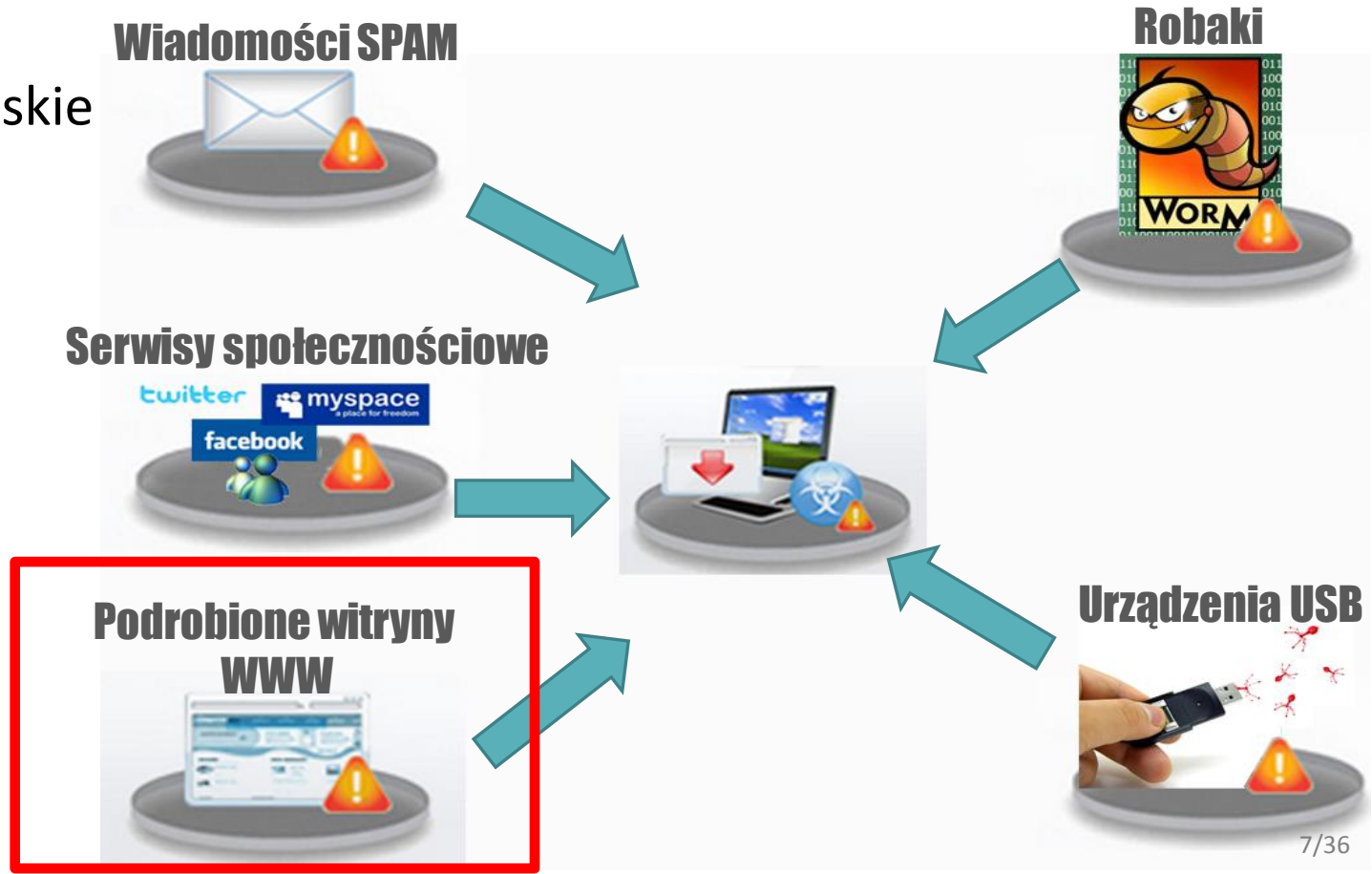
Przeprowadzenie ataku

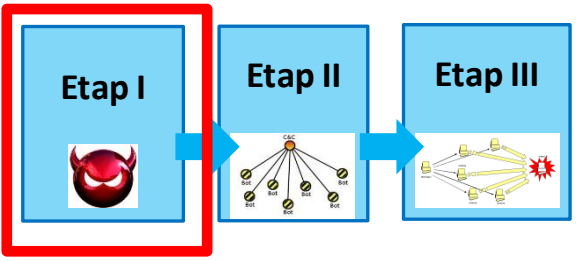




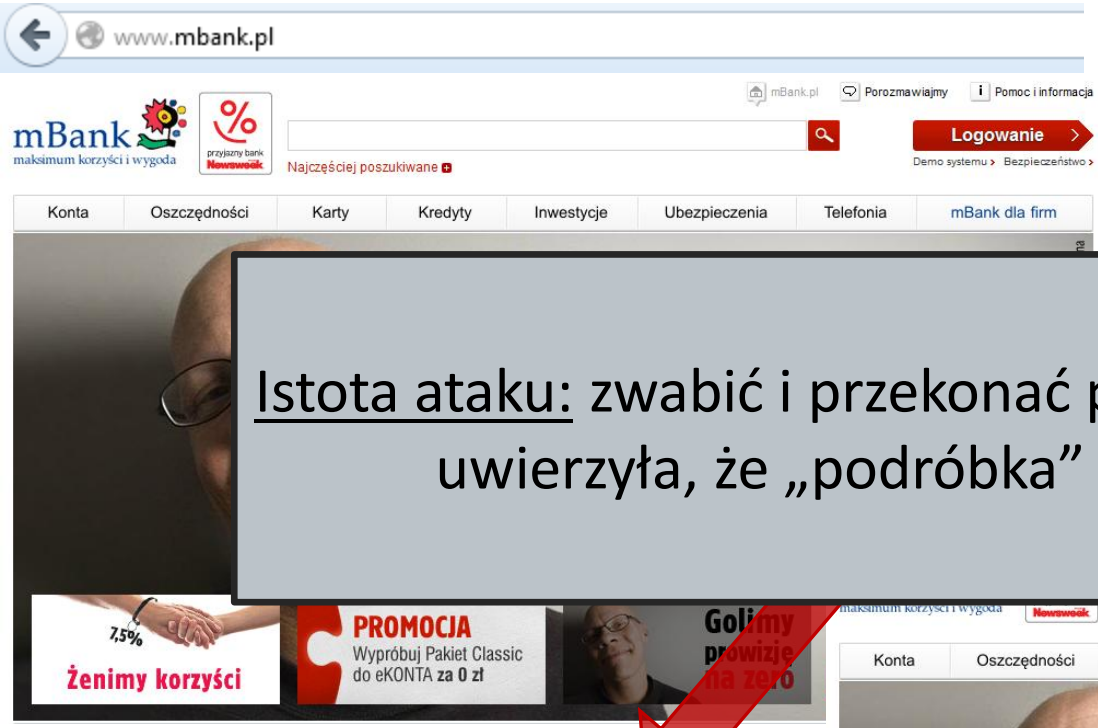
Złośliwe oprogramowanie (malware) i sposoby infekcji

- **Rodzaje złośliwego oprogramowania:**
  - Wirusy (!)
  - Robaki (!)
  - Konie trojańskie
  - Spyware
  - ...

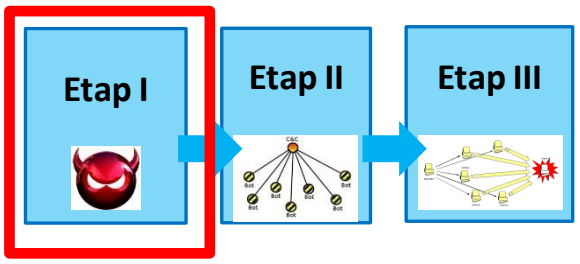




Przykład strony phisingowej

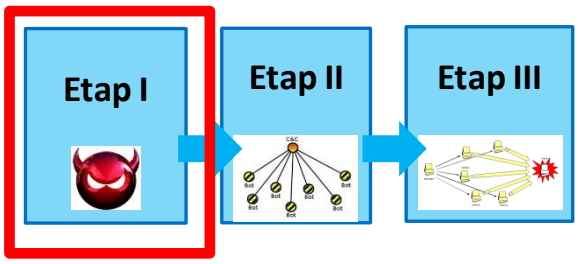


Istota ataku: zwabić i przekonać potencjalną ofiarę, aby uwierzyła, że „podróbka” jest oryginałem



Phising w naturze

- **Żabnica** (*Lophius piscatorius*) nazywana również „diabłem morskim” – rodzaj ryby głębinowej występującej na wybrzeżach Europy i północno-zachodniej Afryki
- Jej jedyną widoczną częścią ciała jest **wijący się jak robak mięsisty wyrostek na końcu długiej wędki wystającej ze szczytu głowy**
- Kiedy podpływa zdobycz, żabnica kusi ją wabikiem w pobliże swojej zamaskowanej paszczy

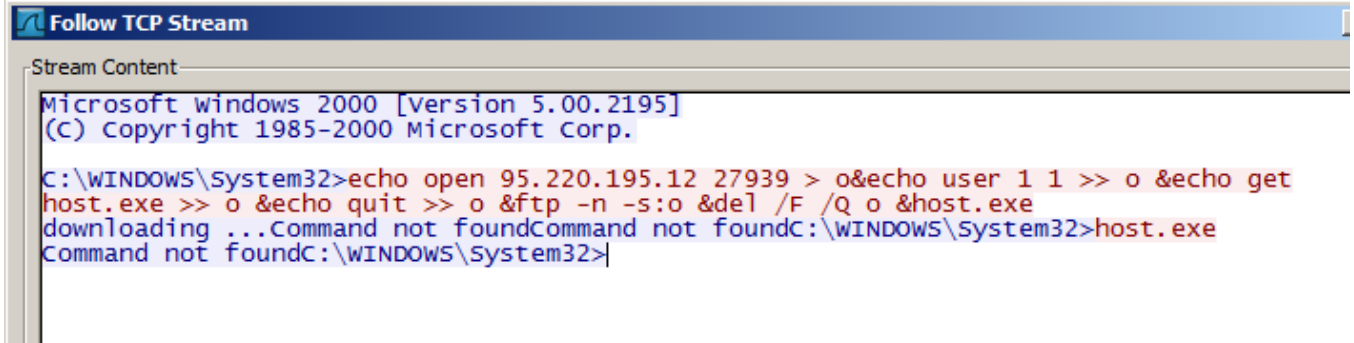


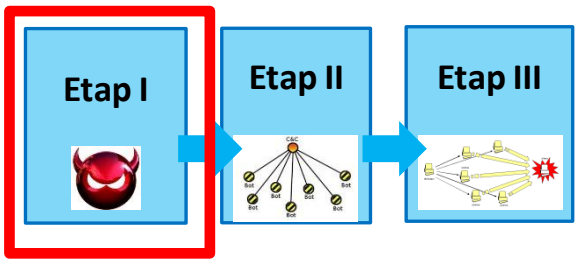
Złośliwe oprogramowanie: robak

- **Robak (worm)** - samo propagujący się kod, który do rozprzestrzeniania się wykorzystuje sieć Internet

Cechy:

- **Nie potrzebuje interwencji użytkownika**, aby przenosić się pomiędzy infekowanymi systemami
- **Wykorzystuje exploit** – dedykowany program, specjalnie spreparowaną sesja komunikacyjnę, itp. mające na celu wykonanie nieautoryzowanego kodu i zwiększenie uprawnień atakującego poprzez wykorzystanie podatności, błędu
- Często prowadzi do **wyłączenia operujących mechanizmów bezpieczeństwa** (np. systemów antywirusowych, czy firewalli)





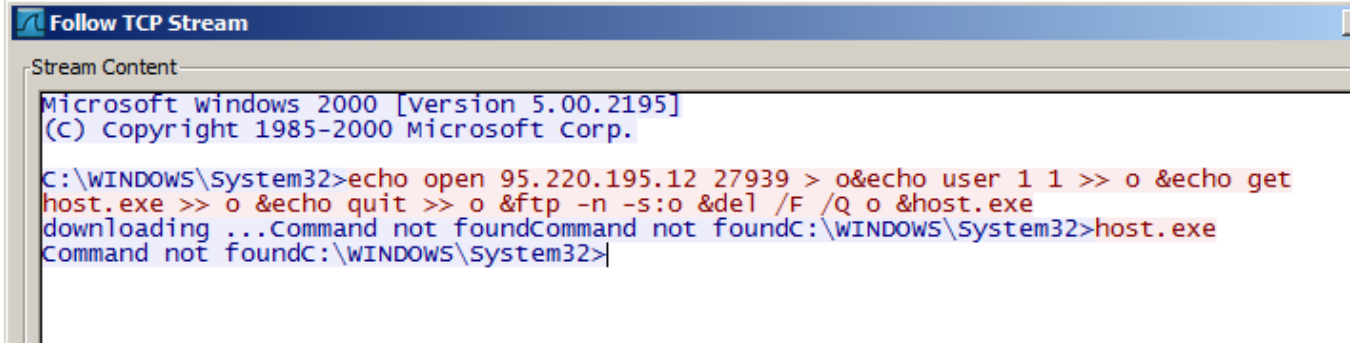
Złośliwe oprogramowanie: robak

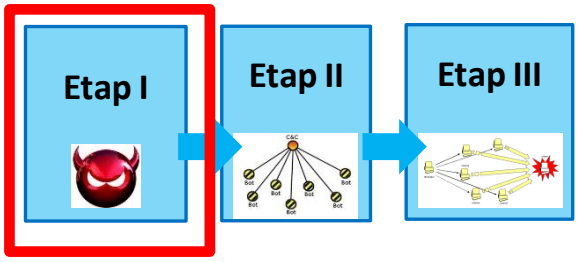
- **Robak (worm)** - samo propagujący się kod, który do rozprzestrzeniania się wykorzystuje sieć Internet

Cechy:

- [illegible] między [illegible]
- [illegible] anie [illegible] poprzez wykorzystanie podatności, błędu
- Często prowadzi do **wyłączenia operujących mechanizmów bezpieczeństwa** (np. systemów antywirusowych, czy firewalli)

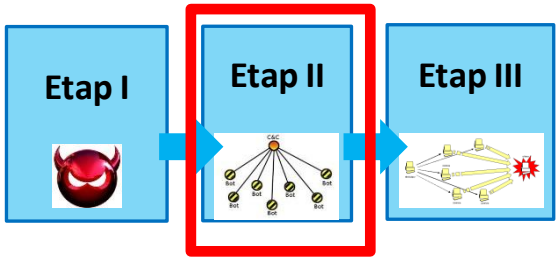
Cecha robaka: zablokowanie operujących mechanizmów zabezpieczeń





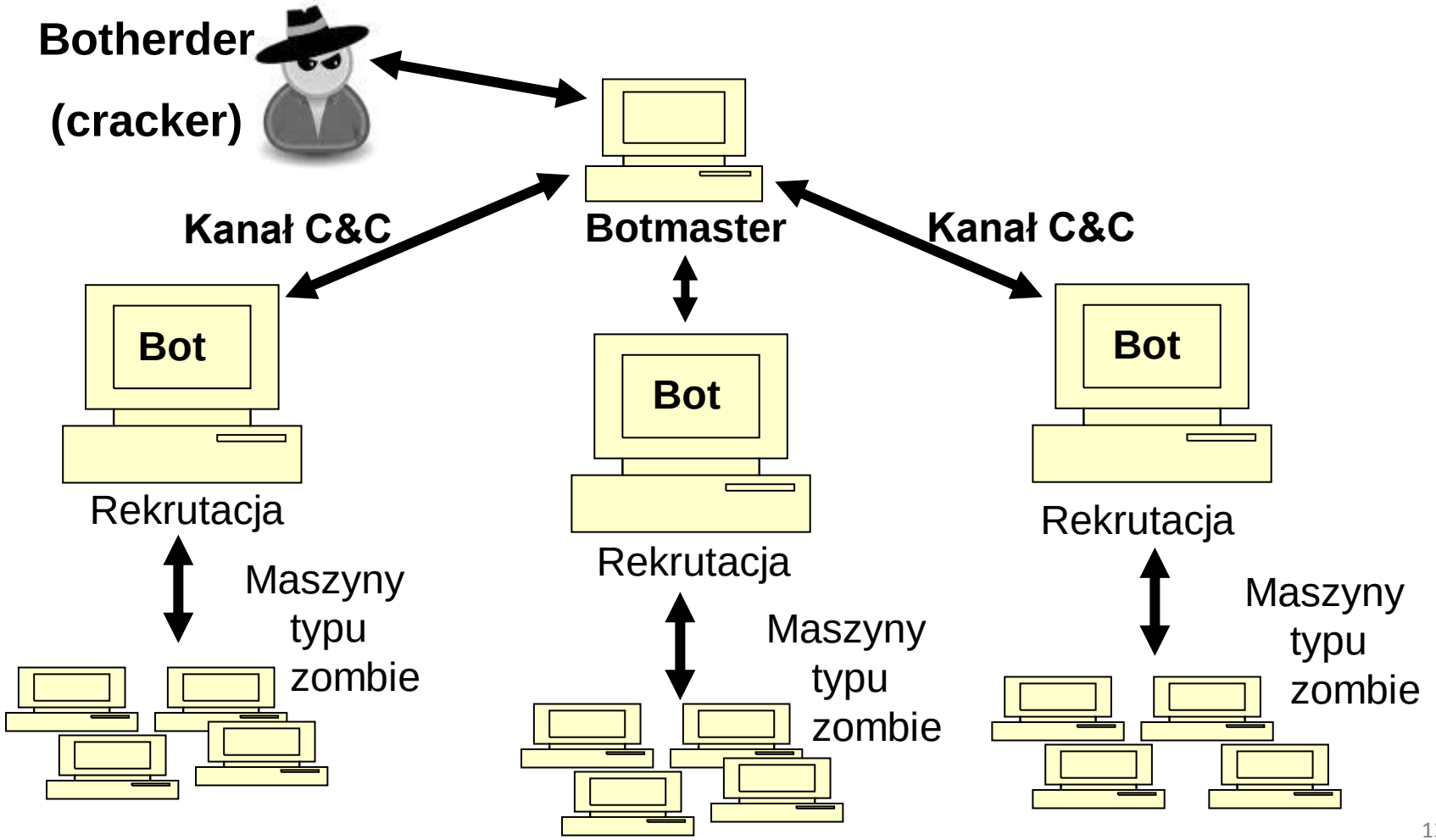
Celowe wyłączanie mechanizmów obronnych w naturze

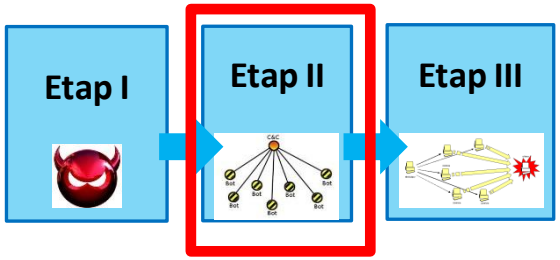
- Bez względu na strategię polowania wszystkie **pająki** wykorzystują **jad**, żeby unieruchomić ofiarę
- Posiadają one masywne szczękoczułki, dwuczłonowe, zakończone ruchomym pazurem, do którego uchodzi przewód jadowy
- Podczas ataku pająki **wbijają szczękoczułki w ofiarę** i wprowadzają jad, który ją paraliżuje uniemożliwiając obronę oraz ucieczkę



Podstawowa architektura i działanie sieci botnet

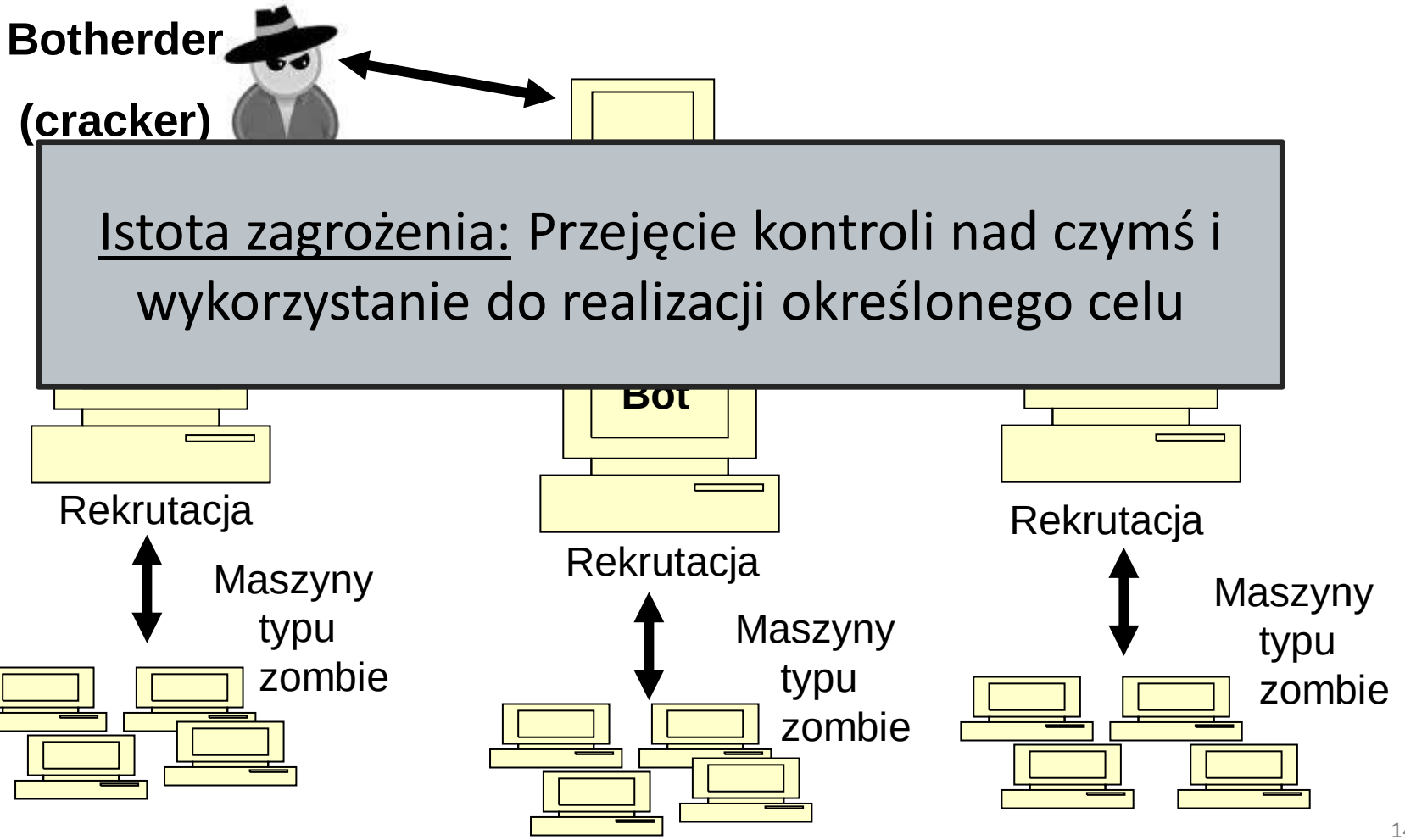
- **Botnet** jest siecią maszyn-zombie, czyli maszyn będących pod kontrolą atakującego (bez wiedzy ich użytkowników)

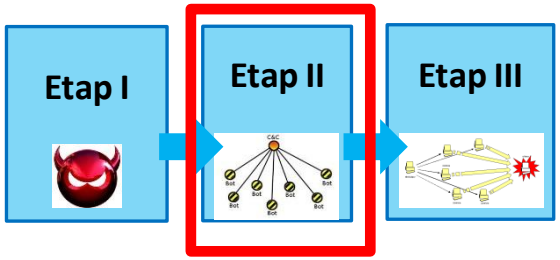




Podstawowa architektura i działanie sieci botnet

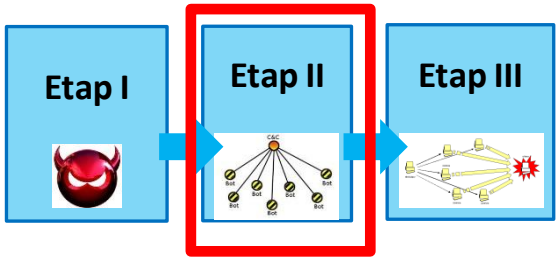
- **Botnet** jest siecią maszyn-zombie, czyli maszyn będących pod kontrolą atakującego (bez wiedzy ich użytkowników)





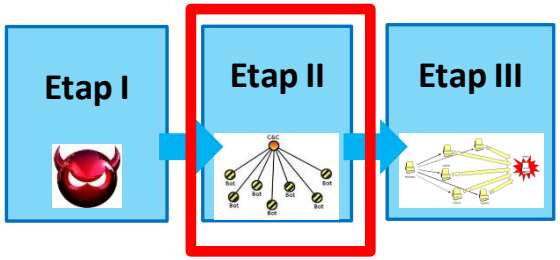
Sieci botnet w naturze

- Gatunek grzybów z rodziny Ophiocordycipitaceae zwany **„grzybem zombie” -** potrzebuje do rozwoju odpowiedniej temperatury i wilgotności oraz odległości od gleby
- Zarodniki grzyba atakują mrówkę i rozrastając się **zmieniają sposób, w jaki reaguje ona na feromony**
- Zainfekowana ofiara (**mrówka zombie**) szuka idealnych warunków dla rozwoju pasożyta wchodzi na drzewo i na odpowiedniej wysokości wbija się żuwaczką w liść i obumiera
- Grzyb przerasta ciało mrówki z tyłu jej głowy wypuszczając **szypułkę, która, pękając, rozsiewa zarodniki, które infekują kolejne mrówki**
- Na drzewach można spotkać wręcz **„mrówcze cmentarzyska”** - nawet 20 do 30 mrówek na metr kwadratowy



Sieci botnet – ukryta komunikacja

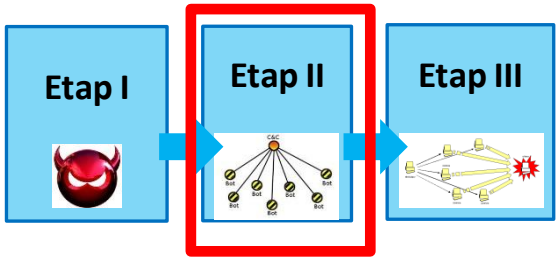
- Coraz częściej do komunikacji w kanale C&C (Command & Control) sieci botnet wykorzystywane są **techniki steganograficzne**
- Techniki ukrywania informacji stosuje się, aby **zamaskować przesyłane komendy** pomiędzy „zarządcą” sieci botnet i maszynami zombie
- Ostatnie przykłady: robak **Duqu** oraz **Alureon**



Sieci botnet – ukryta komunikacja

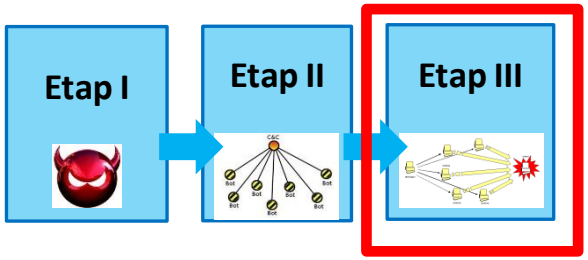
- Coraz częściej do komunikacji w kanale C&C (Command & Control) sieci botnet wykorzystywane są **techniki steganograficzne**
- Techniki ukrywania informacji stosuje się, aby **zamaskować prze**zynami zom
- Osta

Istota: zapewnienie możliwości prowadzenia ukrytej komunikacji



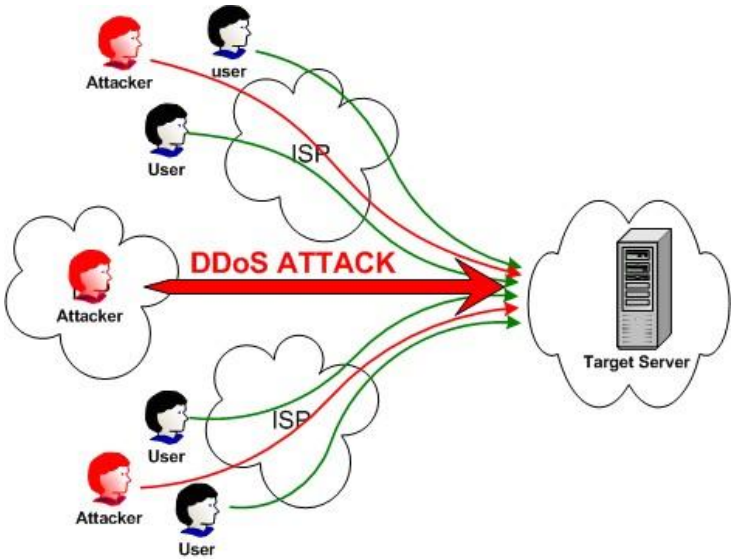
Ukryta komunikacja w naturze

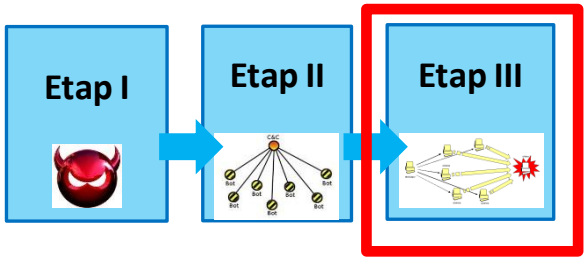
- **Wyraki filipińskie** (*Tarsius syrichta*) – rodzina drapieżnych ssaków naczelnych z rodziny małpiatek żyjących na Filipinach
- Są w stanie usłyszeć dźwięki o częstotliwości nawet **do 91 kHz** i generować dźwięki o częstotliwości **70 kHz** (najwyższe wartości wśród ssaków)
- Pozwala im to na prowadzenie **ultrasoniczej, ukrytej komunikacji**, dzięki której są w stanie informować się o zbliżających się drapieżnikach, czy potencjalnych zdobyczach



Ataki Rozproszonej Odmowy Usługi

- **DDoS (Distributed Denial of Service)** - uniemożliwienie przez atakujących korzystania z określonej usługi prawowitym użytkownikom
- Koncentruje się przede wszystkim na:
  - Wyczerpaniu zasobów **łączności sieciowej** np. pasma lub **urządzeń sieciowych** np. buforów, CPU
  - Przesyłanie celowo danych w **nieprawidłowej postaci** np. zbyt dużych rozmiarów pakietów, nachodzących na siebie



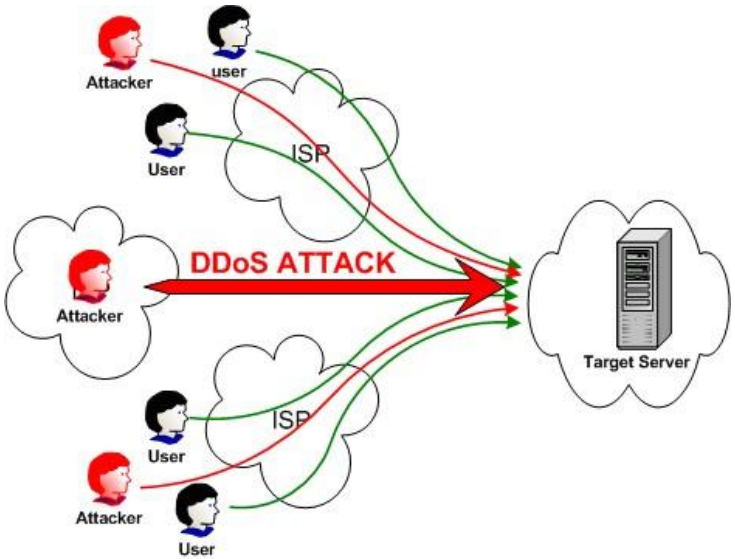


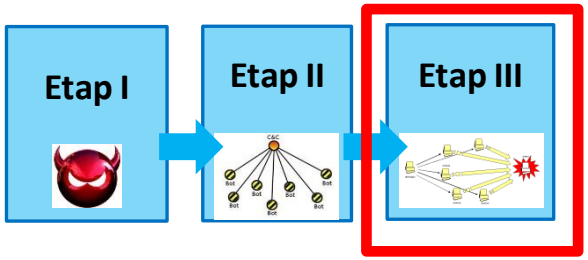
Ataki Rozproszonej Odmowy Usługi

- **DDoS (Distributed Denial of Service)** - uniemożliwienie przez atakujących korzystania z określonej usługi prawowitym użytkownikom
- Koncentruje się przede wszystkim na:
  - **ądzeń**
  - t dużych

Istota ataku: prawowity użytkownik nie ma możliwości skorzystania z określonego zasobu

rozmiarów pakietów, nachodzących na siebie

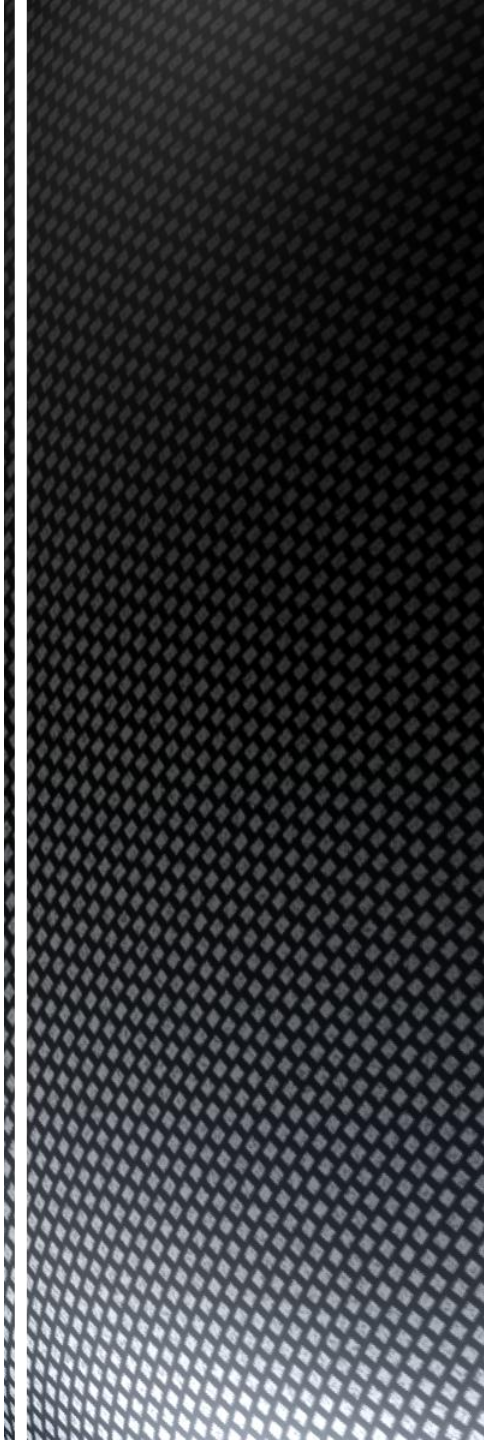




Ataki DDoS w naturze

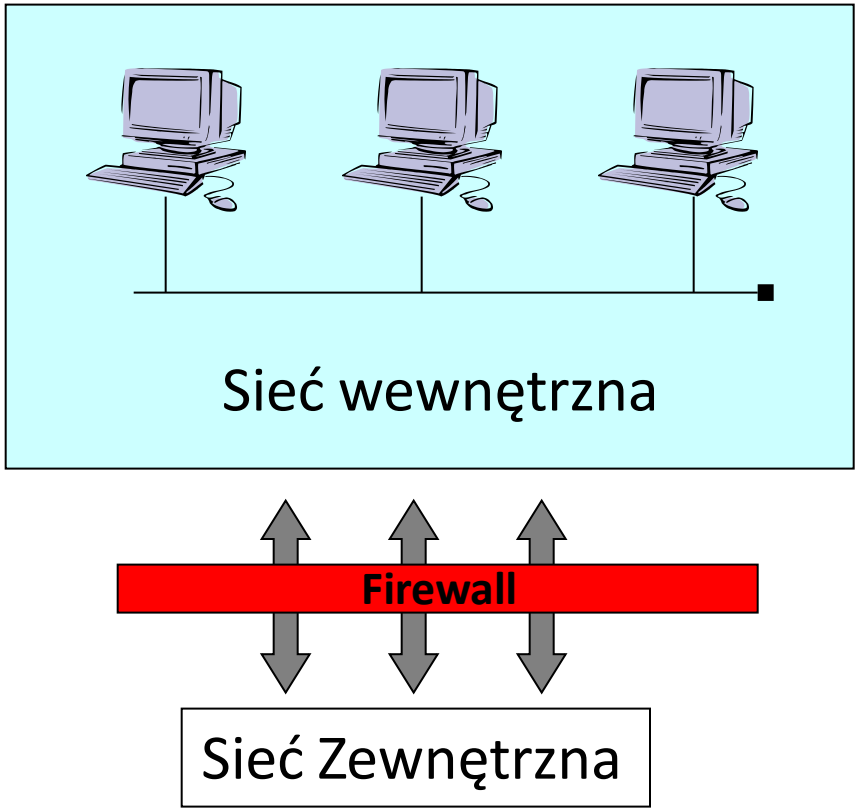
- **Opornik łatkowaty, kudzu** (*Pueraria montana*) – pnącze z rodziny bobowatych występujące naturalnie w Azji południowo-wschodniej oraz na wyspach Oceanii
- Został zawleczony do Ameryki Północnej i Środkowej, Afryki południowej, Azji centralnej i na Ukrainę, gdzie jest uporczywym, bardzo **inwazyjnym chwastem (przyrost do 30 cm dziennie)**
- Kudzu wspina się agresywnie na drzewa i krzewy powodując ich znaczne zacienienie, a w konsekwencji **obumieranie**

Techniki defensywne



Mechanizmy obronne I: systemy firewall

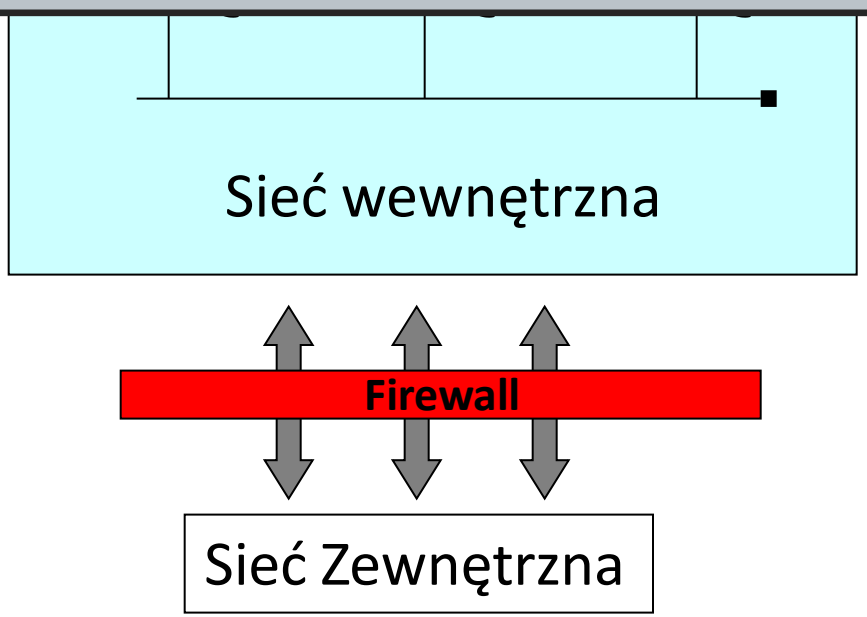
- **Systemy firewall** - „ściana” bezpieczeństwa pomiędzy wewnętrzną, zaufaną siecią i zewnętrzną, potencjalnie niebezpieczną



Mechanizmy obronne I: systemy firewall

- **Systemy firewall** - „ściana” bezpieczeństwa pomiędzy wewnętrzną, zaufaną siecią i zewnętrzną, potencjalnie niebezpieczną

Istota działania: odzielenie się od zagrożeń świata zewnętrznego

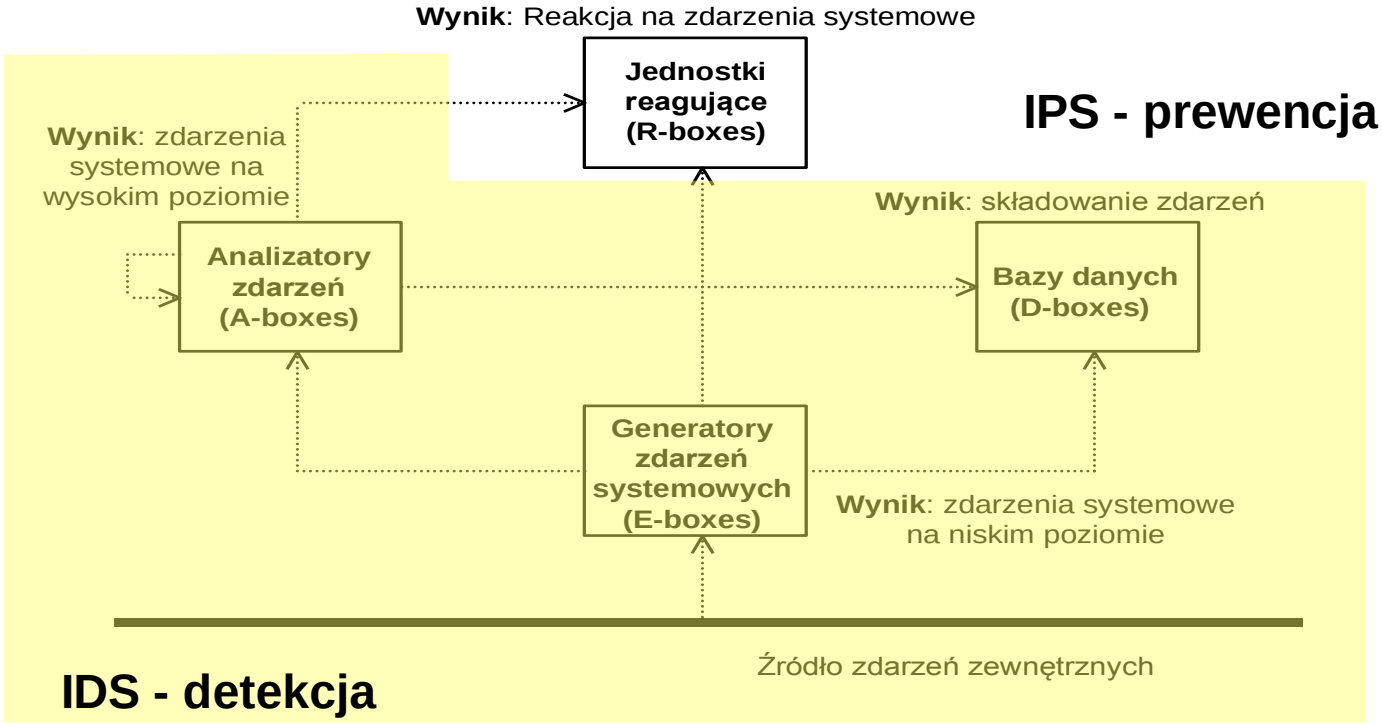


Systemy firewall w naturze

- Skorupy, gniazda, nory, mrowiska...

Mechanizmy obronne II: systemy IDS/IPS

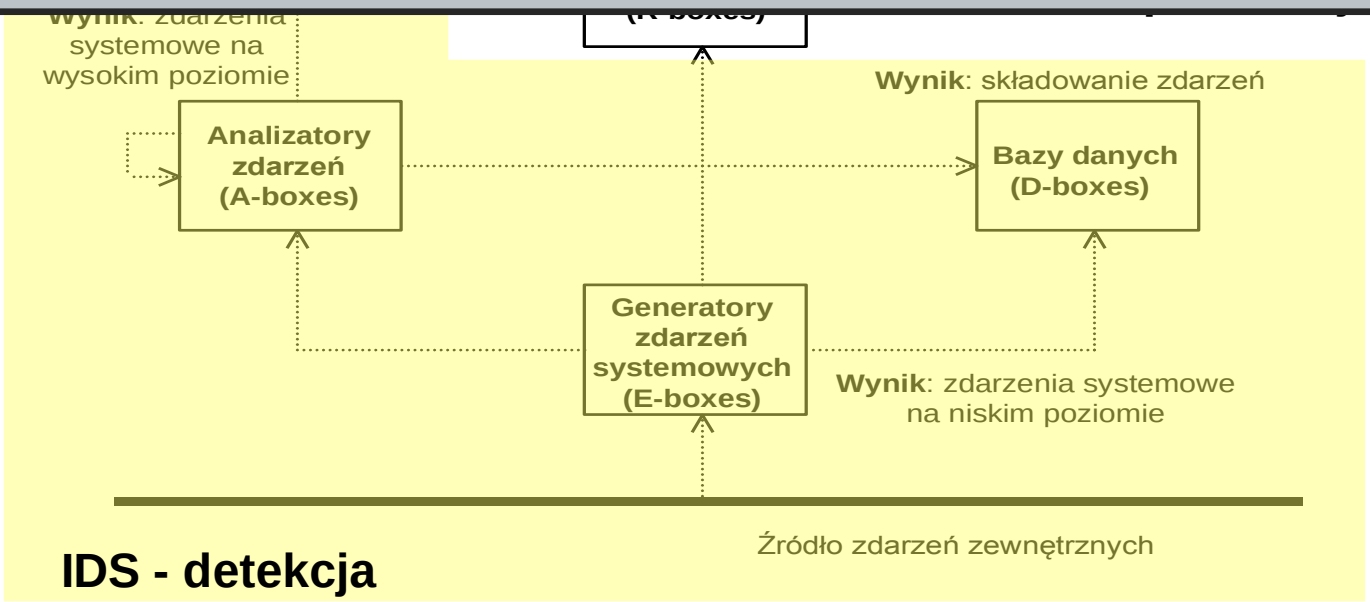
- **Systemy wykrywania i zapobiegania włamaniom** – systemy zwiększające bezpieczeństwo sieci poprzez *wykrywanie* (IDS) i/lub próby *przeciwdziałania* atakom (IPS) najlepiej w czasie rzeczywistym



Mechanizmy obronne II: systemy IDS/IPS

- **Systemy wykrywania i zapobiegania włamaniom** – systemy zwiększające bezpieczeństwo sieci poprzez *wykrywanie* (IDS) i/lub próby *przeciwdziałania* atakom (IPS) najlepiej w czasie rzecz

Istota działania: umiejętność detekcji intruzów oraz reakcja na ich obecność



Systemy IDS/IPS w naturze

- **Larwy motyla** z północnoamerykańskiego gatunku *Drepana arcuata* żerują na brzozach oraz olchach i za pomocą jedwabistej wydzieliny budują na liściu „namiot” chroniąc się w ten sposób przed drapieżnikami i złymi warunkami atmosferycznymi
- Gąsienice **na podstawie drgań liścia powstałych w wyniku zbliżania się intruza** (innej larwy tego gatunku chętnej na schronienie lub drapieżnika) są w stanie **go rozpoznać** (*część detekująca - IDS*) nawet w warunkach złej pogody (deszcz, wiatr)
- Następnie larwa próbuje **odstraszyć intruza poprzez skrobanie w liść** ostatnią parą odnóży **lub bębnienie głową** (*część prewencyjna - IPS*) – metoda skuteczna w przypadku 80% drapieżników!

Podsumowanie: ewolucyjny wyścig zbrojeń

- Zapewnianie bezpieczeństwa w świecie roślin i zwierząt jak i w Internecie wykazuje **wiele podobieństw** zarówno pod względem istoty technik defensywnych jak i ofensywnych
- Obserwujemy swoisty ewolucyjny wyścig zbrojeń: **pojawia się nowa/ulepszona technika ataku**, na którą następnie odpowiedzią jest **dostosowanie/doskonalenie technik obronnych** (inne okno czasowe)

Podsumowanie: ewolucyjny wyścig zbrojeń

- Zapewnianie bezpieczeństwa w świecie roślin i zwierząt jak i w Internecie wykazuje **wiele podobieństw** zarówno pod względem istoty technik defensywnych jak i ofensywnych
- Obserwujemy swoisty ewolucyjny wyścig zbrojeń: **pojawia się nowa/ulepszona technika ataku**, na którą następnie odpowiedzią jest **dostosowanie/doskonalenie technik obronnych** (inne okno czasowe)

Przykład ze świata roślin i zwierząt

Rozkolce

vs.

Krab

Przykład z dziedziny bezpieczeństwa sieciowego

Trojan Zeus/Zbot

vs.

Systemy antywirusowe

Podsumowanie: ewolucyjny wyścig zbrojeń

- Zapewnianie bezpieczeństwa w świecie roślin i zwierząt jak i w Internecie wykazuje **wiele podobieństw** zarówno pod względem istoty technik defensywnych jak i ofensywnych
- Obse
  nowa est
  dosto ve)

Inspiracje dotyczące **nowych** technik ataków/sposobów obrony w świecie wirtualnym **warto czerpać ze świata roślin i zwierząt**

Przykład ze świata roślin i zwierząt

Rozkolce

vs.

Krab

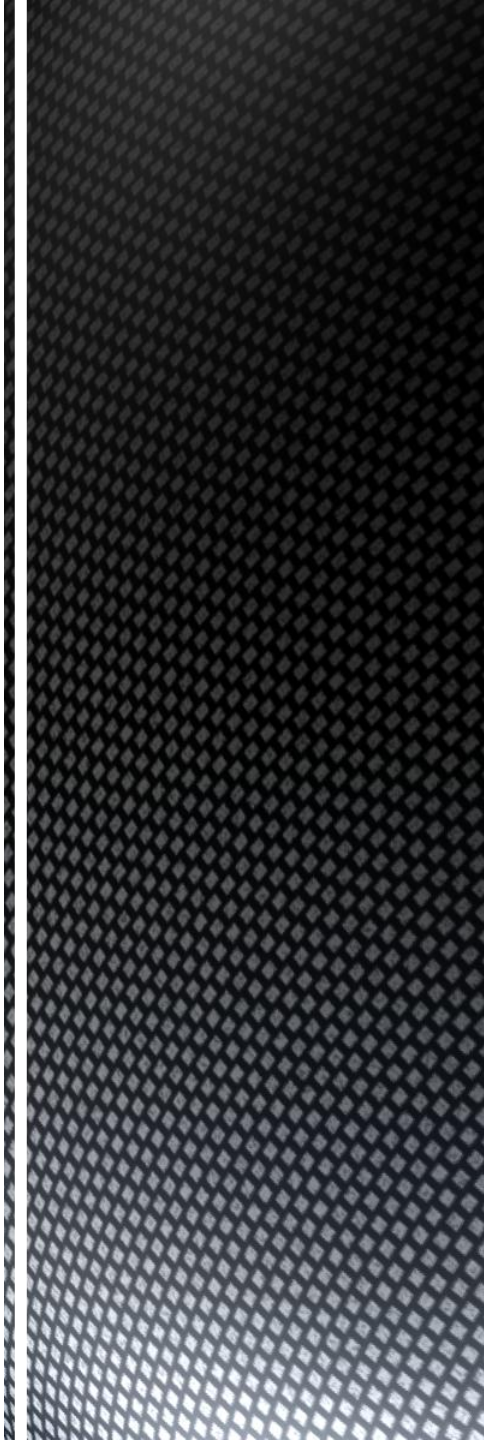
Przykład z dziedziny bezpieczeństwa sieciowego

Trojan Zeus/Zbot

vs.

Systemy antywirusowe

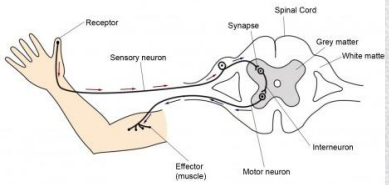
Praktyczne wykorzystanie „lekcji z przyrody”



Cechy warunkujące bezpieczeństwo w przyrodzie

Adaptacyjność

- **reaktywność**
- **heterogeniczność**
- **decentralizacja**
- **nadmiarowość**
- **kooperatywność**



Regin jako przykład wykorzystania cech warunkujących „sukces”

- Regin – koń trojański, który pozostawał niewykryty od 2008 roku, zyskał rozgłos w listopadzie 2014
- **Heterogeniczność** – kod składający się z wielu modułów, praktycznie każda z ofiar otrzymywała inny zestaw modułów
- **Decentralizacja** – ofiary w ramach pojedynczej sieci lokalnej formują sieć P2P, aby ograniczyć ryzyko wykrycia kanału C&C (redukcja liczby połączeń)
- **Nadmiarowość** – wielopoziomowa struktura typu „matrioszka”, kolejne poziomy zaszyfrowane wewnątrz poprzedników; wiele kanałów ukrytej komunikacji z serwerami C&C
- **Kooperacja** – poziom skomplikowania porównywalny do Stuxneta, Duqu, itp. wskazuje na kooperację wielu autorów przy tworzeniu Regina
- **Reaktywność** – (?)

Działania defensywne wykorzystujące w.w. cechy

- **Reaktywność** – w odpowiedzi na utrzymujący się atak (Aurora) ze źródeł chińskich, w 2009 roku podjęto kroki zmierzające do zażegnania kryzysu
- **Kooperacja** – z inicjatywy Google i NSA stworzono narzędzie do wykrywania i reagowania na ataki, Google posiadało niezbędną infrastrukturę, NSA doświadczenie
- **Heterogeniczność** – stworzono dwa narzędzia: Turmoil identyfikuje niepożądany ruch lub oznaki grożącego ataku, Turbine zajmuje się decydowaniem czy ruch należy wstrzymać czy przepuścić, posiada również możliwość (**reaktywność!**) uruchomienia ataku odwetowego
- **Decentralizacja** – efektywność działania zaimplementowanego systemu jest warunkowana przez globalny zasięg infrastruktury Google i liczne, rozproszone punkty monitorowania
- **Nadmiarowość** – wyróżniono instytucje stanowiące tzw. infrastrukturę krytyczną i w ramach danych klas instytucji przeprowadza się regularne briefingi dotyczące aktualnego statusu „cyberwojny”

Shane Harris *„@WAR – The Rise of the Military-Internet Complex”*

Bio-Inspired Cybersecurity Project

http://cybersecurity.bio

E. Rzeszutko, W. Mazurczyk - Insights from the Nature for Cybersecurity

W. Mazurczyk, E. Rzeszutko - Security - a perpetual war: lessons from nature - *IEEE IT Professional*, January/February 2015

O analogiach pomiędzy bezpieczeństwem sieciowym a światem przyrody

Elżbieta Rzeszutko
Politechnika Warszawska

SCS 2014

27 listopada 2014