Advanced Cyber Defence Center(ACDC) projekt

ACDC

the Advanced Cyber Defence Centre

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC projekt – osnovni podaci

- Advanced Cyber Defence Center
- Europski projekt financiran po ICT-PSP okvirnom programu
- Trajanje: 30 mjeseci (1.2.2013. – 31.7.2015.)
- 28 članova iz 14 zemalja
- Cilj projekta: izgraditi EU platformu za borbu protiv *botneta* koja ima svoje nacionalne centre za podršku korisnicima i centralnu lokaciju sa podacima (*Central Clearing House* u SR Njemačkoj)
- Ukupni proračun projekta: 15,5 mil. EUR (učešće EU je 50%)
- Glavni koordinator projekta: ECO (*Association of the German Internet Industry*)

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

ACDC

ACDC udružuje grupacije

- ACDC udružuje grupacije koje su najviše povezane sa problematikom *botneta*
- Partneri predstavljaju zajednicu iz slijedećih grupacija:
  - ISP
  - CERT
  - NREN
  - Sveučilišta
  - Proizvođači sigurnosnih alata i softvera
  - Predstavnici kritične infrastrukture
  - Tijela za provedbu zakona(*Law Enforcement Agencies*)

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

ACDC

Partneri u ACDC projektu koji su članovi konzorcija

- 28 partnera iz 14 zemalja:

CROATIAN ACADEMIC AND RESEARCH NETWORK

ACDC

Ciljevi projekta

- Ciljevi:
  - Osigurati alate i senzore za detekciju prijetnji na internetu koje su vezane uz problem *botneta*
  - Ublažiti efekte napada na mreže, web sjedišta i na krajnje korisnike
  - Osigurati sveobuhvatni pristup pri detekciji *botneta*
  - Pomoći pri eliminaciji *botneta* pomoću svojih usluga

- Planirano je da ACDC projekt bude jedan od glavnih oslonaca EU za provedbu strategije o *cyber* sigurnosti

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK
Nacionalni CERT+
ACDC

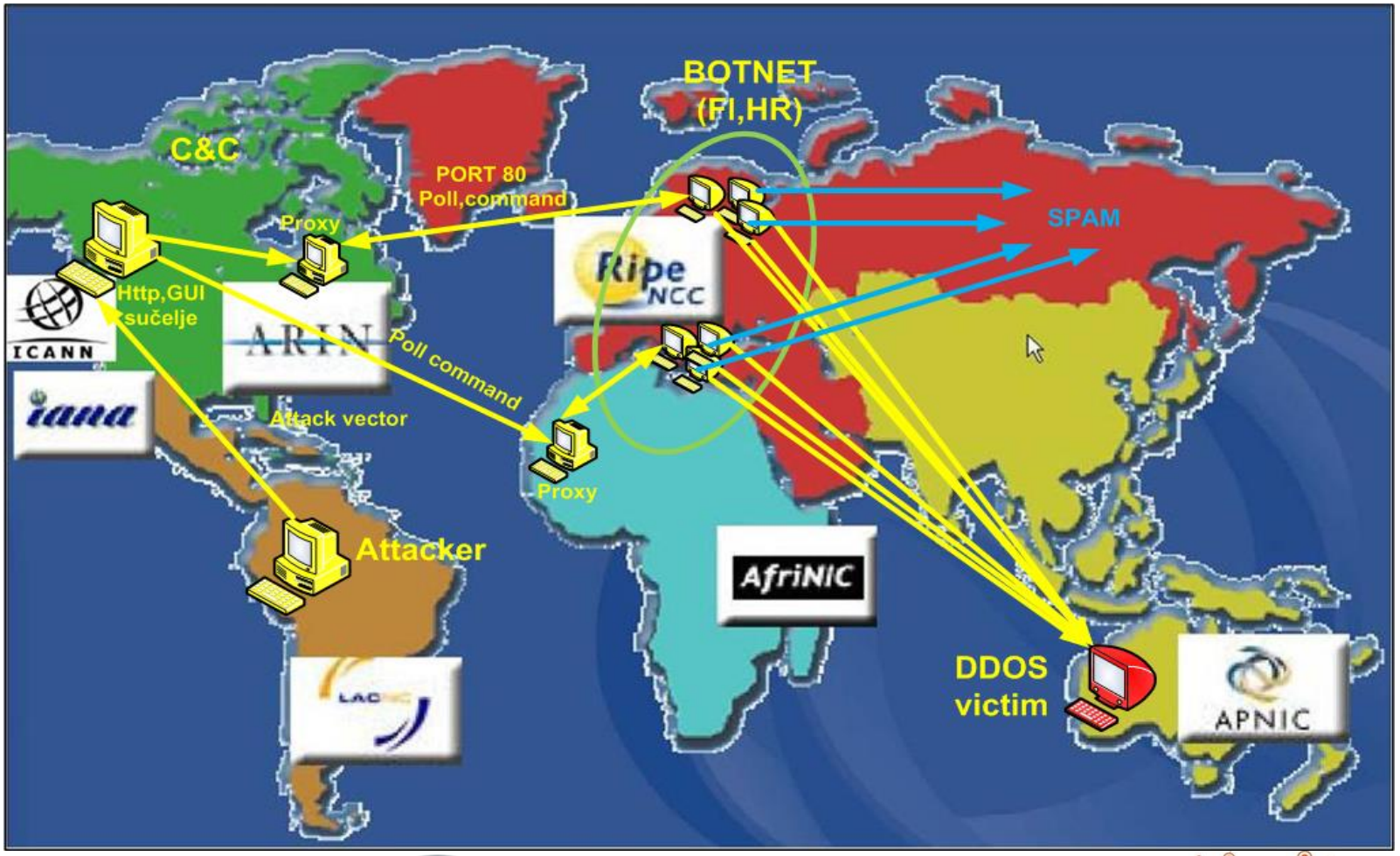
Što je to botnet?

- Botnet je skraćenica od roBOT NETwork
- Botnet je skupina zaraženih računala koja komuniciraju sa svojim kontrolnim centrom
- Botnet je infrastruktura koju upotrebljavaju cyber kriminalaci kao platformu za napade
- Botnet je i servis na internetu kojeg se može iznajmiti za izvršenje određenog napada
- Botnet je teško odstraniti s interneta zbog tehnika sakrivanja kontrolnih centara
- Računalo sa instaliranim botom je također žrtva napada

Prijetnje vezane uz BOTNET

- kompromitiranje radnih stanica i servera te preuzimanje kontrole
- napadi na ostale informatičke sustave u internoj mreži preko inicijalno kompromitiranog računala
- napadi na ostale ciljeve na Internetu bez znanja vlasnika računala
- krađa autentifikacijskih, osobnih i poslovnih podataka
- nanošenje materijalne štete (na. pr. zlouporaba e-banking usluge)
- preuzimanje kontrole nad računalom

Uobičajena arhitektura botneta

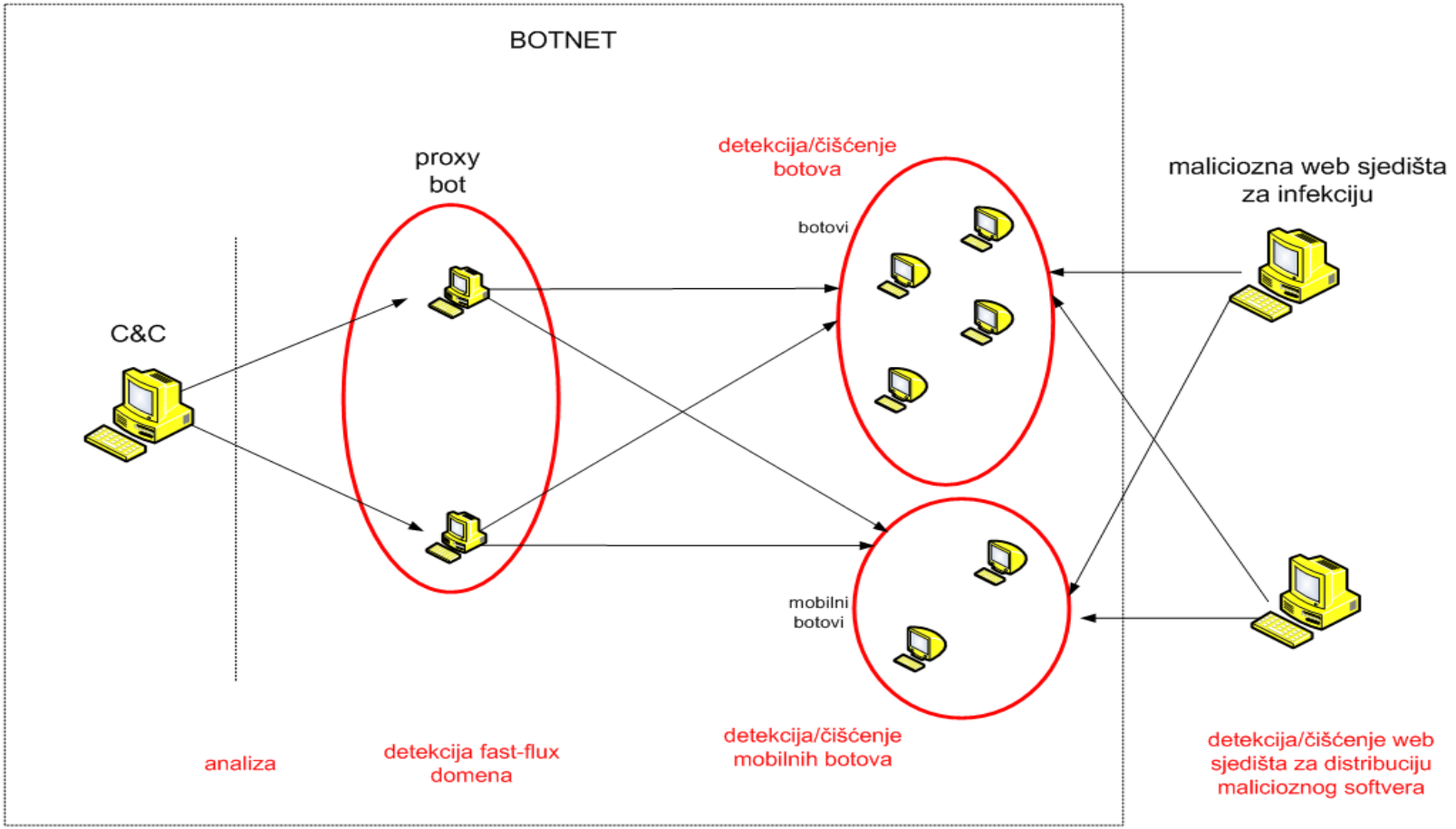


CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Čime se bavi ACDC?



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Od čega se sastoji ACDC?

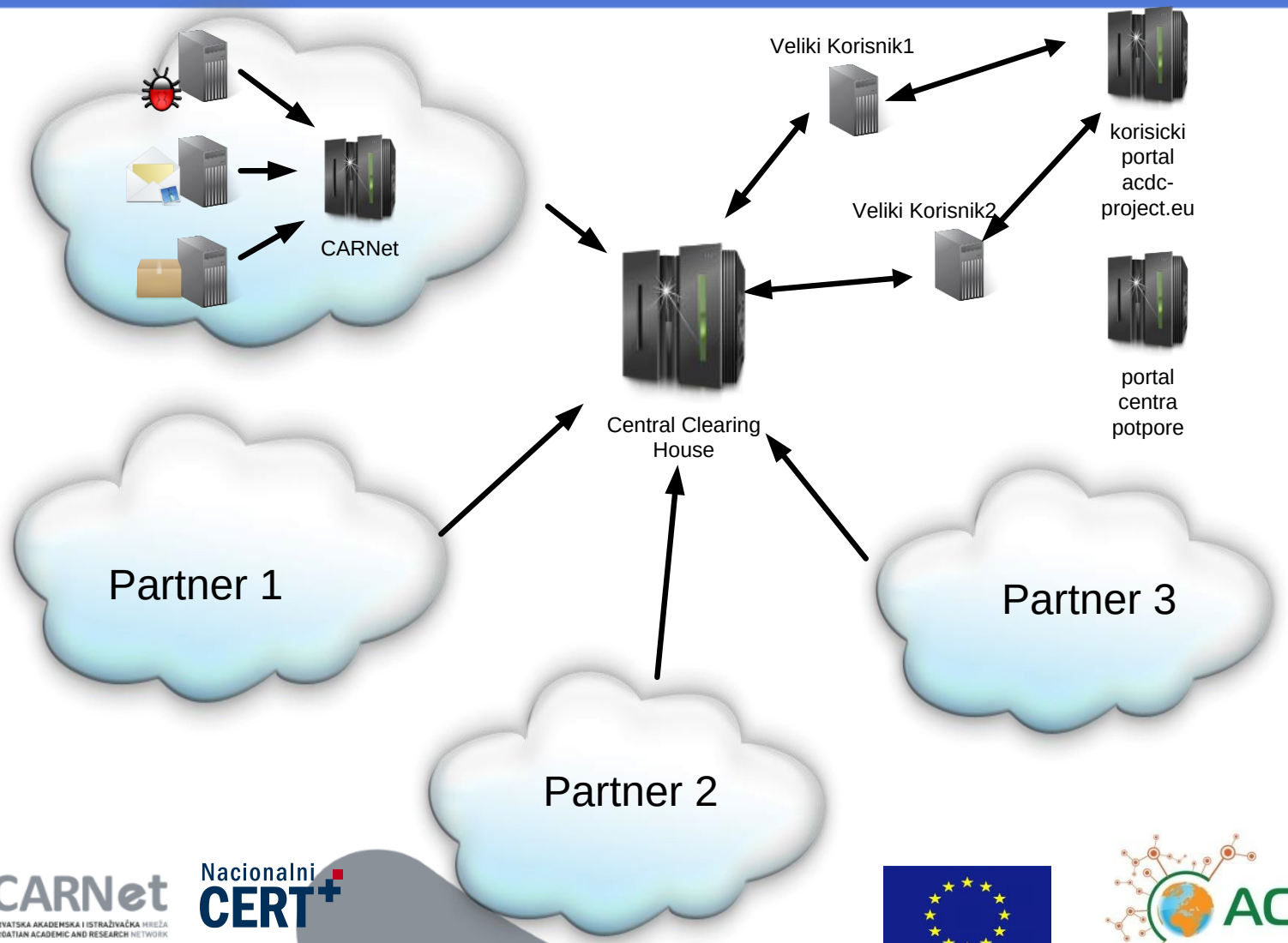
- Central Clearing House
  - jezgra sustava koje prima i obrađuje podatke
  - mogućnost izvještavanja korisnika
- Uređaji/softveri za:
  - detekciju i uklanjanje botova kod krajnjih korisnika
  - detekciju i uklanjanje zlonamjernih web sjedišta
  - analizu mrežnog prometa
  - detekciju fast-flux domena
- 8 Nacionalnih centara potpore povezanih sa CCH

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

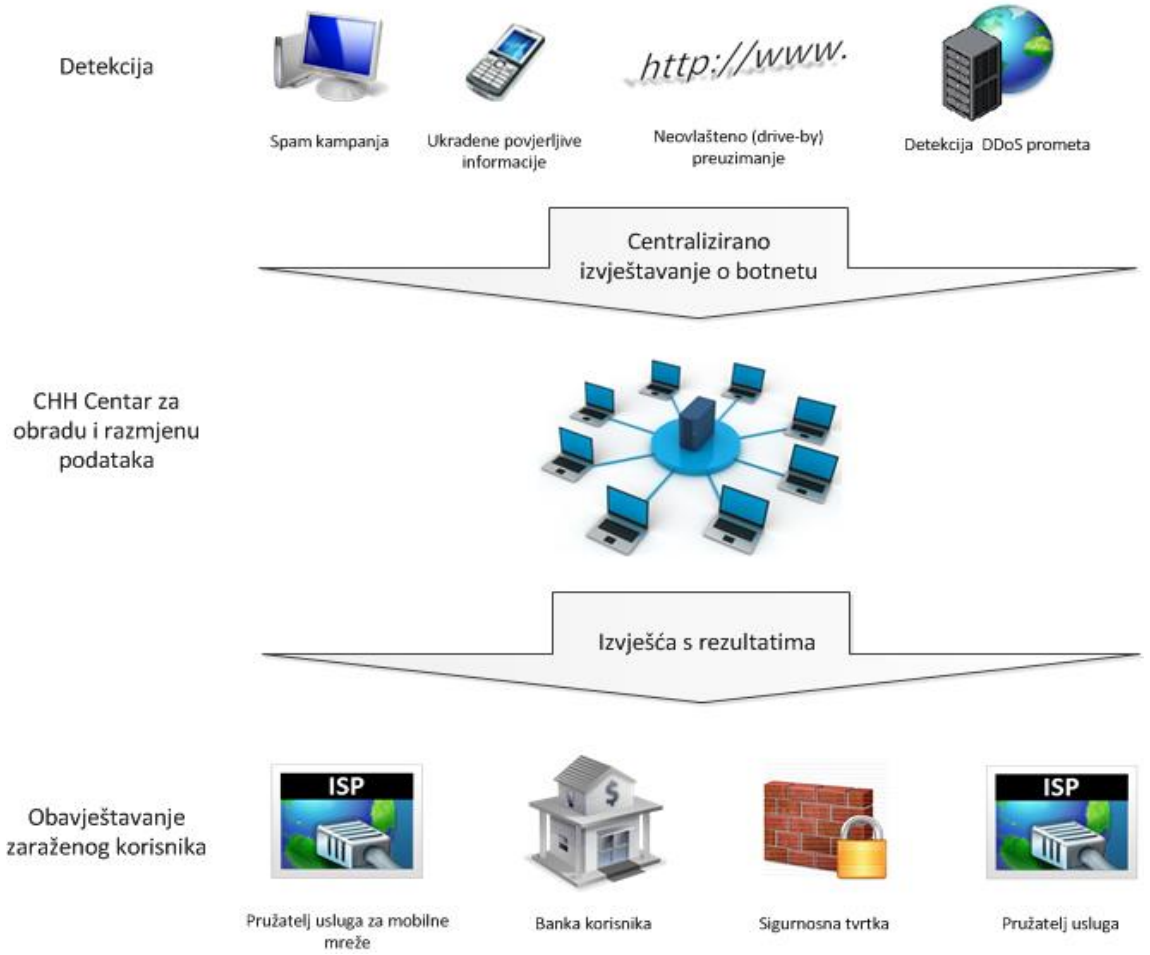
Nacionalni CERT

ACDC

Arhitektura ACDC platforme



Čemu služi CCH?



CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

ACDC

Potencijalni korisnici ACDC projekta

- Veliki korisnici – ISP, hosting provideri, kritična IT infrastruktura, financijske institucije
  - mogu imati pristup do informacija na CCH koristeći dostupne feed-ove
- Mali krajnji korisnici
  - mogu se koristiti alatima koji se nalaze na web sjedištu nacionalnog centra potpore

Uloga CARNet-a u ACDC projektu

- Razvoj komponenti koje se odnose na mrežne senzore i alate za detekciju
  - *Honeypot* sustavi
  - *Spamtrap*
  - *Sustav za detekciju fast-flux domena baziran na pDNS*
  - *NIRC*
- Uspostava nacionalnog centra za podršku
- Rad s korisnicima ACDC projekta

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK
Nacionalni CERT+
ACDC

Uloga CARNet-a u ACDC projektu - komponente

- *Honeypot*
  - Sustav koji je naizgled ranjiv za što veći broj napada
  - Za svaki napad sakuplja podatke o tipu napada i napadaču

- *Spamtrap*
  - Sustav koji prikuplja neželjenu elektroničku poštu
  - Analizom se utvrđuje zlonamjernost upućene poruke (URL,attachemnt)
  - Dodatnom analizom se utvrđuje koji pošiljatelji pripadaju *botnetu*

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

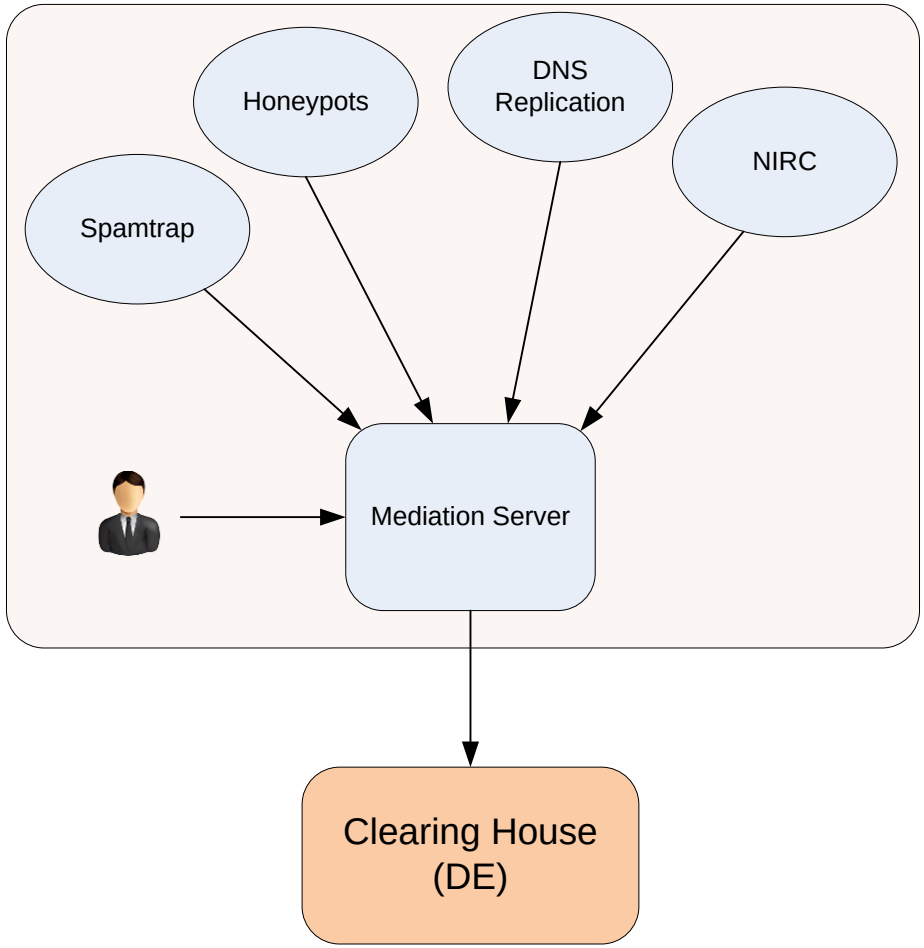
ACDC

Uloga CARNet-a u ACDC projektu - komponente

- *Passive DNS*
  - Sustav pomoću kojeg se iz anonimiziranog DNS prometa detektiraju *fast flux* domene i računala koja sudjeluju u njima
  - *Fast flux* je tehnika pomoću koje vlasnici *botneta osiguravaju otpornost botneta na gašenje*

- *NIRC*
  - Kolektor za prikupljanje javno dostupnih informacija o napadima

Uloga CARNet-a u ACDC projektu - komponente



www.antibot.hr

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Ciljevi portala www.antibot.hr

- nastao u sklopu projekta ACDC
- informiranje krajnjih korisnika o prijetnji botneta
- servisi za zaštitu
- alati za zaštitu i čišćenje računala
- provjera otvorenih portova

Pitanja i odgovori