



Advanced Cyber Defence Center(ACDC) projekt



ACDC 

the Advanced Cyber Defence Centre

ACDC projekt – osnovni podaci

- **A**dvanced **C**yber **D**efence **C**enter
- 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*)

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*)

Partneri u ACDC projektu koji su članovi konzorcija

•28 partnera iz 14 zemalja:



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

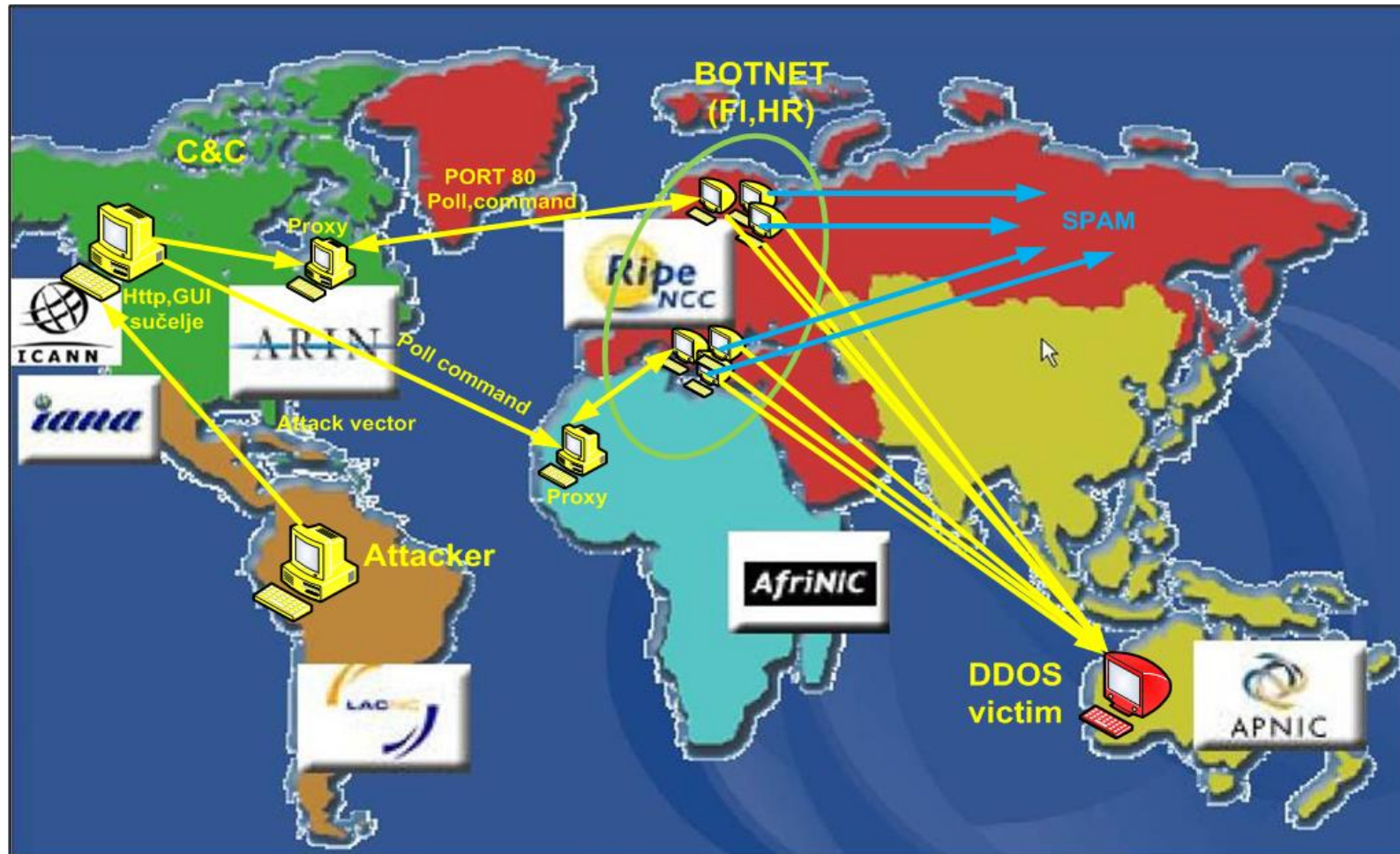
Što je to botnet?

- 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

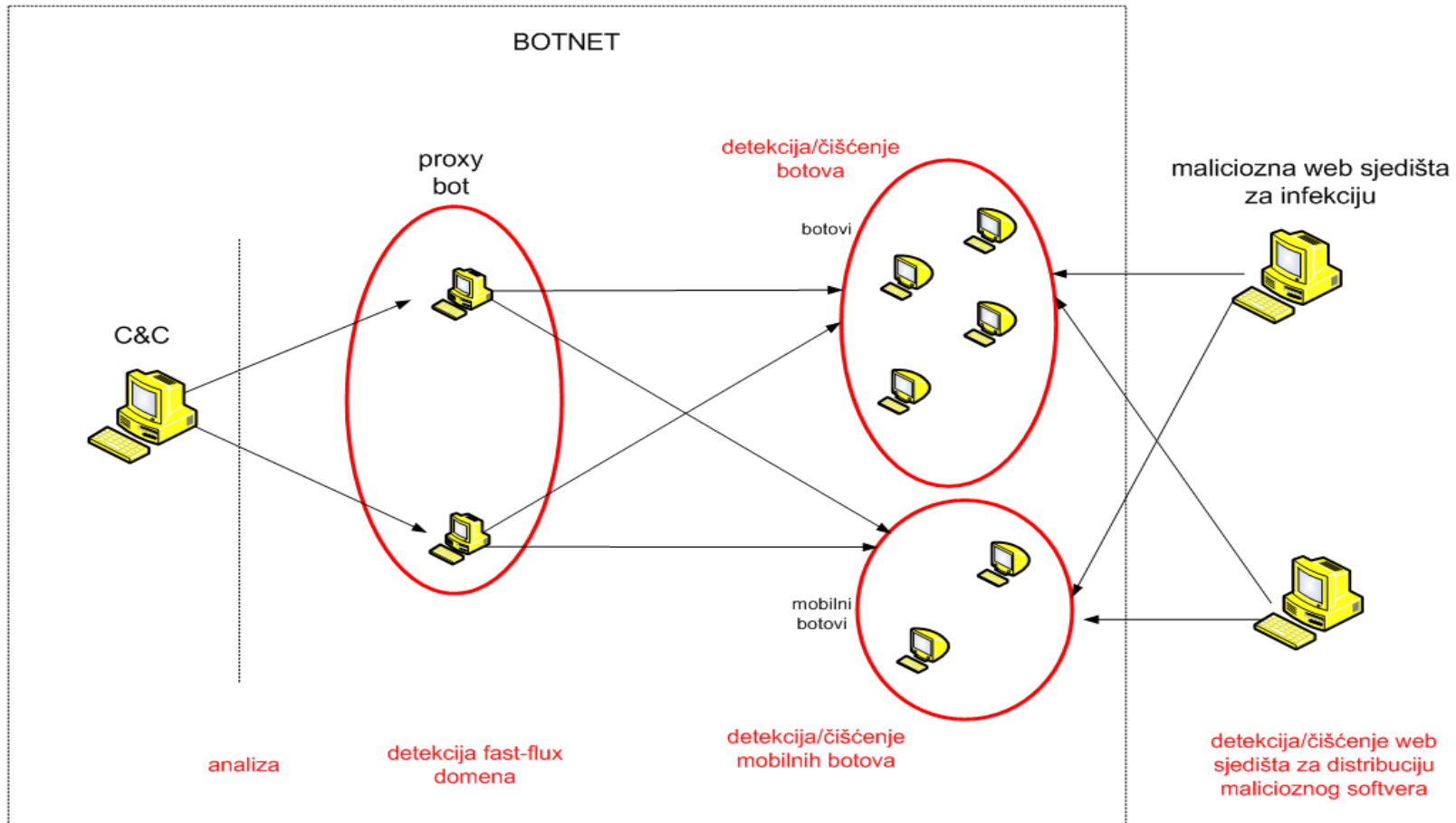
Prijetnje vezane uz BOTNET

- 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



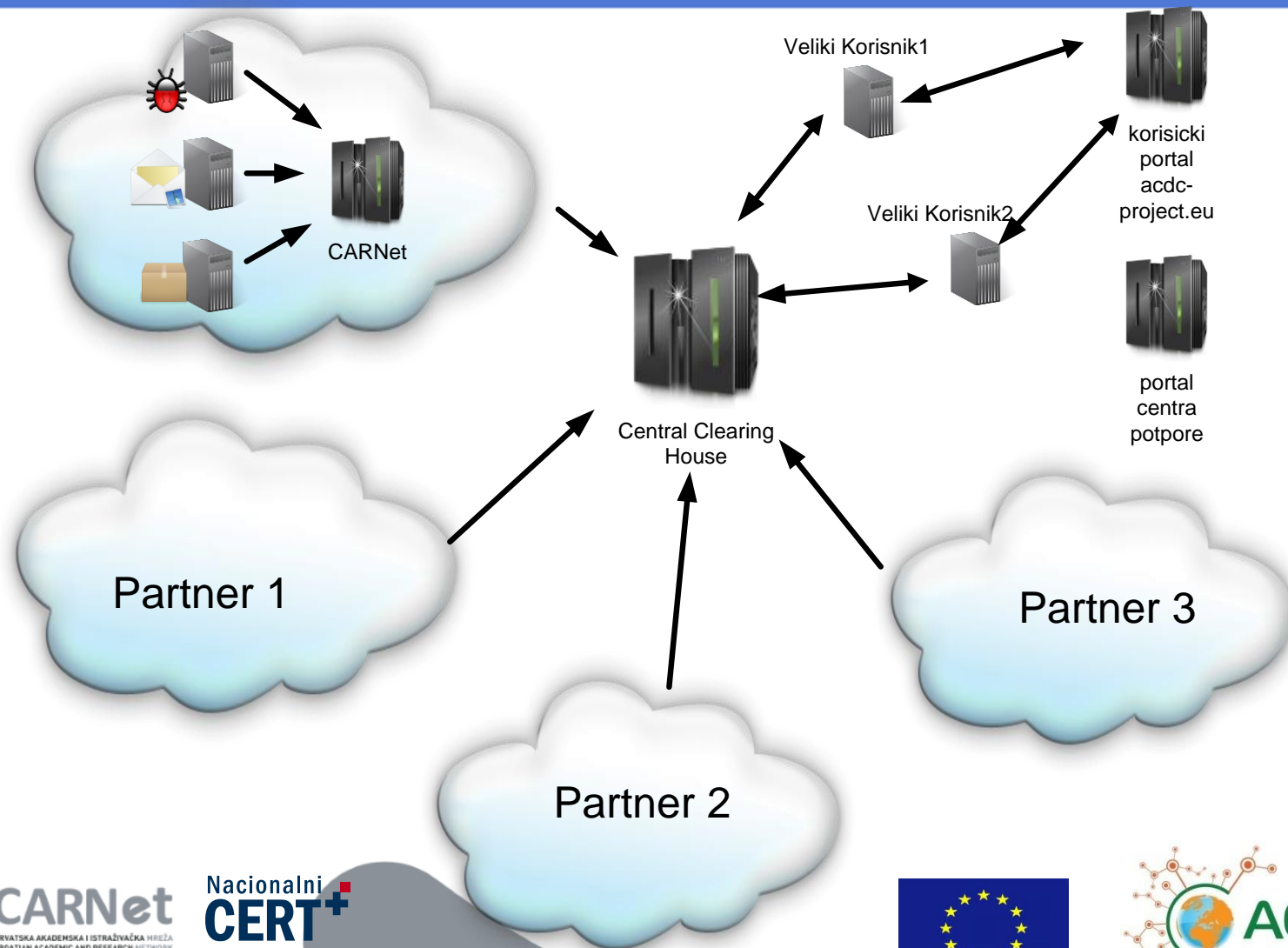
Čime se bavi ACDC?



Od čega se sastoji ACDC?

- Central Clearing House
 - jezgra sustava koje prima i obrađuje podatke
 - mogućnost izvještavanja korisnika
- Uređaji/software 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

Arhitektura ACDC platforme



Čemu služi CCH?

Detekcija



Spam kampanja



Ukradene povjerljive informacije

http://www.

Neovlašteno (drive-by) preuzimanje



Detekcija DDoS prometa

Centralizirano izvještavanje o botnetu

CHH Centar za obradu i razmjenu podataka



Izvješća s rezultatima

Obavještanje zaraženog korisnika



Pružatelj usluga za mobilne mreže



Banka korisnika



Sigurnosna tvrtka



Pružatelj usluga

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

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*

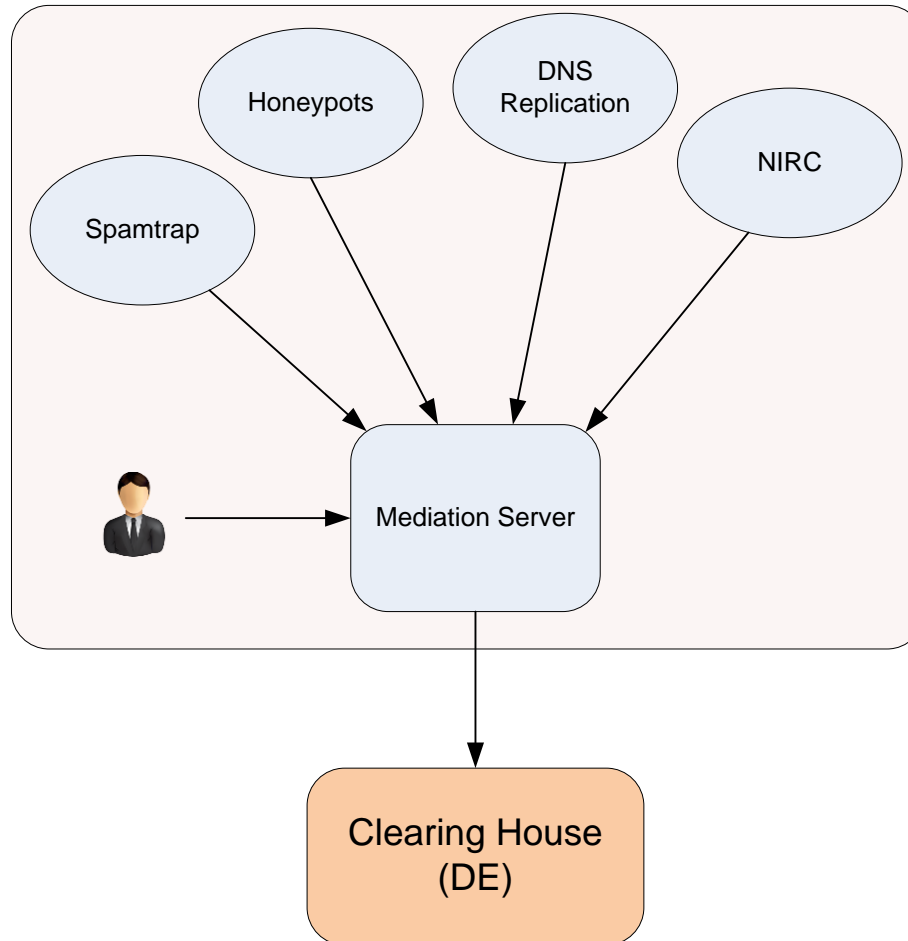
- Sustav koji prikuplja neželjenu elektroničku poštu
- Analizom se utvrđuje zlonamjernost upućene poruke (URL, attachemnt)
- Dodatnom analizom se utvrđuje koji pošiljatelji pripadaju *botnetu*



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



Anti-Botnet

Nacionalni centar podrške

1. INFORMIRAJ | 2. OČISTI | 3. SPRIJEČI

  Nacionalni  



Dobrodošli!     

O projektu
Sudionici projekta
Kontakt
Privatnost podataka
Uvjeti korištenja

Blog
Više o botnetima [pdf]
Upute za korištenje [pdf]

Provjeri i osiguraj

 **INITIATIVE^S**
Scanned: 2014-09-05

InitiativeS provjera web stranice
(upute)

Dobrodošli na Anti-Botnet Nacionalni centar podrške.

- [Hakirana još jedna kuća za posluživanje reklama na webu](#)
- [Uspješnost hakiranja aplikacija preko 90%](#)
- [Xiaomi uređaji potajno šalju osjetljive podatke kineskim poslužiteljima](#)
- [Lažni Googlebotovi obavljaju zlonamjerne aktivnosti](#)
- [Kompromitiran najveći Cydia repozitorij](#)
- [Novi bankarski trojanac „Kronos“](#)
- [Nova zlonamjerna aplikacija HijackRAT napada korisnike Androida](#)
- [Sigurnosni propust u Androidu omogućuje izvlačenje osjetljivih informacija](#)
- [Hakiran servis za distribuciju web oglasa](#)

U poglavlju [Informiraj](#) saznajte što su Botneti, kakvu štetu mogu napraviti i na koji način mogu biti prijetnja podatcima na vašem računalu. U poglavlju [Očisti](#) dostupan je [EU-Cleaner](#). S ovim alatom možete očistiti Vaše računalo od malicioznog softvera. U poglavlju [Spriječi](#) pronaći ćete korisne savjete kako zaštititi vaše računalo od ponovne zaraze.

1. Informiraj | 2. Očisti | 3. Spriječi

Impressum | Privatnost podataka
Uvjeti korištenja

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

