Računalna sigurnost na Internetu u RH

Nacionalni CERT

Jagor Čakmak

Inženjer za računalnu sigurnost, Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

O Nacionalnom CERT-u

- Osnovan je 2008. godine u skladu sa Zakonom o informacijskoj sigurnosti sa funkcijom očuvanja sigurnosti javnih informatičkih sustava u RH
- Zadaća mu je očuvanje sigurnosti javnih informatičkih sustava u RH
- Jedan je od odjela u CARNet-u i ima 10 djelatnika
- Predhodnik Nacionalnog CERT-a je CARNet CERT koji je osnovan 1996. godine
- Nacionalni CERT preuzima nacionalnu funkciju od CARNet CERT-a 2008. godine

Zakon o informacijskoj sigurnosti o Nacionalnom CERT-u

V. NACIONALNI CERT

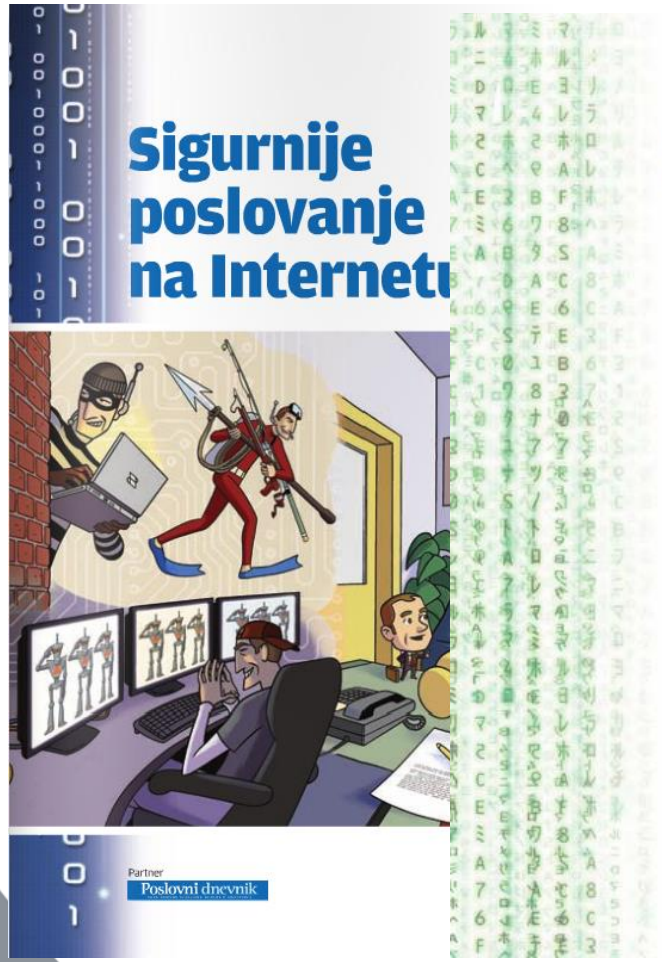
Članak 20.

(1) CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.
(2) CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu: CARNet).
(3) CERT usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom.
(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.

Usluge Nacionalnog CERT-a -Proaktivne mjere:

- Diseminacija informacija:
  - Novosti i aktualnosti vezane uz informacijsku sigurnost
  - Izdavanje sigurnosnih preporuke (cca 1500 godišnje)
  - Izdavanje tehničkih dokumenata vezanih uz sigurnost na Internetu (*white paper*) (cca 20 godišnje)
  - Sigurnosni alati (cca 20-30 godišnje)
  - Tehnološke novosti – evaluacija u laboratoriju
  - Provjere ranjivosti javnih sustava
  - Izdavanje brošura i ostalih materijala
  - Javni nastupi
  - Edukacija ciljanih skupina

Brošure – proaktivna mjera koju provodi Nacionalni CERT



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

www.cert.hr

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

Usluge Nacionalnog CERT-a - Reaktivne mjere:

- Prikupljanje informacija o kompromitiranim računalima i incidentima u RH, većinom iz stranih izvora, sustav (HR@SRU)
- Obrada i koordinacija incidenata (cca 500 godišnje). Odnosi se samo na poslužitelje.
- Nacionalni CERT obrađuje incidente pri kojima su barem jedna strana (napadnuti ili napadač) u RH (IP adresa, domena .hr ili je vlasnik domene hrvatski državljanin)
- Najčešći cilj je što prije sa Interneta ukloniti maliciozni sadržaj uz predhodnu analizu problema
- Forenzika *malvera* i poslužitelja

Granice hrvatskog Internetskog prostora, odnosno ovlasti Nacionalnog CERT-a nad tim prostorom

IP adresa	Domena	Fizička lokacija	Vlasnik domene
Hrvatski ISP	.hr	RH	Domaći i strani
Hrvatski ISP	.com .net .org….	RH	Domaći i strani
Strani ISP	.hr	Izvan RH	Domaći i strani
Strani ISP	.com .net .org	Izvan RH	Domaći

Granice Hrvatskog internetskog prostora nisu identične geografskim granicama

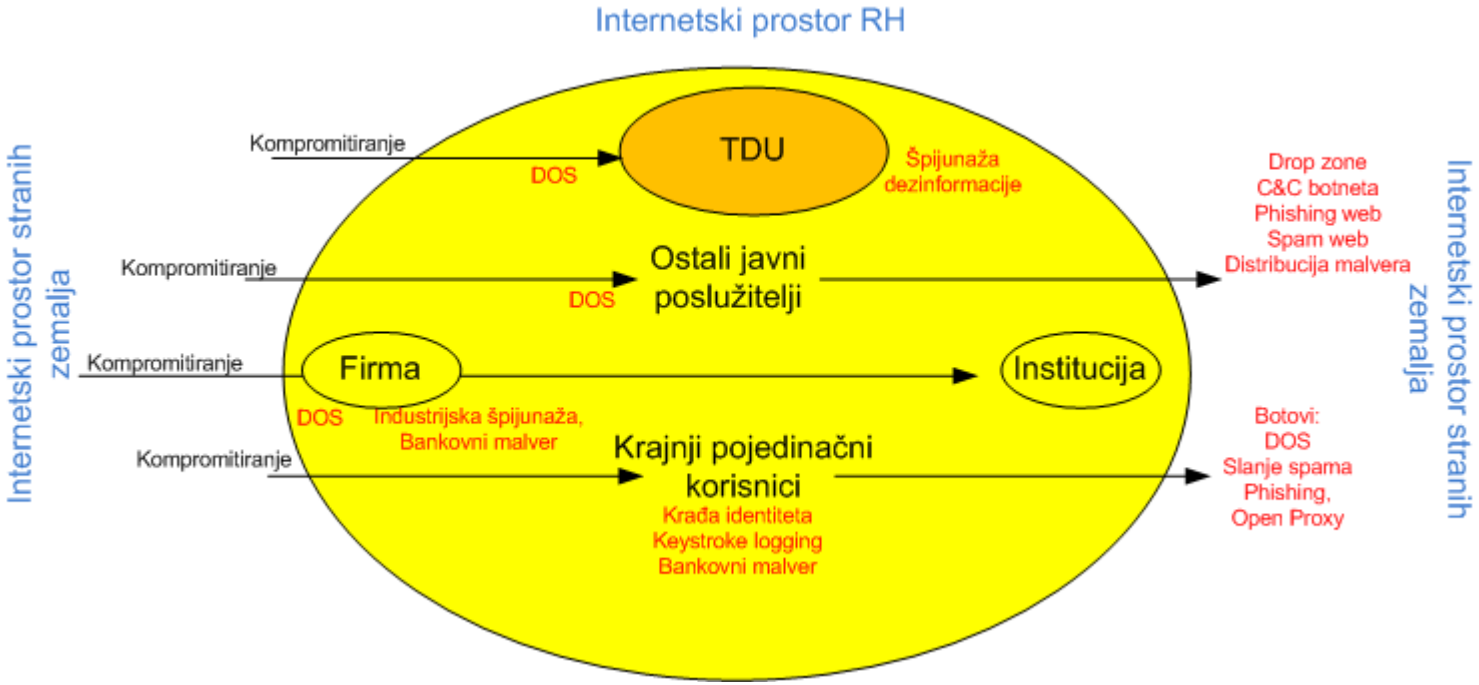
Vrste incidenata koji su u nadležnosti Nacionalnog CERT-a

- Onemogućavanje rada pojedine usluge (DoS/DDoS)
- Onemogućavanje rada mrežne infrastrukture ISP-a i poslužitelja (DDoS)
- Kompromitiranje poslužitelja
- Nedozvoljene mrežne aktivnosti (*port scan*)
- Slanje *spama*
- *Phishing* i ostale prijevare putem Interneta

Incidenti koji se prijavljuju Nacionalnom CERT-u

- Incidenti se odnose na računala koja imaju statičke ili dinamičke IP adrese
- Nacionalni CERT obrađuje incidente sa statičkim IP adresama jer je vlasnik računala poznat (najčešće poslužitelj)
- Nacionalni CERT ne može obraditi incidente na računalima s dinamičkom IP adresom jer ne zna tko je vlasnik računala te stoga iste podatke prosljeđuje ISP-u
- Nacionalni CERT vodi statističku obradu incidenata na računalima s dinamičkom IP adresom

Vrste napada hrvatski prostor Interneta i vrste napada iz hrvatskog adresnog prostora



CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

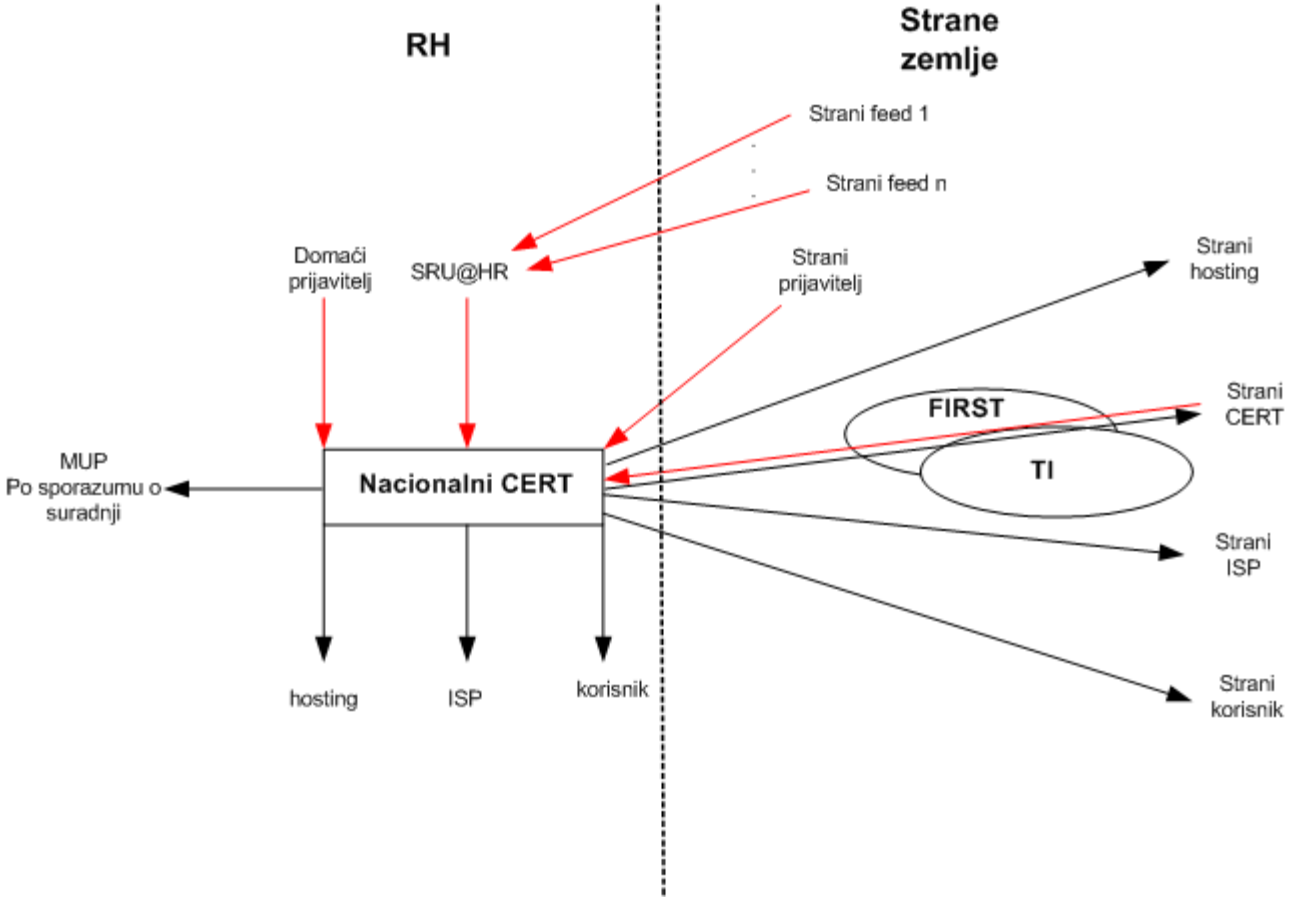
Direktni korisnici Nacionalnog CERT-a

- Korisnici Nacionalnog CERT-a (*constituency*) su:
  - Građani RH
  - Poslovni subjekti – firme, banke i sl.
  - ISP-ovi, abuse službe, hosting provideri
  - Institucije
  - …
  - Generalno gledajući - svi korisnici interneta u RH

Suradnja Nacionalnog CERT-a sa drugima

- Krajnji korisnici usluge pristupa Internetu
- Izvori informacija o incidentima u RH (Shadowserver, Arbor, RSA, Honeypot Project, SpamCop i drugi)
- Strani i domaći ISP-ovi i abuse službe
- Strani i domaći hosting provideri
- Proizvođači sigurnosnog softvera i opreme
- FIRST, TF-CSIRT i strani CERT-ovi
- UVNS i ZSIS – zakonom definirana suradnja
- MUP – suradnja na polju edukacije i obradi incidenata koji uključuju kazneno djelo

Suradnja pri obradi incidenata



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Incidenti u Republici Hrvatskoj

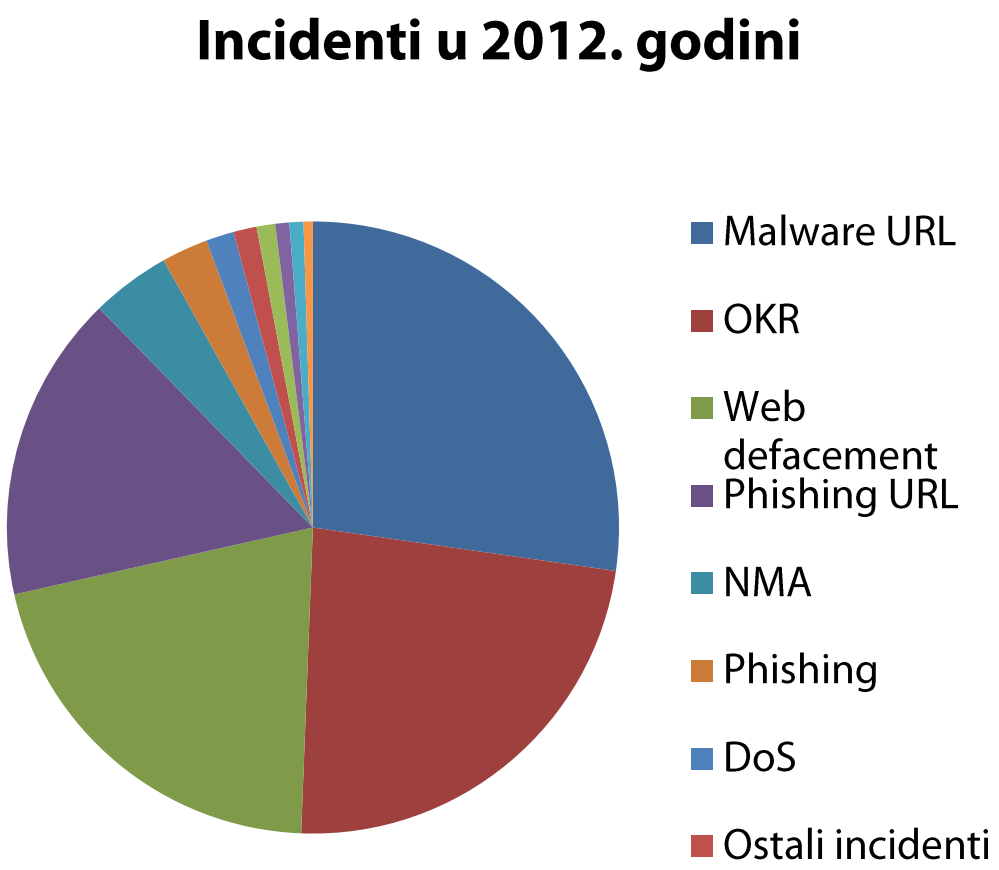
Statistike

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Statistike – raspodjela incidenata

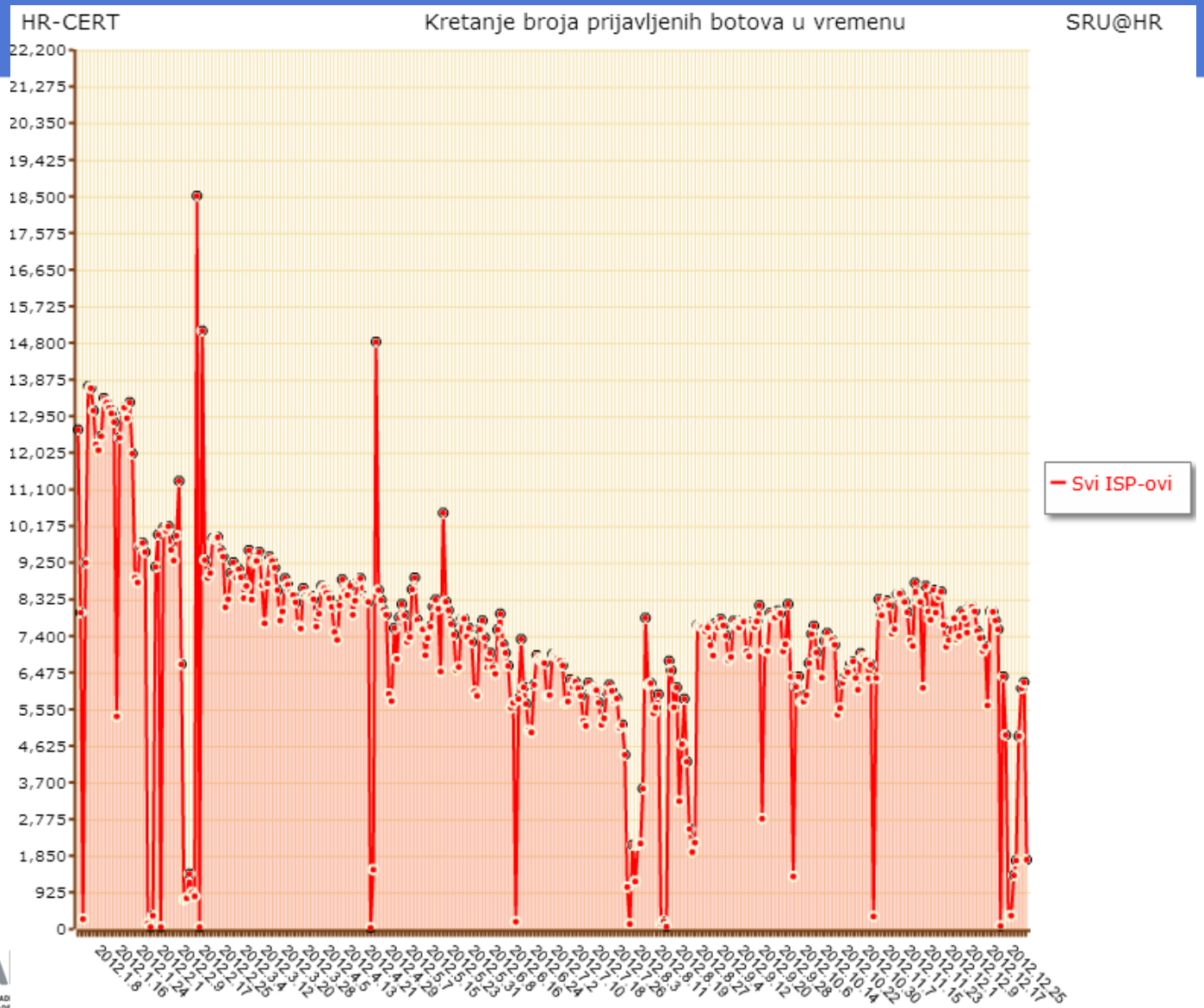
- Više od 500 incidenata tijekom 2012. godine
- Više od 400 incidenata u prvoj polovici 2013. (75% web *defacement* napadi)



CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Statistike – kretanje broja botova



Statistike

- Uočavamo povećanje broja DoS napada
- Kampanje *web defacement* napada
- Pojavili su se ozbiljni napadi koji su rezultirali krađom financijskih sredstava
- Incidenata se događaju svaki dan

Mjere obrane – SRU@HR

- SRU@HR je sustav koji omogućuje praćenje broja incidenata na Internetu u Republici Hrvatskoj
- Razvio ga je Nacionalni CERT
- Jedna je od reaktivnih mjera kojima Nacionalni CERT ispunjava svoju misiju
- U SRU@HR broje se oni incidenti koje Nacionalni CERT obrađuje temeljem svojeg pravilnika

Kako funkcionira SRU@HR

1. Prikupljanje informacija s izvora na internetu

3. Diseminacija informacija prema ISP-ovima i *ticketing* sustavu

2. Analiza i izdvajanje relevantnih incidenata

5. Izrada izvješataja na zahtjev iz baze podataka

4. Ručna obrada incidenata i unos u bazu

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

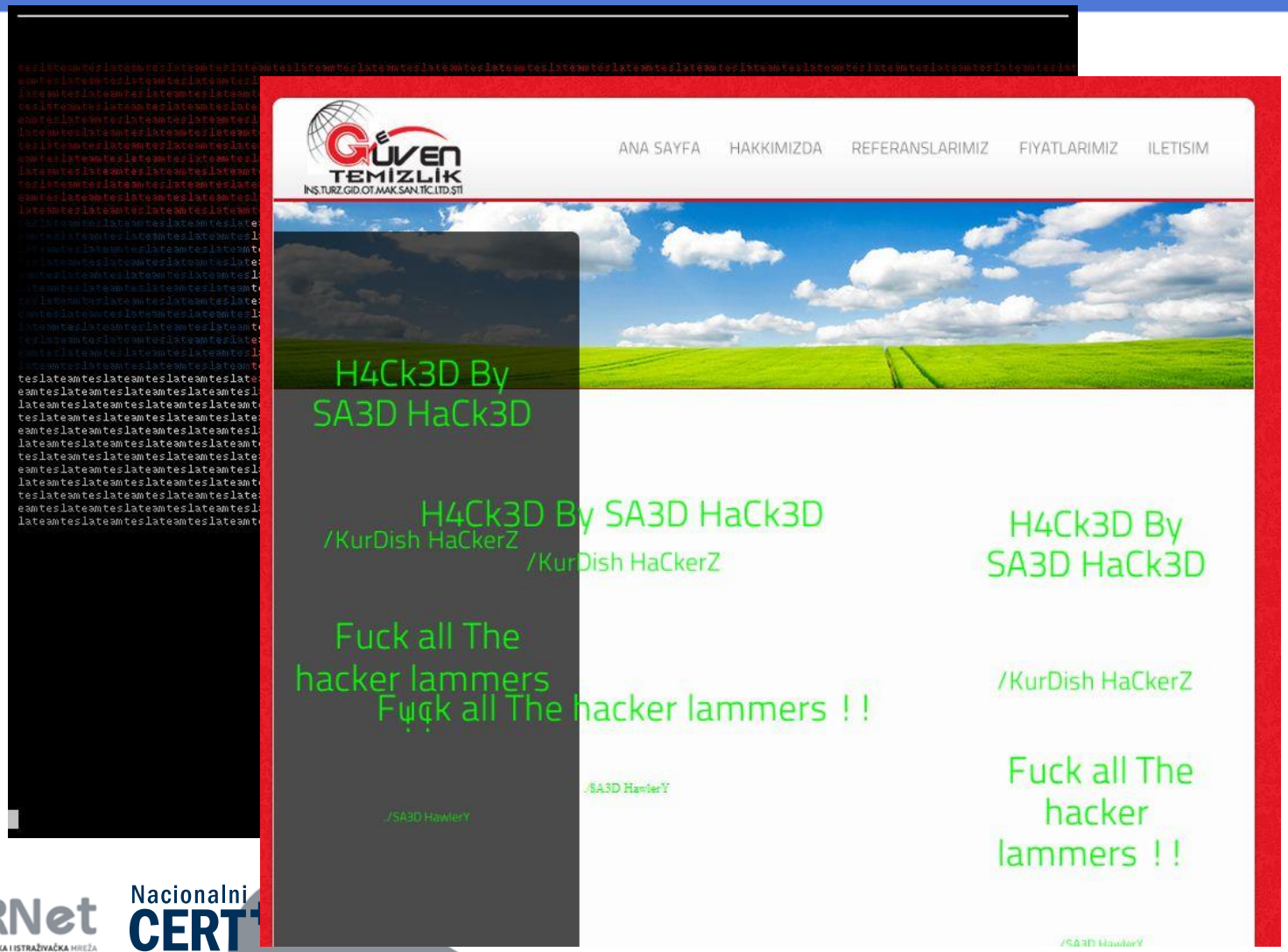
Incidenti u Republici Hrvatskoj

Primjeri

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Primjeri incidenata – Defacement



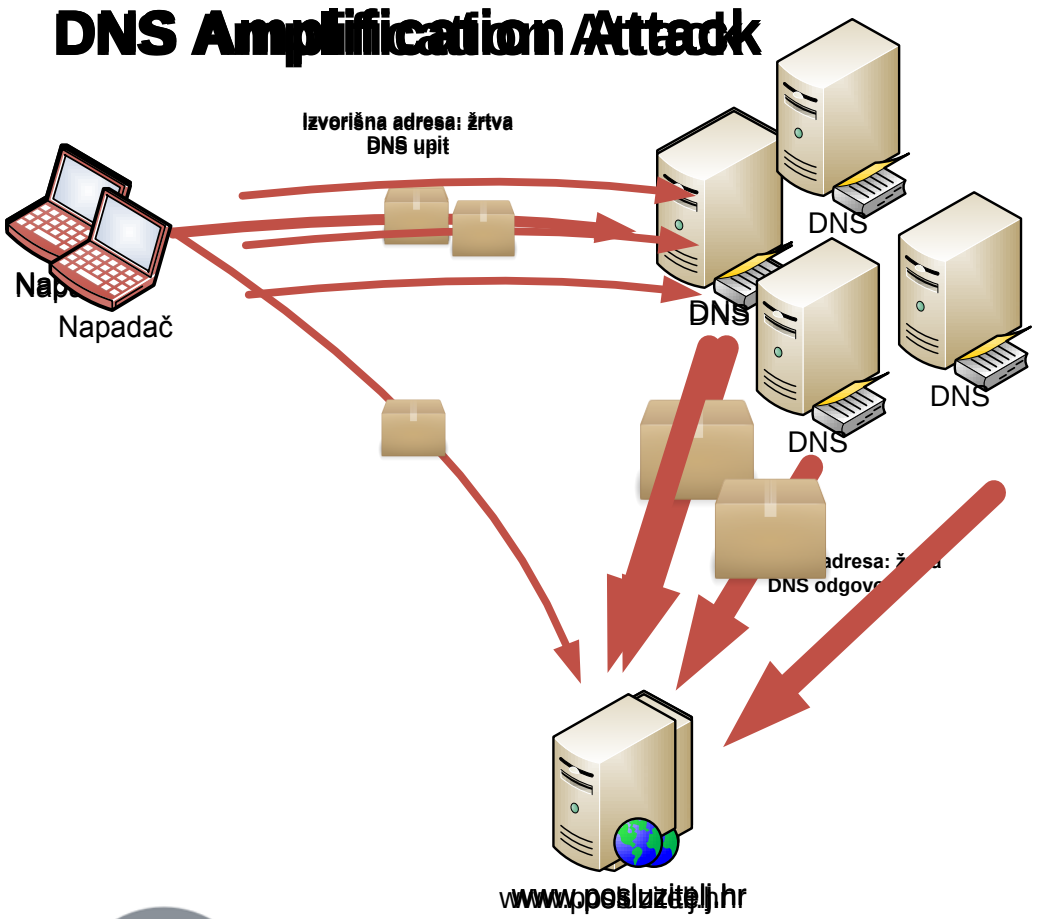
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni
CERT

Primjeri incidenata – DOS napadi

- Raznoliki tipovi napada
- Često veliki obujam napada
- Razne tehnike napada
  - Jednostavni *brute force* napadi
  - Geografski raspodijeljeni napadi (preko 7000 računala u *botnetu*)
  - *DNS amplification* napadi sa faktorom povećanja do 50 puta

Primjeri incidenata – DOS napadi



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Primjeri incidenata – kompleksni napadi

- Napadi pripadaju tipičnim APT (*Advanced Persistent Threat*) napadima
- Dugo pripremani
- Korištene raznih tehnika:
  - Socijalni inženjering
  - Posebno napisan maliciozni softver
  - …
- Nacionalni CERT napravio je reverzni inženjering do tada nepoznatog malicioznog koda

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 CIP-PSP programu
- Trajanje: 30 mjeseci (1.2.2013. – 31.7.2015.)
- 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)
- Cijena 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

Partneri u ACDC projektu koji su članovi konzorcija

- 24 partnera iz 14 zemalja:

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*)

Ciljevi projekta

- Projekt će:
  - 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

Uloga CARNet-a u ACDC projektu

- Uspostava nacionalnog centra za podršku
- Razvoj komponenti koje se odnose na mrežne senzore i alate za detekciju
  - *Honeypot* sustavi
  - *Spamtrap*
  - *Passive DNS*
- Rad sa 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 na neobjavljenim adresama
  - Sav prikupljen mail nužno je neželjen
  - Dodatnom analizom se utvrđuje koji pošiljatelji pripadaju *botnetu*

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

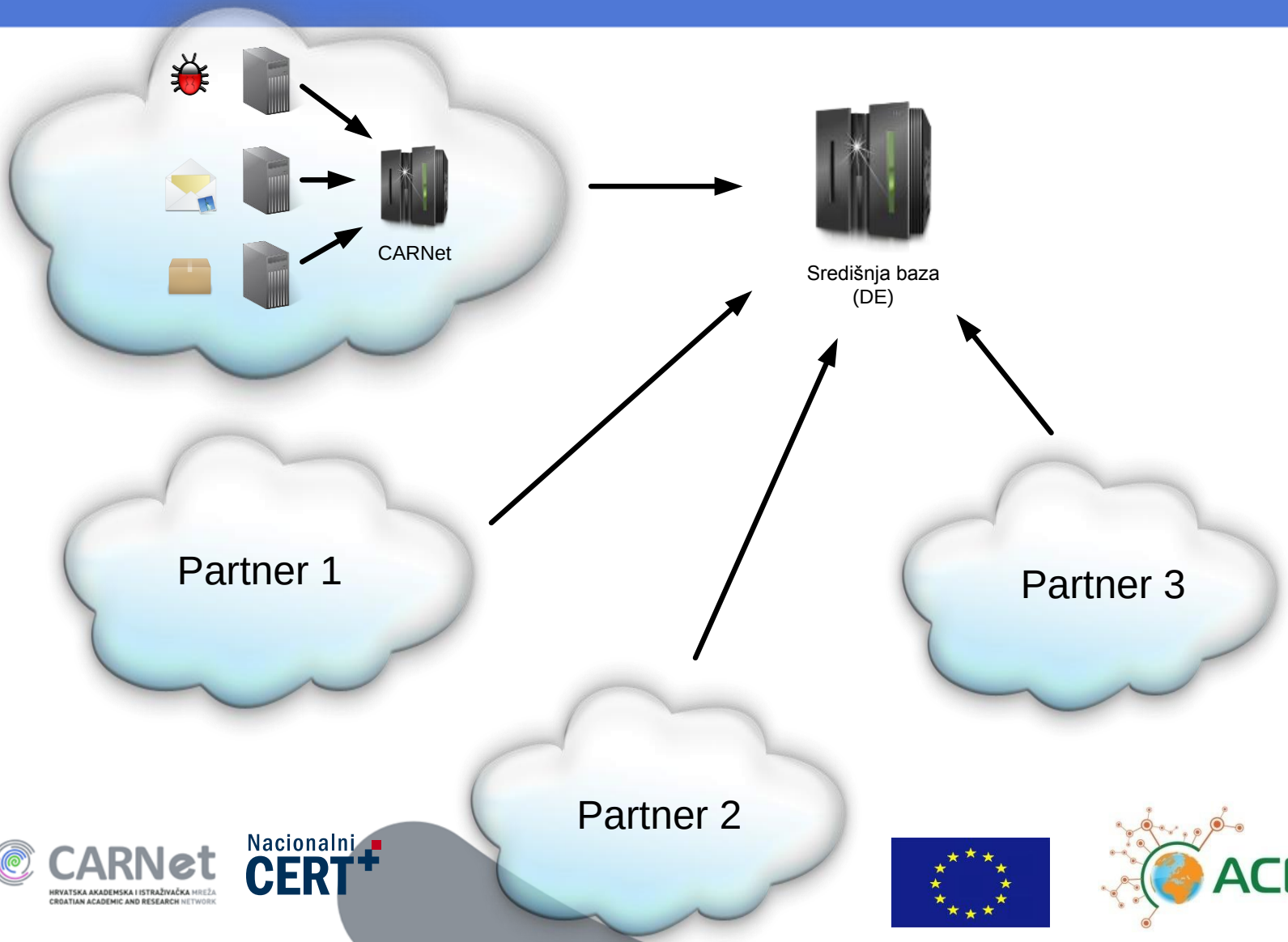
Nacionalni CERT

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* organiziraju komunikaciju između zaraženih računala kako bi izbjegli jednu točku ispada

Uloga CARNet-a u ACDC projektu - pregled



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Pitanja i odgovori

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT