CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Centar za naprednu računalnu zaštitu- platforma EU za sigurnost korisnika Interneta

NCERT-PUBDOC-2015-1-345

Nacionalni CERT

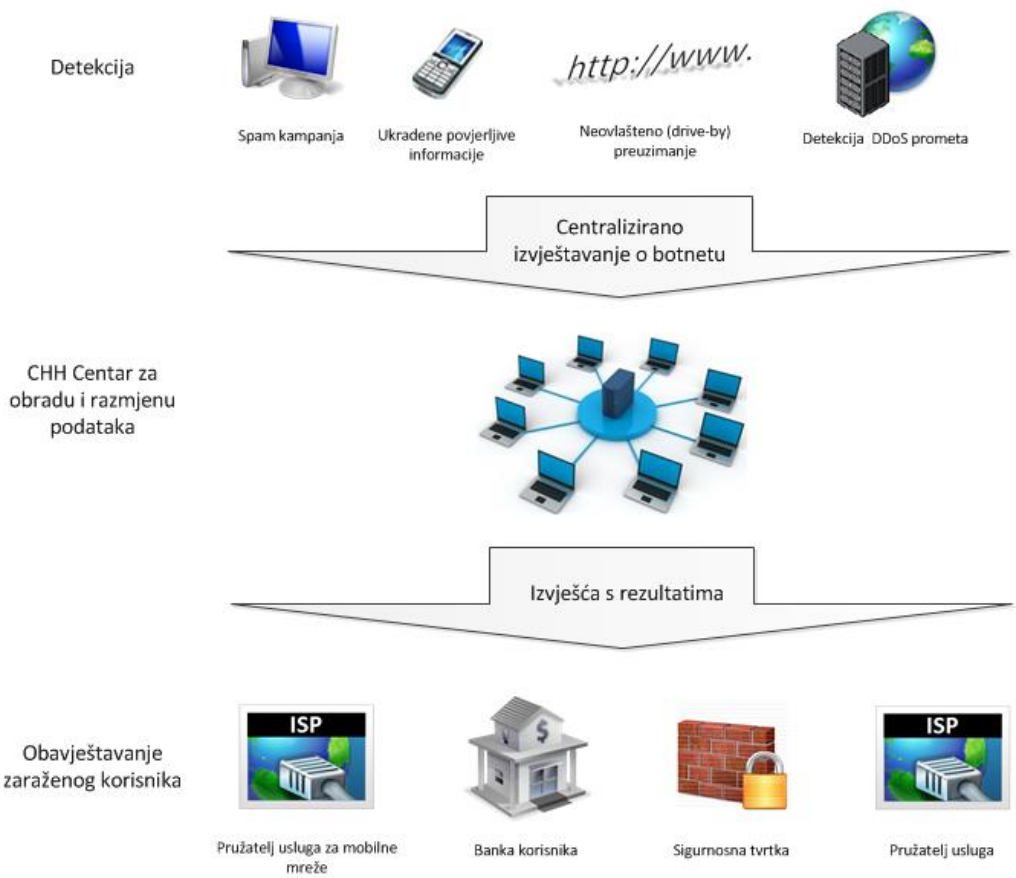
ACDC

Sadržaj

1 Uvod

Advanced Cyber Defence Center (ACDC) je projekt financiran iz okvirnog programa potpore politike za konkurentnost i inovacije u ICT području (CIP-ICT). U projektu sudjeluje 28 partnera iz 14 europskih država, a na čelu konzorcija se nalazi njemačko udruženje internetske industrije ECO.
Glavni cilj projekta je borba protiv botneta i uspostava jedinstvene platforme Europske Unije. Projekt je započeo u veljači 2013. godine i uključuje sljedeće aktivnosti: detekciju botneta, mjerenja, analize, prevencije i oporavak od šteta nastalih djelovanjem botneta.

Plan je uspostaviti osam nacionalnih centara podrške s jednim centrom za obradu i razmjenu podataka (engl. Centralized Clearing House - CCH). Centri podrške u zemljama pojedinih partnera bi trebali pomoći krajnjim korisnicima da pomoću objavljenih usluga i alata na portalu centra otklone, detektiraju ili spriječe sigurnosne probleme na svojim računalima. Na slici 1 prikazani su primjeri velikih korisnika koji imaju i mogućnost dobivanja rezultata vezanih za njihove mreže s time da su sigurnosni incidenti prije bili registrirani na senzorima priključenim na CCH.

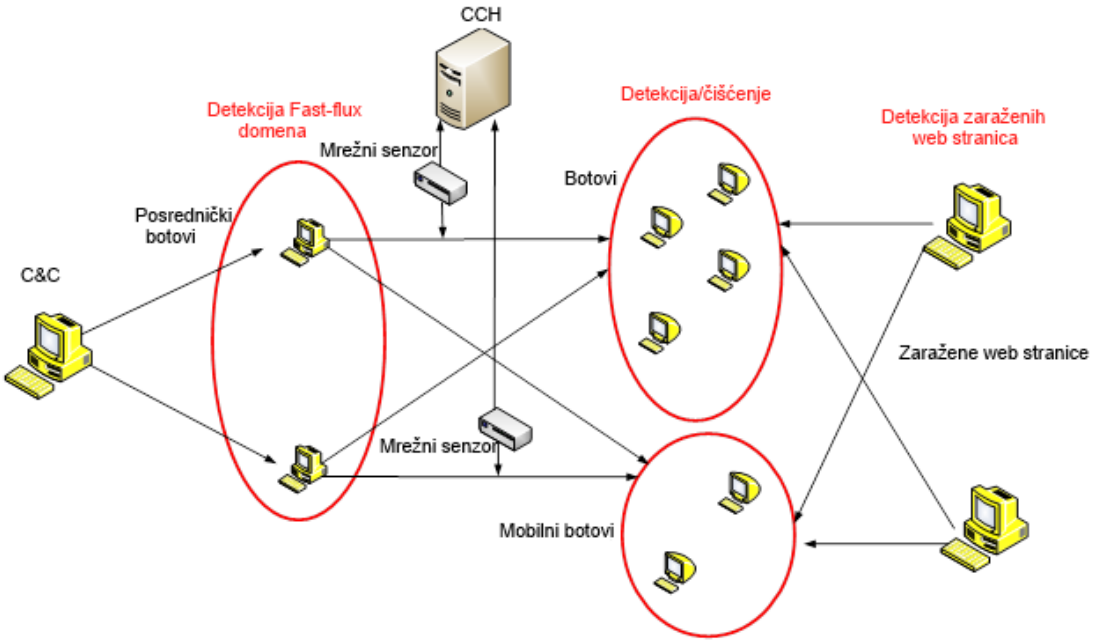


Slika 1. ACDC tok podataka

2 Botneti i načini obrane

Botnet je skup računala koja su zaražena zlonamjernim programom koji omogućava osobi koja upravlja njime, kontrolu nad zaraženim računalima. Pri tome korisnik zaraženog računala nije ni svjestan da mu je računalo zaraženo i da sudjeluje u raznim, obično zlonamjernim aktivnostima. Na taj način zaraženo računalo postaje zombi ili bot (skraćeno od roBOT) koji čeka i izvršava komande koje mu je poslalo glavno računalo odnosno komandno-kontrolni centar.

Centralizirani botneti su vrsta botneta u kojoj su sva zaražena računala povezana s jednim ili više komandno-kontrolnih centara (engl. Command and control centar - C&C). Nakon infekcije zaraženo računalo ostvaruje komunikaciju sa C&C koji ga registrira u svojoj bazi podataka, prati njegov status i šalje naredbe koje treba izvršiti. Upravitelj botneta komunicira s C&C-om i na taj način upravlja cijelom mrežom zaraženih računala. C&C komunicira s botovima preko niza posredničkih računala koja udomljava fast-flux domena. Cilj posredničkih računala je otežavanje detekcije komandnog centra.



Slika 2. ACDC vs botnet

Borba protiv botneta u ACDC projektu se svodi pojednostavljeno na tri akcije: detekciju i ukidanje fast-flux domena, detekciju i ukidanje malicioznih web stranica kojima je cilj primarna infekcija računala koja ih posjećuju, te detekcija i čišćenje zaraženih korisničkih računala od zlonamjernih programa kako je prikazano na slici 2.

Vlasnici fast-flux domena su „cyber“ kriminalci i one služe u najvećem broju slučajeva sakrivanju glavnih C&C poslužitelja. U tu svrhu, koristi se imenički poslužitelj - DNS (engl. Domain Name System) koji omogućava dinamičke promjene IP adresa u domeni.

Fast-flux metode iskorištava mogućnost DNS-a da jednom FQDN-u (engl. Fully Qualified Domain Name) dodijeli na tisuće raznih IP adresa u raznim vremenskim intervalima. Iza

tih IP adresa se kriju botovi koji funkcioniraju kao posrednički poslužitelji, prosljeđujući svu klijentsku komunikaciju do C&C poslužitelja, koji se skriva iza njih.
Vaše računalo/smartphone može postati dio botnet mreže na više načina, a najčešći od njih su: posjećivanje zaraženih web stranica, otvaranje malicioznih privitaka u elektroničkkoj pošti te instalacijom piratskih programa koji u sebi sadrže maliciozni kod.

Način na koji botovi komuniciraju sa C&C poslužiteljem su preko HTTP ili IRC protokola što često omogućava prolaz paketa kroz sigurnosne uređaje (vatrozid, IPS i sl.).
IRC protokol je dizajniran za tip komunikacije „jedan na više“ te time ne ograničava broj korisnika unutar jednog komunikacijskog kanala i to je primarni razlog zašto je postao popularan protokol za botnete. IRC također pruža mogućnost direktne komunikacije i slanja naredbi samo određenim botovima.
Drugi način komunikacije u botnet mreži je putem HTTP protokola koji je zbog svoje prisutnosti na Internetu rijetko kad blokiran i filtriran te se upravo zbog toga koristi u botnetima za upravljanje i kontrolu.

3 ACDC infrastruktura

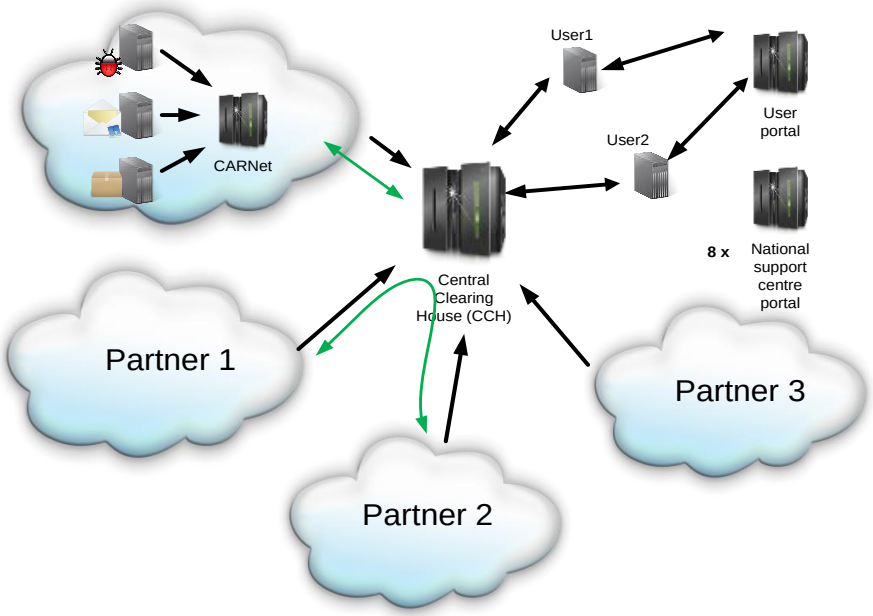
Infrastruktura ACDC platforme se sastoji od 3 glavna dijela (servisa):

1. Centar za obradu i razmjenu podataka (CCH) je središnja točka za pohranu i razmjenu podataka. Pristup podatcima mogu imati veliki korisnici zainteresirani za sudjelovanje u ACDC projektu i članovi konzorcija koji provode projekt.

2. Nacionalni Centri Potpore (NCP) pružaju mogućnost preuzimanja alata za detekciju i uklanjanje zlonamjernih programa te pružaju mogućnost korištenja „online“ sigurnosnih usluga. S njega je moguće preuzeti alat Avira EU-Cleaner, prijenosni antivirusni program koji otkriva i uklanja zlonamjerne programe s vašeg računala. Isto tako je moguće preuzeti DE Cleaner CD za spašavanje sustava, koji služi za spašavanje zaraženog operacijskog sustava. On uklanja zlonamjerne programe s vašeg računala u slučaju da je računalo zaraženo u toj mjeri da se antivirusni program ne može ažurirati ili da se zaražene datoteke ne mogu pobrisati. Portal također sadrži poveznice na mnogo sigurnosnih alata različitih proizvođača. Na stranicama web sjedišta NCP je moguće također aktivirati i online servise koji će povremeno skenirati web sjedište korisnika ili njegovo osobno računalo.

3. Senzori za identifikaciju botova, zlonamjernih web sjedišta i fast-flux domena te malicioznog mrežnog prometa koji su instalirani na infrastrukturi partnera u ACDC konzorciju čija je uloga izvedba projekta.

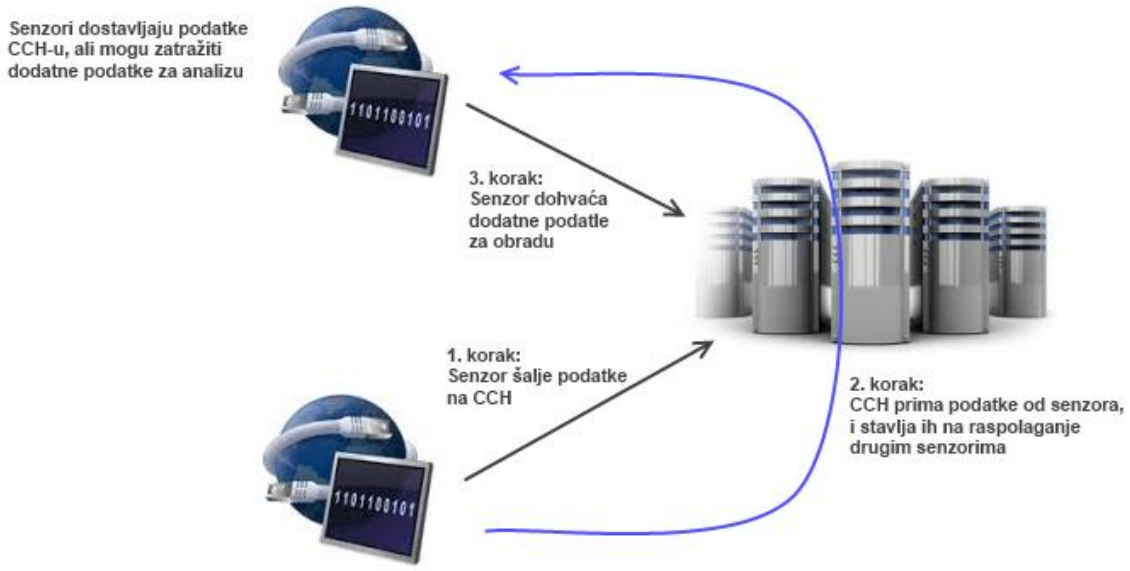
Centralna točka cijelog sustava je CCH (Central Clearing House) koji dobiva izvješća o spam kampanjama, ukradenim podatcima, Fast-flux domenama, DDoS napadima, zlonamjernim web sjedištima i ostale izvještaje o aktivnostima botneta od senzora koji su spojeni na njega. Na taj način CCH može dostaviti davatelju usluge podatke o incidentima u njegovoj mreži, a kasnije davatelj usluge može uputiti svoje korisnike na portal NCP-a gdje je moguće pronaći alate za čišćenje ili provjeru računala. Cijela infrastruktura ACDC projekta je na jednostavan način prikazana na slici 3.



Slika 3. ACDC shema

Senzori se na CCH mogu spajati direktno, ili pak preko posrednika, takozvanih koncentratora sa ulogom koncentriranja i obrade podataka. Koncentratori, na primjer, mogu dohvaćati i analizirati podatke sa senzora, i tek potom rezultat analize slati na CCH, a neki od uređaja mogu također čitati podatke sa CCH i tada ih korelirati te ponovno slati kao rezultat na CCH.
Partneri projekta prikazani na slici 3 pripadaju jednoj od slijedecih grupa: pružatelji internetskih usluga, CERT-ovi, znanstvene ustanove, zakonodavna i administrativna tijela, predstavnici kritične infrastrukture, te proizvođači sigurnosnih rješenja.

Osim pohrane podataka, CCH je dizajniran i za dijeljenje podataka prije navedenima partnerima projekta, a također i za dijeljenje podataka između partnera koji imaju na CCH priključene svoje senzore kao što je to prikazano na slici 4.

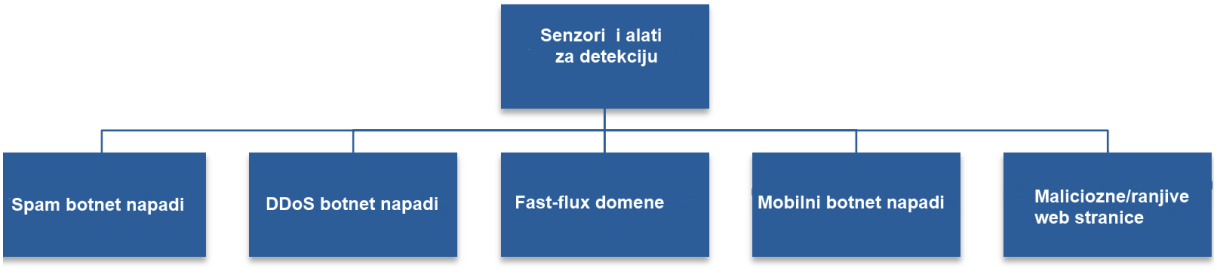


Slika 4. Razmjena podataka između senzora preko CCH-a

Kako bi se partneri ili veliki korisnici pretplatili na pojedine podatke, potrebna je registracija senzora ili velikih korisnika putem „community“ portala. Nakon registracije svaki partner dobiva API ključ kojim je moguće pristupiti traženim podatcima ali u zavisnosti o njihovoj ulozi i autorizaciji.
ACDC projekt je zamišljen da u tehničkom smislu, zajedno sa središnjim CCH, integrira alate i senzore partnera projekta koji su već implementirani u njihovom okruženju sa zajedničkim ciljem borbe protiv botneta gdje se zajedničkim djelovanjem svih članova postiže efikasno i centralizirano rješenje protiv rastuće prijetnje računalnog kriminala.

4 Eksperimenti

U smislu verifikacije rezultata projekta, svaki partner vrši eksperimente na vlastitom adresnom prostoru te ovisno o svojim mogućnostima i dostupnim senzorima u projektu može sudjelovati do maksimalno 5 područja/eksperimenta kako je prikazano na slici 5.



Slika 5. Eksperimenti

Na slici 5 su prikazani sljedeći eksperimenti koji se provode u sklopu ACDC projekta:

- **Spam botnet napadi** - naglasak je na detekciji botova korištenih primarno za slanje spam poruka, preko koji se korisnik zarazi otvaranjem malicioznih URL-ova ili privitaka.

- **DDoS botnet napadi** - naglasak je na prikupljaju informacije o DDoS botnetima i žrtvama DDoS napada.

- **Maliciozne/ranjive web stranice** - naglasak je na razvijanju alata koji ISP-ovi i administratori web stranica koriste kako bi ublažili i očistili malver na web poslužiteljima i detektirali ranjivosti.

- **Mobilni botnet napadi** - naglasak je na poboljšanju sigurnosti korisnika pametnih mobitela. Alati razvijeni u ovu svrhu provjeravaju konfiguraciju, analiziraju konekcije i upozoravaju korisnika ukoliko je uspostavljena maliciozna veza, odnosno ako je pametni mobitel dio mobilnog botneta.

- **Fast–flux domene** - naglasak je na detekciji Fast-flux domena koje botneti koriste za prikrivanje C&C servera.

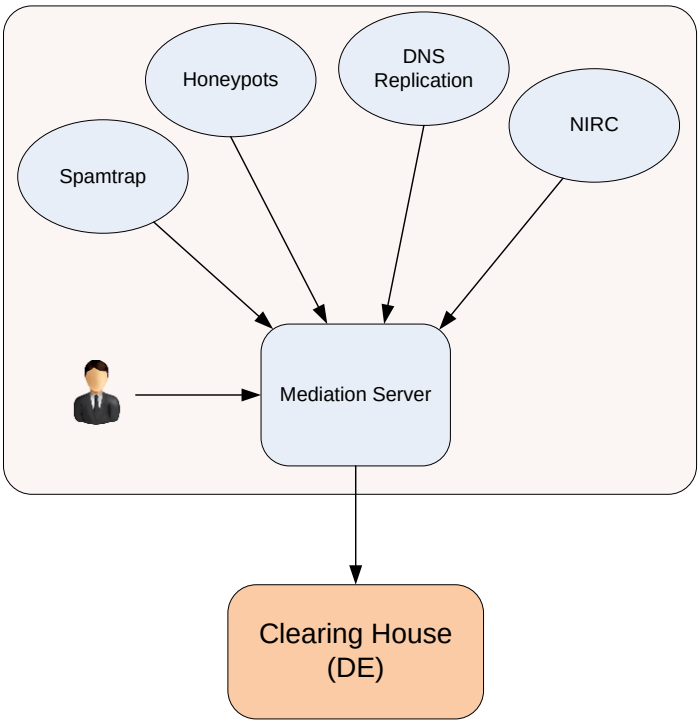
5 Uloga CARNeta u projektu

CARNet je jedan od ravnopravnih partnera ACDC projekta u kojem sudjeluje u sklopu 3 područja borbe protiv botneta: detekciji spamova, detekciji fast-flux domena i detekciji RFI (engl. Remote file inclusion) napada na web sjedišta. U sklopu projekta, CARNet je razvio svoj softver i dodatno koristi open source programsku podršku za sljedeće senzore:
Spamtrap senzor je vrsta senzora koja prikuplja podatke vezane za spam botnete čija je primarna svrha slanje spam poruka. Pomoću spam poruka se u velikom broju slučajeva napadaju krajnji korisnici na način da prenose zarazu na računala krajnjih korisnika. Računalo se može zaraziti ukoliko korisnik otvori zaraženu web stranicu čija se poveznica nalazi u spam poruci ili otvaranjem malicioznog programa u privitku poruke. Ovisno o vrsti senzora, primaju se ulazni podatci poput e-mail privitaka, tijela spam poruke, e-mail logova i slično. Senzor potom vrši analizu i šalje podatke o otkrivenim botnet aktivnostima CCH-u.

Fast-flux senzor je orijentiran na detekciju sustava i domena koje se upotrebljavaju za fast-Flux aktivnosti na Internetu, a kao input koristi komunikaciju između dva DNS poslužitelja.

Honeypot senzor je vrsta senzora koja za potrebe projekta prikuplja jedino informacije o RFI napadima na web sjedišta.

Poslužitelj za medijaciju i korelaciju podataka je centralni server smješten na strani partnera koji periodički dohvaća podatke prikupljene od strane senzora te ih obrađuje i sprema u svoju centralnu bazu podataka. Pruža grafičko sučelje u kojem je moguće dobiti informacije o stanju senzora i pristup prikupljenim podatcima. Na njemu se odvija i obrada prikupljenih podataka (deduplikacija, skeniranje u potrazi za malicioznim kodom, te ostale vrste detekcije i korelacije).



Slika 6. Prikupljanje, obrada i slanje podataka u CARNet mreži

6 Zaključak

ACDC je pilot projekt koji je jedinstven po svojoj namjeri da konsolidira i udruži rezultate pojedinih sigurnosnih alata koji su već prije bili u funkciji kod pojedinih partnera koji učestvuju u projektu. Takvim udruživanjem postiže se više ciljeva, kao što je implementacija centralnog mjesta sa podacima o incidentima registriranim u EU, te mogućnost korelacije tih podataka sa mogućnosti centralnog izvještavanja. Udruživanje i konsolidacija rezultata na jednom mjestu također daje daleko bolji sinergijski učinak nego rezultati svakog pojedinog alata. Distribuirani nacionalni centri podrške, sa druge strane, omogućavaju u 8 zemalja EU centralno mjesto na kojem krajnji korisnici mogu pronaći sigurnosne alate koji će im pomoći u prevenciji i čišćenju infekcija što može rezultirati smanjenjem broja infekcija pod uvjetom da davatelji usluge pristupa Internetu izvještavaju svoje korisnike o postojanju infekcije na njihovom računalu.

Poveznice:
http://www.antibot.hr
http://www.acdc-projekt.eu
http://www.cert.hr

Ovaj dokument pripremljen je uz financijsku podršku Europske unije. Sadržaj rada izražava
mišljenje autora i ni na koji način ne izražava mišljenje i stavove Europske unije.