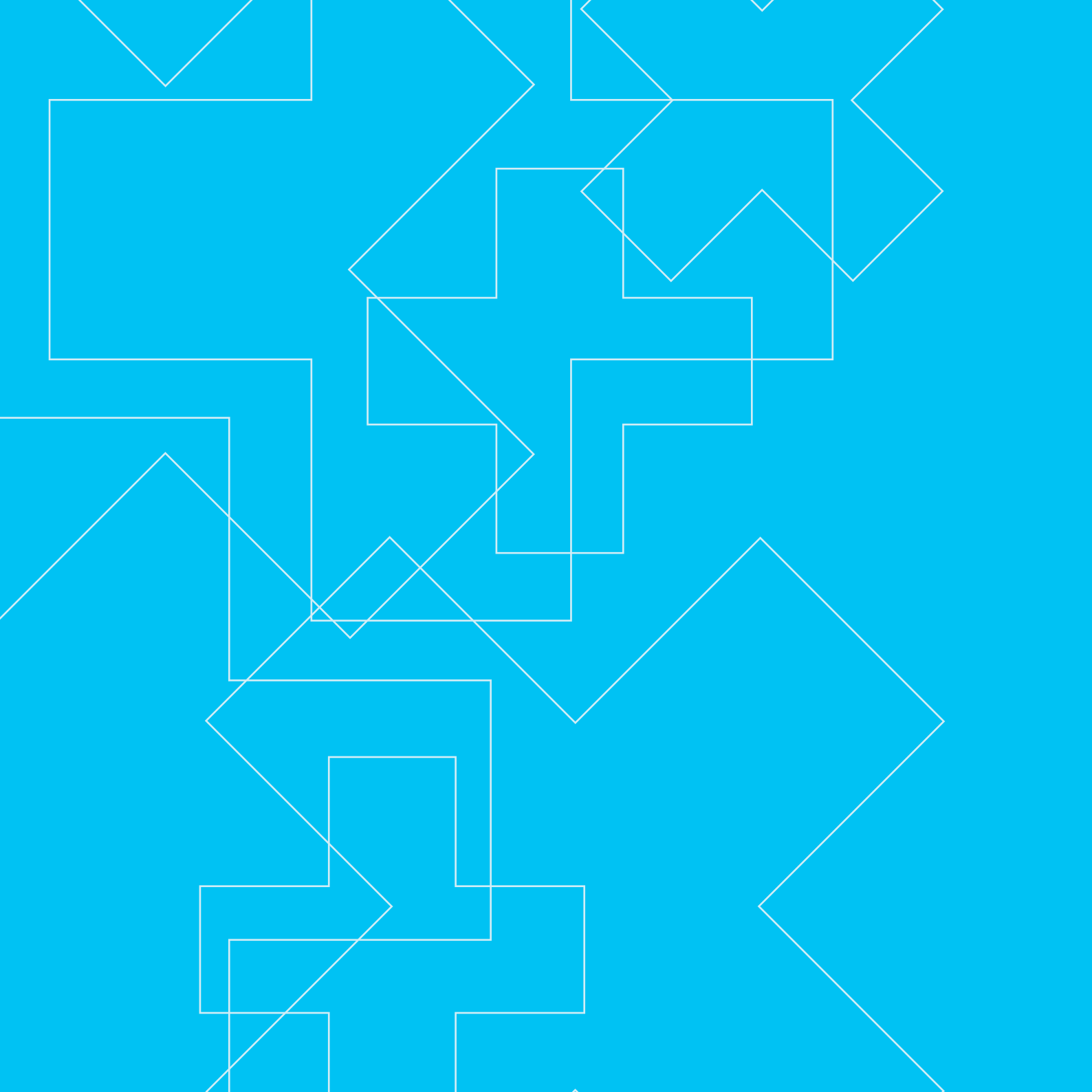
Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

IZVJEŠĆE O AKTIVNOSTIMA NACIONALNOG CERT-A.

Pregled sigurnosti na Internetu u RH i u svijetu u 2015. godini



Sadržaj

1. Usluge Nacionalnog CERT-a

U 2015. godini Nacionalni CERT, odjel Hrvatske akademske i istraživačke mreže - CARNeta, nastavio je svoju proaktivnu i reaktivnu ulogu kako bi se smanjio rizik od pojave sigurnosnih incidenata i umanjila šteta pri njihovom nastupanju. U tom je smislu Nacionalni CERT svakodnevno obavljao sljedeće usluge:

1.1. Proaktivne mjere:

- Svakodnevno izdavanje sigurnosnih preporuka za najpopularnije operativne sustave
- Izdavanje i objavljivanje tehničkih dokumenata o temama iz područja informacijske sigurnosti
- Izdavanje i objavljivanje tehničkih informacija o sigurnosnim alatima
- Praćenje i objavljivanje novosti koje su povezane sa sigurnošću Interneta
- Provjera ranjivosti ustanova članica CARNet mreže
- Provjera ranjivosti vanjskih korisnika u RH po dogovoru
- Informiranje javnosti putem portala www.antibot.hr s ciljem suzbijanja botova

Sljedeća tablica prikazuje broj objavljenih objava ili izvršenih proaktivnih mjera u 2015. godini.

Tablica 1. Prikaz broja izvršenih proaktivnih mjera

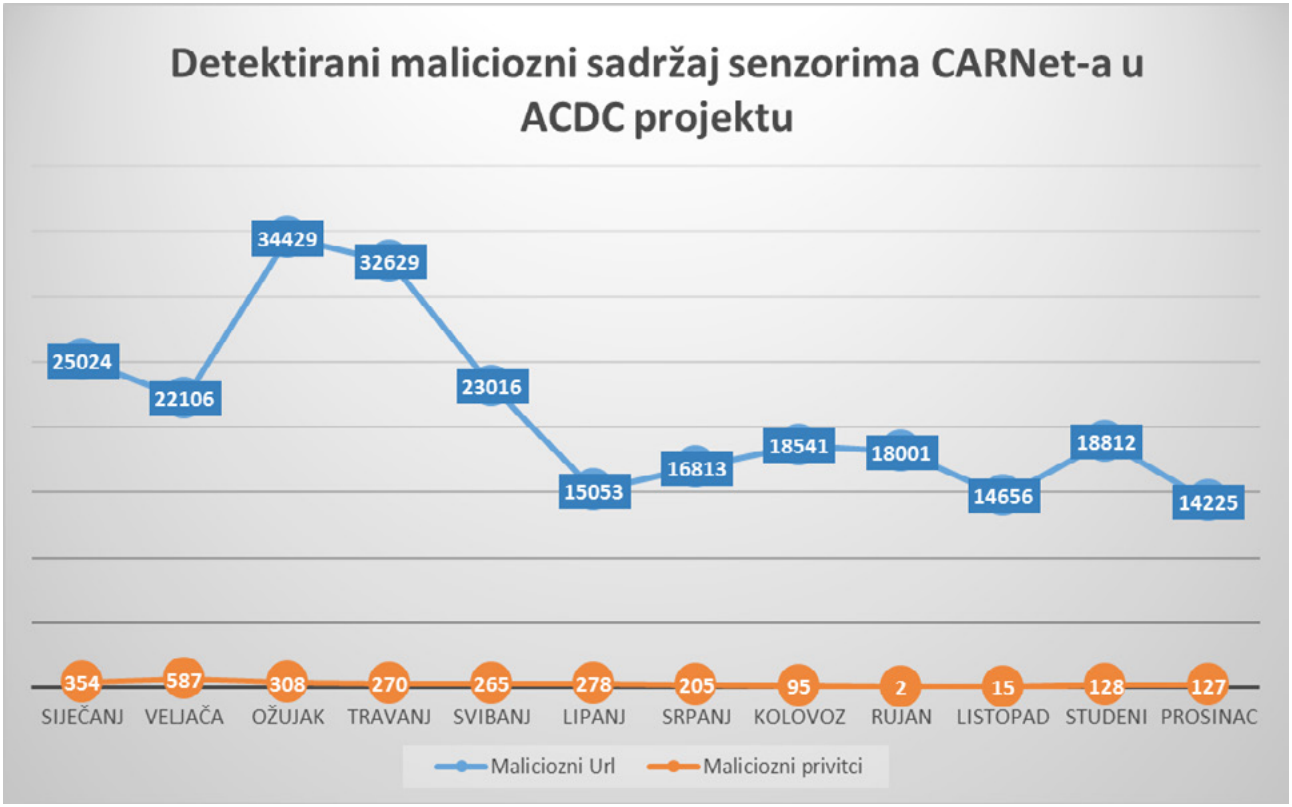
Alati	19
Dokumenti	2
Novosti	105
Ukupno preporuka	2402
Broj provjera ranjivosti	227

Slika 1. Ekranski prikaz portala antibot.hr

Nacionalni centar potpore **„Antibot“** omogućuje krajnjim korisnicima bolju detekciju i uklanjanje malicioznog koda s njihovih radnih stanica, *online* usluge poput provjere ranjivosti *web* preglednika ili otvorenih *portova* na korisničkoj opremi te usluge periodičke provjere ranjivosti *web* sjedišta. Isto tako, putem portala dostupni su i drugi sigurnosni alati, poput alata za detekciju tzv. napada MITB (*„Man In The Browser“*), koji može otkriti aktivnosti bankovnog malicioznog koda na računalu te specijalizirani alat za detekciju tzv. *ransomwarea*. Sve usluge i alati dostupni su putem portala www.antibot.hr.

Pružatelji internetskih usluga (Internet Service Provider - ISP) u Republici Hrvatskoj obaviješteni su o postojanju portala www.antibot.hr i upućeni su u njegovu svrhu. Prema povratnim informacijama, većina ISP-ova upućuje svoje korisnike na portal radi skeniranja i čišćenja kompromitiranog korisničkog računala antivirusnim alatom. Slično je i kod klijenata domaćih banaka. Provođenje svih tih mjera sasvim će sigurno rezultirati smanjenjem broja zaraženih računala krajnjih korisnika i povećanjem sigurnosti Interneta u RH.

Pomoću instaliranih senzora unutar većih ISP-ova i fakulteta u Hrvatskoj CARNet (Nacionalni CERT) može detektirati aktivne zlonamjerne domene kojima pristupaju zaražena korisnička računala. Također se prikuplja i analizira neželjena elektronička pošta *(spam)* koja može sadržavati zlonamjerne URL-ove ili privitke. Takva elektronička pošta najčešće je prvi korak pri infekciji računala krajnjeg korisnika. Rezultati koji detaljno prikazuju maliciozne neželjene elektroničke poruke *(spam)* također se mogu naći na portalu www.antibot.hr.



1.2. Reaktivne mjere:

- Obrada incidenata (svi korisnici u RH, uključujući korisnike CARNeta)
- Prikupljanje podataka o kompromitiranim računalima i njihovim aktivnostima s izvora na Internetu i njihova analiza
- Prikupljanje i analiza podataka o napadima dobivenih sa sustava ili senzora
- Abuse služba CARNet mreže
- Godišnje i mjesečne statistike Abuse službe i zabilježenih incidenata

1.3. Provjera ranjivosti

CARNet već niz godina nudi uslugu redovite provjere ranjivosti ustanova članica koje su priključene na CARNet mrežu. Redovita provjera ranjivosti obavlja se periodički svaka tri mjeseca, a rezultat ove provjere izvještaj je koji sadrži listu pronađenih sigurnosnih propusta i upute za njihovo rješavanje. Ovu uslugu koristi oko 60 ustanova članica. Budući da je na CARNetovu mrežu spojeno više od 2350 ustanova iz sustava prosvjete, visoke naobrazbe, kulture te neka državna tijela, stručnjaci Nacionalnog CERT-a radili su na projektu masovnog skeniranja ranjivosti CARNet mreže. U okviru tog projekta razvijeni su alati za upravljanje programom (softverom) za provjeru ranjivosti (Nessus®) pomoću kojih se automatizirano i u kratkom vremenu provjeri velik broj ustanova. Automatizirano masovno skeniranje omogućava softverska komponenta SPORt (sustav za pohranu, obradu i preuzimanje rezultata), razvijena u Nacionalnom CERT-u. SPORt omogućava dostavu izvještaja o pronađenim ranjivostima putem *web* sjedišta uz prethodnu prijavu administratora. Tijekom 2015. godine obavljene su dvije takve provjere kojima je obuhvaćeno gotovo 1000 ustanova spojenih stalnom vezom na CARNet mrežu, nakon čega je napravljena analiza rezultata te su rangirane ustanove prema razini pronađenih ranjivosti. Rezultati obavljenih provjera dali su uvid u sigurnosno stanje CARNet mreže te smjernice za daljnje planiranje s ciljem smanjenja broja ranjivosti.

2. Suradnja Nacionalnog CERT-a s institucijama izvan RH

Pored institucija **EU-a** i **NATO-a**, Nacionalni CERT surađuje s međunarodnim asocijacijama CERT-ova **FIRST** *(Forum for Incident Response and Security Teams)* i **TI** *(Trusted Introducer)* kao akreditirani član.

enisa European Union Agency for Network and Information Security

Nacionalni CERT pomagao je *Agenciji Europske unije za mrežnu i informacijsku sigurnost* (ENISA) u izradi nastavnih materijala koji omogućuju bolju obuku nacionalnih CERT-ova u području analize sigurnosnih prijetnji, odnosno *malvera*. Stoga je ENISA odala važno priznanje stručnjacima Nacionalnog CERT-a, odnosno CARNeta, koji su svojim savjetima sudjelovali u izradi navedenih nastavnih materijala.

3. Suradnja i djelovanje Nacionalnog CERT-a unutar RH

3.1. Nacionalna strategija kibernetičke sigurnosti (NSKS)

Nacionalni CERT sudjelovao je u procesu izrade Nacrta prijedloga Nacionalne strategije kibernetičke sigurnosti za koji je Ured Vijeća za nacionalnu sigurnost proveo postupak savjetovanja sa zainteresiranom javnošću od 27. travnja do 27. svibnja 2015. godine. Pojam „kibernetički“ uveden je u pravni poredak RH ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu prije 12 godina. Slijedom toga, uvriježilo se koristiti pojam „kibernetički“ u obliku pridjeva za nešto što uključuje ili koristi računala, a osobito Internet, ili je povezano s njima.
S obzirom na to da se radi o prvoj sveobuhvatnoj Strategiji u RH u području kibernetičke sigurnosti, primarni je cilj Strategije prepoznavanje organizacijskih problema u njezinoj provedbi te širenje razumijevanja važnosti ove problematike u društvu. Poticanje koordinacije i suradnje svih državnih tijela i pravnih osoba s javnim ovlastima, ali i drugih sektora društva, nužno je kako bi se uspostavile nove funkcionalnosti, podigla učinkovitost rada relevantnih aktera te učinkovitije koristilo postojeće resurse i bolje planiralo potrebu i ostvarenje novih resursa.

3.2. Djelovanje preko javnih medija i obraćanje javnosti

Nacionalni je CERT s ciljem podizanja svijesti o informacijskoj sigurnosti djelovao kroz sljedeće aktivnosti:
- izdao novu inačicu (br. 3) popularne brošure „Zaštitite privatnost na Facebooku“
- nastupio na HRT-u u emisiji „Potrošački kod“ gdje se raspravljalo o problematici zaštite privatnosti na društvenim mrežama
- održao niz predavanja na domaćim konferencijama i prezentacija akademskoj zajednici, javnim i privatnim institucijama te široj javnosti, između ostalih: „Korporativna sigurnost 2015“, “FSEC 2015“ i „Internet Security Days 2015“
- upozorio korisnike AAI@EduHr identiteta o prijetećim *phishing* kampanjama.

Mnogo informacija bilo je diseminirano putem web sjedišta Nacionalnog CERT-a, čiji je ukupni broj posjeta u 2015. godini bio 338.166. Broj posjeta porastao je u odnosu na prethodnu godinu, i to za 21 % .

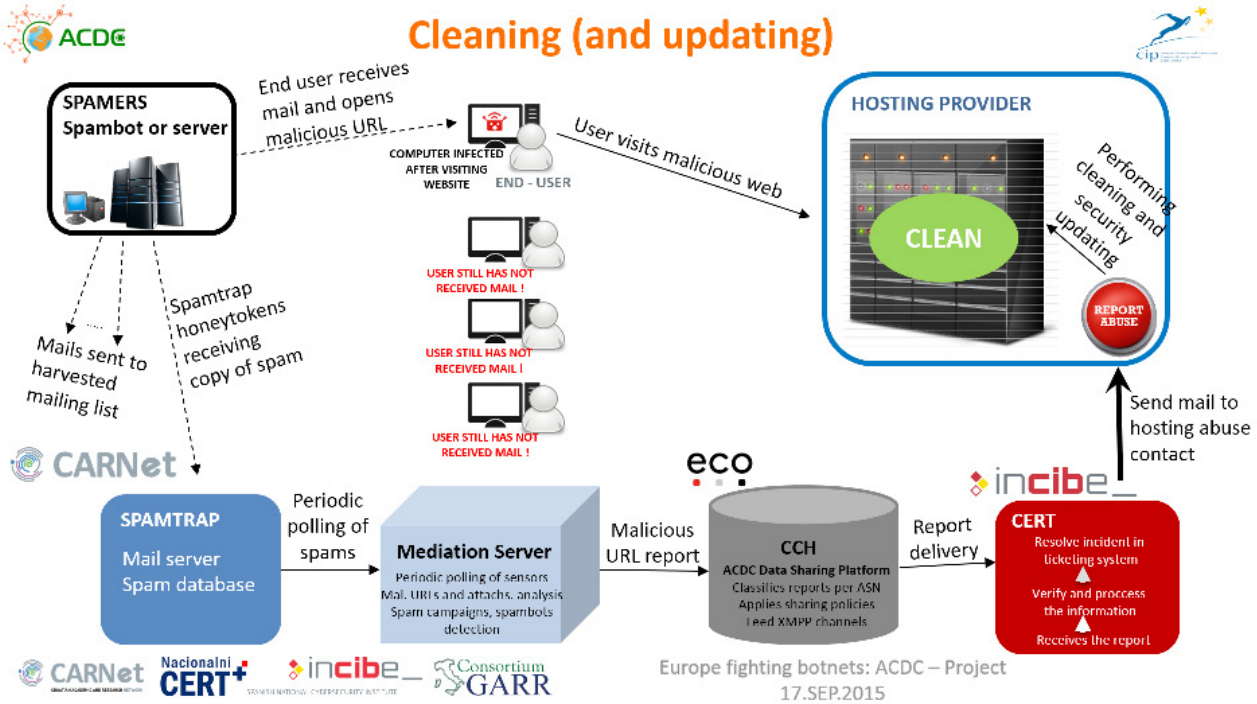
4. Suradnja i sudjelovanje na projektima

4.1. e-Škole

Nacionalni CERT sudjelovao je u planiranju, dimenzioniranju i testiranju sustava SIEM *(Security Information and Event Management)* s ciljem unaprjeđenja sigurnosnog nadzora CARNetove računalne i mrežne infrastrukture u stvarnom vremenu. Implementacijom sustava SIEM planirano je sigurnosnim nadzorom obuhvatiti sve CARNetove kritične resurse koji se koriste u informacijskoj infrastrukturi projekta e-Škole. Tijekom postupka testiranja koje je provedeno analizom stvarnog prometa s niza računalnih i mrežnih uređaja ispitano je nekoliko sustava SIEM koji omogućuju obradu velike količine podataka u stvarnom vremenu, preciznu detekciju sigurnosnih ugroza i pravovremeno alarmiranje, uz naglasak na mogućnost prilagodbe SIEM-a specifičnim potrebama CARNetove infrastrukture.
Po završetku testiranja Nacionalni CERT izradio je tehničku specifikaciju i dimenzioniranje sustava SIEM te definirao plan implementacije, što je iskorišteno za izradu dokumentacije za javno nadmetanje s ciljem nabave adekvatnog SIEM rješenja.

4.2. ACDC

U veljači je održana radionica projekta ACDC za kritičnu infrastrukturu u kojoj su sudjelovali predstavnici HŽ-a, Croatia Airlinesa, Janafa, Hrvatske kontrole zračne plovidbe, Plinacroa i dr.
Glede tehničkog dijela projekta ACDC, implementirano je prikupljanje podataka iz središnje baze podataka *(Central Clearing House)* i dizajnirana pripadajuća lokalna baza podataka u kojoj se spremaju prikupljeni podaci koji se odnose na računalnosigurnosne incidente u Hrvatskoj.
Nacionalni je CERT u sklopu radnog paketa 3 sudjelovao u pisanju periodičnih izvještaja za *spam*-eksperiment te je bio suvoditelj tog eksperimenta koji je izrađivao sumarne izvještaje svih partnera u projektu. Provedena su i stres-testiranja senzora i testovi funkcionalnosti slanja podataka prema središnjoj bazi podataka.
U travnju je Nacionalni CERT sudjelovao na završnom sastanku radnog paketa 2 na kojem je prezentiran rad mrežnih senzora. U rujnu se održao završni sastanak cijelog projekta u Bruhlu (Njemačka) na kojem su prezentirani rezultati rada pred revizorima. Na tom je sastanku Nacionalni CERT demonstrirao rad svojeg uređaja *spamtrap* u stvarnom primjeru detekcije malicioznog URL-a u *spam*-poruci i prosljeđivanja podataka od senzora do krajnje točke (zaraženog korisnika) putem središnje baze podataka.



Uspješno uklonjen malver s poslužitelja. Tijek međudjelovanja partnera projekta u sklopu spam-eksperimenta, demonstriran na stvarnom primjeru (završni review u Bruhlu u Njemačkoj, 17.9.2015.).

Nacionalni CERT i nakon završetka projekta nastavlja koristiti infrastrukturu iz projekta. Velik dio prijavljenih incidenata dolazi upravo iz središnje baze podataka ACDC-a.

4.3. HR-MISP

U svibnju je potpisan memorandum o uspostavi platforme HR-MISP za dijeljenje podataka o zloćudnom kodu. Platforma MISP *("Malware Information Sharing Platform")* platforma je otvorenog koda koja omogućava suradnju i dijeljenje informacija pri rješavanju računalnih incidenata, digitalnoj forenzici zloćudnog koda i dr.

HR-MISP neutralna je i neprofitna platforma koju održava Nacionalni CERT na svojoj infrastrukturi bez naknade. Pristup platformi mogu dobiti pravne osobe koje se više godina profesionalno bave sigurnošću informacijskih sustava.

Informacije unesene u platformu označavaju se oznakom protokola *Traffic light.*

5. Stanje računalnih incidenata i statistike

5.1. Statistika o obrađenim incidentima koji su prijavljeni Nacionalnom CERT-u

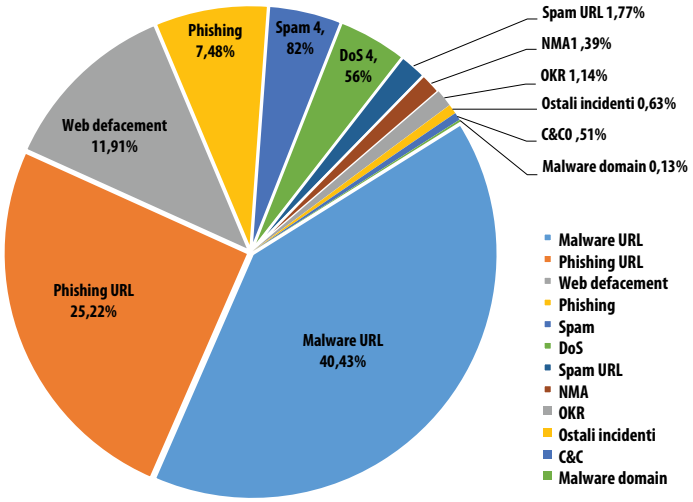
Nacionalni je CERT u 2015. godini zaprimio i obradio ukupno 789 prijava koje se mogu klasificirati kao računalni incidenti u nadležnosti Nacionalnog CERT-a.
Vodeći tip incidenata predstavlja kompromitirano *web* sjedište s malicioznim kodovima i *phishing* stranicama. Najznačajnija promjena u odnosnu na prethodnu godinu rast je broja zlonamjernih URL-ova kojima se uređaji krajnjih korisnika mogu zaraziti malverom. Često su ti URL-ovi povezani s rastućom prijetnjom ***„ransomwarea“***, tipa malvera. Drugi važan faktor **napadi** su **uskraćivanjem usluge** čiji je broj porastao za gotovo 50 % u odnosu na prošlu godinu. To je povezano s rastućim brojem hakerskih skupina u regiji koji traže otkupninu od kompanija kako bi obustavili DDoS napade.
U odnosnu na 2014. godinu, broj *web defacement*-incidenata značajno je manji, što je smanjilo ukupni broj incidenata. Međutim, riječ je samo o prividnom smanjenju jer je Nacionalni CERT dobio manje prijava putem svojih automatiziranih kolektora incidenata (SRU-a). Broj upravljačkih poslužitelja botnet mreža unutar RH pao je na samo četiri u jednoj godini, što je, vjerujemo, rezultat kontinuiranog rada unutar projekta **ACDC.**

TIP INCIDENTA	BROJ	
Malver URL	319	▲
Phishing URL	199	▼
Web defacement	94	▼
Phishing	59	▲
Spam	38	
DoS	36	▲
Spam URL	14	
Nedozvoljena mrežna aktivnost	11	
Ostala kompromitirana računala	9	
Ostali incidenti	25	
C&C	4	▼
Malver domena	1	
UKUPNO	**789**	

Tablični prikaz incidenata po tipu u 2015. godini:


http://www
scam!
User:
Password:

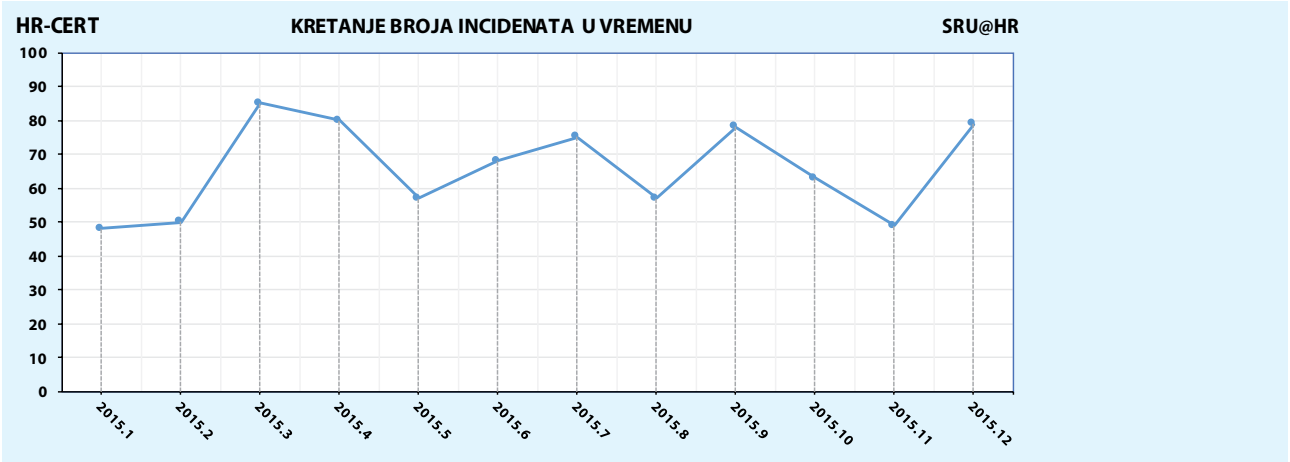
5.2. Raspodjela incidenata po tipu:



Prijavitelji su incidenata, kao i u prošloj godini, u većini slučajeva bili izvan Republike Hrvatske ili je incidente registrirao softver SRU@HR, odnosno dobiveni su od partnera putem projekta ACDC.

5.3. Trendovi pojava incidenata na poslužiteljima u 2015. godini

Sljedeća slika prikazuje broj obrađenih incidenata na poslužiteljima na mjesečnoj bazi, koji su prošli kroz *„ticketing“* sustav Nacionalnog CERT-a.



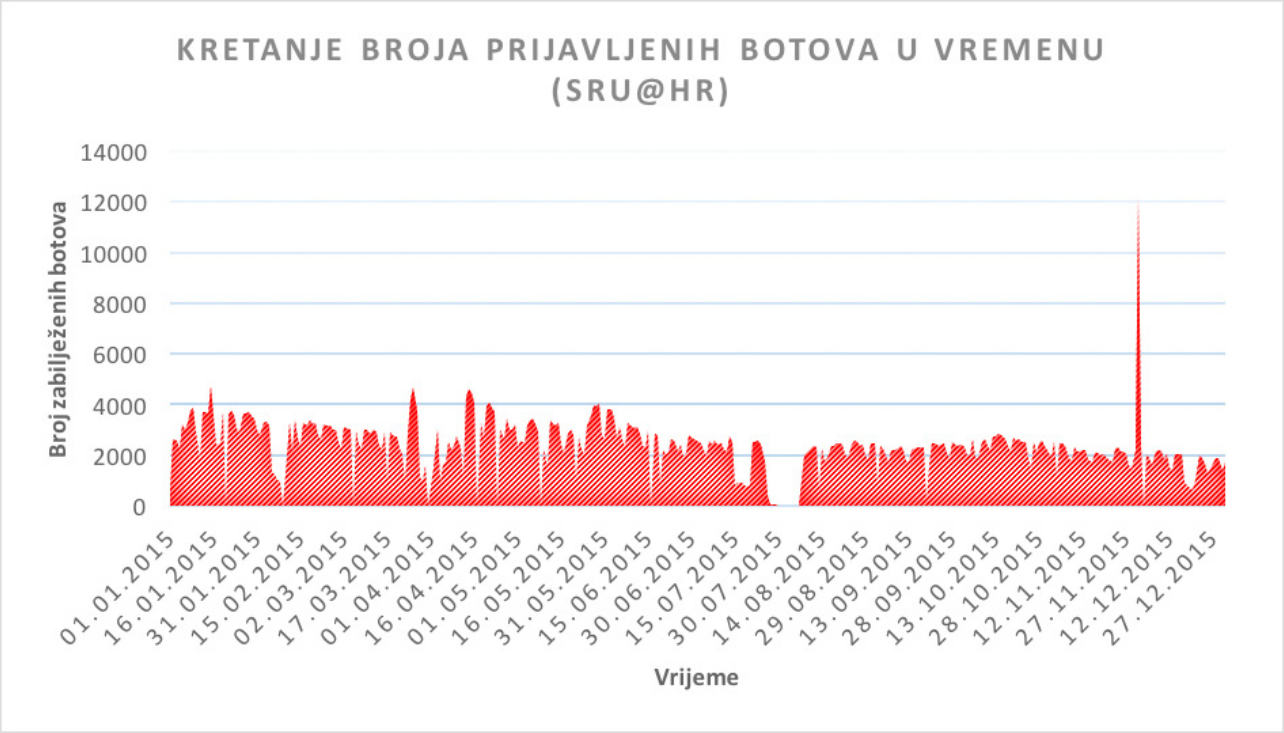
5.4. Registrirani botovi u RH

Nacionalni je CERT primao i statistički obrađivao podatke o botovima na računalima krajnjih korisnika. Podaci su prosljeđivani pripadajućim davateljima internetskih usluga i pružateljima usluga udomljavanja Internet stranica *(hosting provider)*. Iz grafa koji prikazuje godišnji trend broja botova moguće je očitati da je u RH broj registriranih zaraženih računala u stagnaciji i da ih u prosjeku ima manje nego prošle godine. Broj otkrivenih botova prikazan ovim statistikama temelji se na vanjskim izvorima koji dostavljaju podatke Nacionalnom CERT-u te ne odgovara broju stvarno zaraženih korisničkih računala, ali prikazuje trend i okvir stvarnog stanja.

Raspodjela i trend broja prijavljenih botova kroz godinu dana koji su bili diseminirani davateljima usluge pristupa Internetu:

Tablični prikaz prikazuje najveći izmjereni broj pojedinih botova u jednom danu tijekom 2015. godine.

NEPOZNATO	**9746**	
Conficker	2319	▼
Tinba	1822	▲
Bamital	1388	
Geodo	1051	
ZeroAccess	620	▼
Zeus	340	
Sality	314	
XcodeGhost	287	
Cutwail	246	
Kovter	223	
Ponmocup	205	
Virut	154	
CoreBot	125	
Pushdo	106	



Broj botova u odnosu na prethodnu godinu značajno je pao. Zloglasni bankarski bot **Zeus** pao je s preko 30.000 (potencijalno) zaraženih računala na samo 340, dok je **Conficker** pao s preko 18.000 na oko 2300. **Tinba** („Tiny Bankar“) bio je stalna prijetnja te je pogodio i klijente nekih domaćih banaka.

6. Značajniji incidenti, otkrivene ranjivosti i događaji u 2015. godini

1. KVARTAL

Putem asocijacije CERT-ova **Trusted Introducer** u siječnju je prijavljeno kako je veći broj zaraženih računala iz Hrvatske zaraženo DDoS botovima **„Madness“** i **„Ferret“**. Računala su se koristila za napade uskraćivanjem usluge.

U veljači je zabilježena *phishing* kampanja na korisnike CARNetovog AAI identiteta. Napadači su koristili kopiju stranice za pristup elektroničkoj pošti.

U CARNetu je u utorak, 17. veljače 2015. godine, održana prezentacija EU- projekta Centra za naprednu računalnu zaštitu (ACDC – *Advanced Cyber Defence Centre*) i Nacionalnog CERT-a s ciljem informiranja predstavnika **kritične informacijske i komunikacijske infrastrukture** o svim aspektima projekta i aktivnostima Nacionalnog CERT-a.

Što se tiče globalne mreže, prvi kvartal obilježilo je kompromitiranje baze podataka *web* portala za pronalaženje partnera, Ashley Madison. Oteto je ukupno 37 milijuna korisničkih podataka. S obzirom na vrlo visok stupanj osjetljivosti tih podataka, ovo je definitivno jedan od najvećih hakerskih upada u neki informacijski sustav u povijesti.

U veljači je američka privatna osiguravajuća kuća **Anthem** objavila da je oteto 80 milijuna zapisa o klijentima koji koriste njihovo zdravstveno osiguranje. Kaspersky, Interpol i Europol objavili su u veljači da su otkrili najveću *cyber* pljačku banaka u povijesti. Eksperti tvrde da su u pljački sudjelovali hakeri iz Rusije, Ukrajine, ostalih dijelova Europe te iz Kine. Tijekom dvije godine pokušana je pljačka čak 100 financijskih institucija, a ukradeno je nevjerojatnih **milijardu američkih dolara.**

Istraživači su u ožujku otkrili još jednu ranjivost kod SSL klijenata. Ova ranjivost napadačima je omogućavala promjenu postavki kod klijenata tako da koriste slabije šifriranje i izvođenje napada *„man-in-the-middle“* nakon toga. Takav napad nazvan je **FREAK** (Factoring RSA Export Keys). Napad je pogađao nekoliko SSL implementacija, između ostalih i **OpenSSL**.

U ožujku je nekoliko dana u tijeku bila **intenzivna *phishing* kampanja** prema korisnicima **internetskog bankarstva** u Republici Hrvatskoj. Napadači su se u phishing poruci predstavljali kao banka.

2. KVARTAL

Od 27. travnja do 27. svibnja trajao je postupak izrade Nacrta prijedloga **Nacionalne strategije kibernetičke sigurnosti** sa zainteresiranom javnošću. Nacionalni CERT sudjelovao je u procesu koji je koordinirao Ured Vijeća za nacionalnu sigurnost.

Otkriveno je da oglas ***(banner)*** na *web* portalu jednih dnevnih novina iz Hrvatske vodi do zaraženog *web* sjedišta (botneta). Da se zaraze korisnicima je bilo dovoljno posjetiti *web* portal uz korištenje neosvježene inačice Flasha ili Jave.

Hakeri su „upali“ u neklasificiranu mrežu **Bijele kuće**, priopćeno je u travnju. Pretpostavlja se da je riječ o grupi iz Rusije. Upad je prouzročio privremeni prestanak rada nekih usluga te izazvao debatu kod službenika.

U svibnju je otkrivena velika ranjivost upravljača za disketne *(floppy)* jedinice, nazvana **VENOM** (CVE-2015-3456). Napadač može iskoristiti navedenu ranjivost za izvršavanje proizvoljnog programskog koda, a posebno je rizičan kod virtualizacijskog softvera koji koriste usluge u oblaku (cloud servisi). U istom mjesecu objavljeno je kako je uočena ranjivost **Logjam**, koja je slična ranjivosti FREAK.

3. KVARTAL

U srpnju su zabilježeni **DDoS** napadi na infrastrukturu CARNeta i SRCA.

Hacking Team, talijanska kompanija koja se bavi prodajom softvera za prisluškivanje komunikacije, doživjela je ono što takva kompanija nikad ne bi smjela doživjeti – hakirana je. Ukupno 400 GB elektroničke pošte objavljeno je na Internetu, između ostalog i komunikacija nekoliko hrvatskih tvrtki i Sigurnosne obavještajne agencije.

4. KVARTAL

Vlada Republike Hrvatske donijela je, na sjednici održanoj 7. listopada 2015. godine, Odluku o donošenju **Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana** za provedbu Nacionalne strategije kibernetičke sigurnosti, koja je objavljena u Narodnim novinama broj **108/15.**

U izradi strategije sudjelovao je, kao član Povjerenstva za izradu Nacrta prijedloga nacionalne strategije kibernetičke sigurnosti koji je osnovala Vlada RH, i predstavnik Nacionalnog CERT-a, odnosno CARNeta.

Nacionalni CERT u studenom je sudjelovao u NATO-ovoj vježbi **Cyber Coalition 2015.**

U listopadu je Nacionalnom CERT-u prijavljen tzv. napad **reflection SSDP DDoS** na jedan poznati domaći web portal za kupnju.

U studenom je jednu domaću banku ucjenjivala kriminalna skupina izvođenjem DDoS napada.

Hakeri su oteli podatke s 15 milijuna korisničkih računa klijenata **T-Mobilea.** Upad se zapravo dogodio u mrežu kompanije **Experian** koja posluje s podatcima.

Direktor **CIA**-e John Brennan nasjeo je na socijalni inženjering i tako mu je njegov osobni pretinac e-pošte hakiran. Upadom se u američkom magazinu „Wired“ pohvalio jedan američki školarac. Pritom je koristio niz trikova kako bi zaobišao sigurnosne provjere.

7. Zaključak

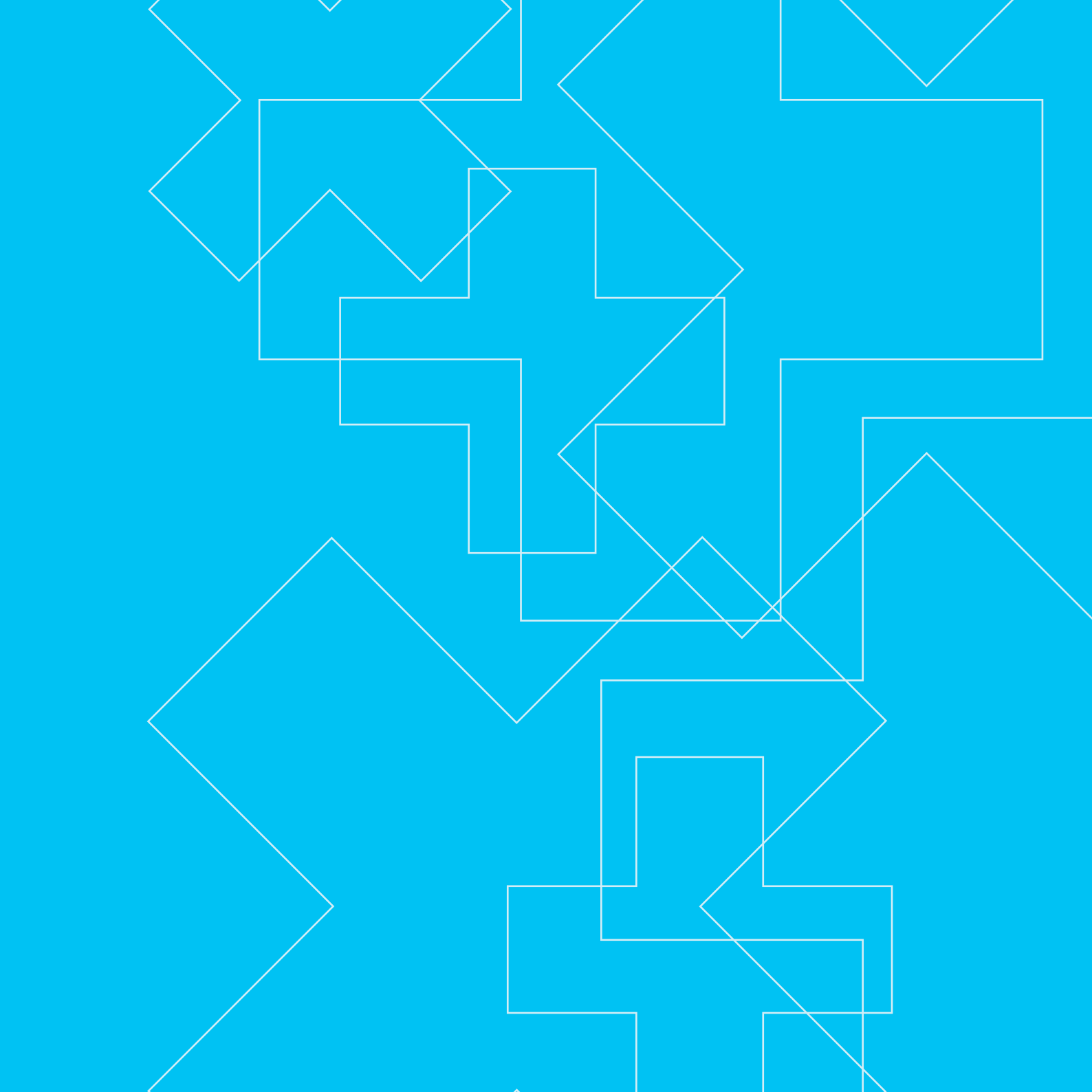
Tijekom 2015. godine Nacionalni CERT nadogradio je svoj sustav za ranu detekciju incidenata u RH (SRU@HR) u otkrivanju incidenata vezanih uz RH. Naglasak je bio na povećanju broja otkrivenih *phishing* URL-ova.

Nacionalni je CERT i u 2015. godini uspješno sudjelovao u NATO-ovoj vježbi CyberCoalition, u kojoj je RH sudjelovala u svojstvu igrača. Vještine djelatnika koji se bave digitalnom forenzikom i obradom incidenata morale su ponovo biti podignute na jednu još višu razinu. Donošenje Nacionalne strategije kibernetičke sigurnosti u 2015. godini još je jedan korak u povećanju svijesti o problemu informacijske, odnosno kibernetičke sigurnosti te početak koordiniranog rada na jačanju zaštite javne infrastrukture u Republici Hrvatskoj.

Sumarno, prema statistikama se može zaključiti da razina incidenata koji se odnose na broj registriranih botova konstantno pada, dok broj incidenata stagnira. Posjećenost portala antibot.hr u porastu je te je tijekom 2015. godine premašila brojku od 19.000 posjetitelja mjesečno, što je u korelaciji s manjim brojem zabilježenih zaraženih računala krajnjih korisnika (botova). Međutim, nove prijetnje kao što je *ransomware* pokazuju da manji broj određenih incidenata može pak prouzročiti veću štetu za fizičke osobe. Alati i metode obrane od takvih prijetnji od prosječnog korisnika zahtijevaju stjecanje sve većih znanja o mogućim prijetnjama s kojima je suočen. Što se tiče većih pravnih subjekata, značajno se bilježi porast distribuiranih napada uskraćivanjem usluge (DDoS), zajedno s ucjenom.

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.

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi, njime se može svatko koristiti i na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNeta, a sve sukladno zakonskim odredbama Republike Hrvatske.



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

—

Hrvatska akademska i istraživačka mreža - CARNet
Josipa Marohnića 5, Zagreb
tel: 01 6661 616
fax: 01 6661 615
http://www.carnet.hr

—

Nacionalni CERT

—

Odjel za Nacionalni CERT
ncert@cert.hr
http://www.cert.hr

—