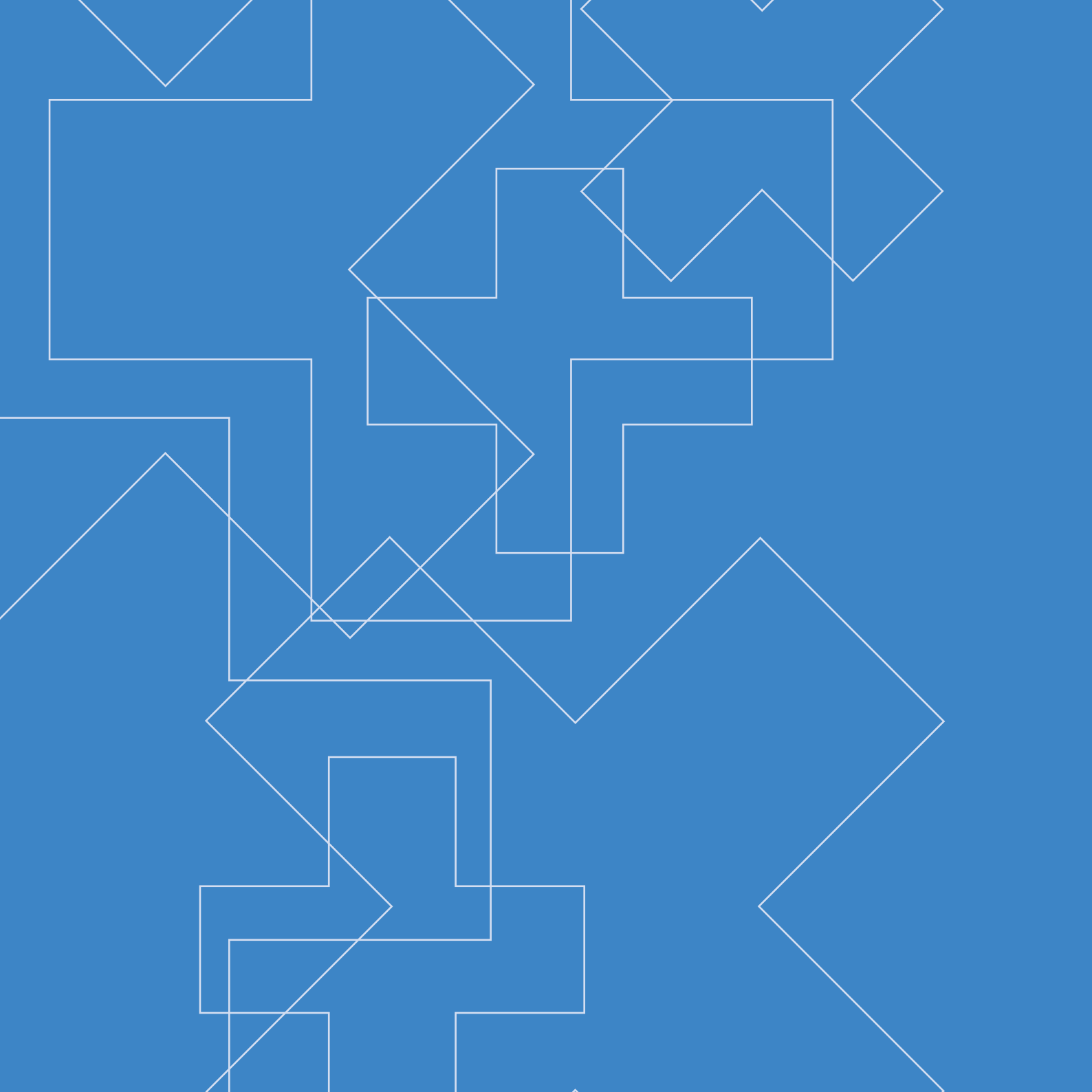
Nacionalni CERT

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 2016. godini



Sadržaj

1. Usluge Nacionalnog CERT-a

U 2016. godini Nacionalni CERT, odjel Hrvatske akademske i istraživačke mreže - CARNet, nastavio je svoju proaktivnu i reaktivnu ulogu kako bi se smanjio rizik od pojave sigurnosnih incidenta i umanjila šteta pri njihovom nastupanju. U tom je smislu Nacionalni CERT svakodnevno vršio proaktivne i reaktivne mjere čije su aktivnosti navedene u nastavku.

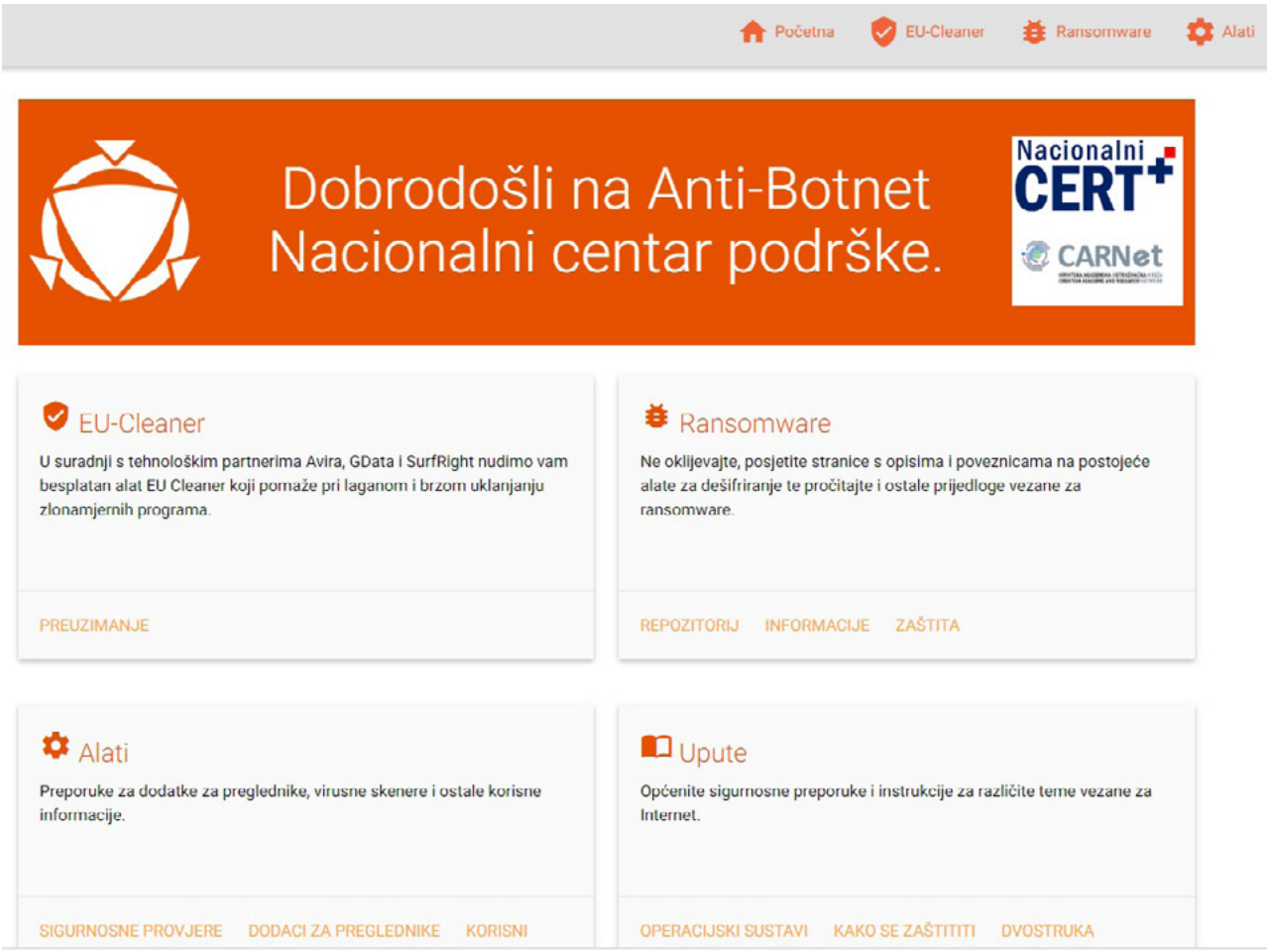
1.1. Proaktivne mjere

- Svakodnevno izdavanje sigurnosnih preporuka za najpopularnije operativne sustave
- Izdavanje i objavljivanje 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*
- Sudjelovanje u TV i radio emisijama
- Sudjelovanje na predavanjima u sklopu konferencija i radionica

Sljedeća tablica prikazuje broj objava za širu javnost ili izvršenih proaktivnih mjera u 2016. godini:

Tablica 1. Prikaz broja izvršenih proaktivnih mjera

Alati	14
Dokumenti	2
Novosti	99
Ukupno preporuka	2 493
Broj provjera ranjivosti	228

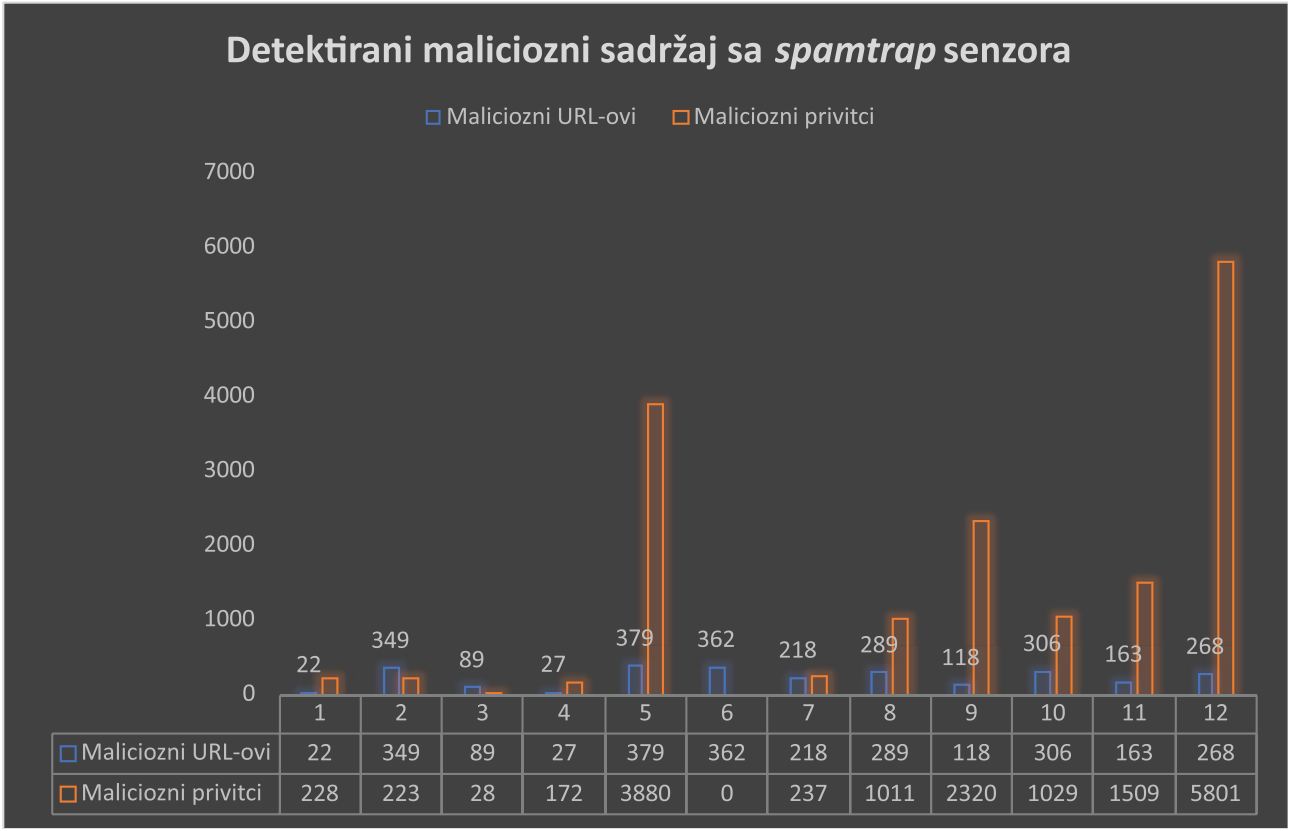


Slika 1. Novi izgled portala antibot.hr

Tijekom 2016. godine osvježen je izgled portala Antibot.hr. Krajnjim je korisnicima sada jednostavnije doći do alata za uklanjanje zlonamjernih programa s njihovih računala. Uvedena je posebna kategorija ***„Ransomware“*** u kojoj se mogu pronaći upute i savjeti kako se zaštititi te alati za dešifriranje podataka u slučaju zaraze nekom od vrsti *ransomwarea* iz repozitorija.
Također je uvedena nova potkategorija koja na jednom mjestu nudi vrlo koristan pregled dodataka koji nadopunjavaju *web* preglednike s ciljem povećanja sigurnosti računala te poveznice za preuzimanje istih. Dodane su i poveznice za različite *online* servise (antivirusne skenere, provjeru *phishing web* stranica itd.).

Od novih potkategorija valja navesti i potkategoriju **„Korisni alati“** koja donosi poveznice za preuzimanje različitih alata kao što su alati za izradu sigurnosnih kopija, spremanje lozinki i mnogi drugi. 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 neželjene elektroničke poruke *(spam)* sa zlonamjernim sadržajem također se mogu pronaći na portalu www.antibot.hr, pod kategorijom ***“Spam“***.

Grafikon 1. Detektirani maliciozni sadržaj sa *spamtrap* senzora



	1	2	3	4	5	6	7	8	9	10	11	12
Maliciozni URL-ovi	22	349	89	27	379	362	218	289	118	306	163	268
Maliciozni privitci	228	223	28	172	3880	0	237	1011	2320	1029	1509	5801

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 te njihova analiza
- Prikupljanje i analiza podataka o napadima dobivenih sa sustava ili senzora
- Abuse služba CARNet mreže

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 rezultati ove provjere šalju se odgovornim osobama na ustanovi u izvještaju koji sadrži listu pronađenih sigurnosnih propusta i upute za njihovo rješavanje. Ovu uslugu koristi 56 ustanova članica. Budući da je na CARNetovu mrežu spojeno više od 2400 ustanova iz sustava prosvjete, visoke naobrazbe, kulture te neka državna tijela, stručnjaci Nacionalnog CERT-a osim redovite provjere ranjivosti provode i masovne provjere ranjivosti CARNet mreže. Automatiziranu masovnu provjeru velikog broja ustanova u kratkom vremenu 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 na ustanovi. Tijekom 2016. 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.

Slika 2. Ekranski prikaz pregleda obavljenih provjera

1.4. Promjene u organizaciji CARNeta

Početkom 2016. Služba za sigurnost usluga, koja je do tada djelovala u sklopu Odjela za razvoj usluga (OZRU) Hrvatske akademske i istraživačke mreže – CARNet, počela je djelovati unutar odjela Nacionalnog CERT-a kao dio postojeće dvije službe Nacionalnog CERT-a (Službe za obradu incidenata i Službe za analitiku i forenziku).

Pripajanjem Službe za sigurnost usluga Nacionalnom CERT-u pridodaju se ciljevi navedene službe ciljevima Nacionalnog CERT-a. Ti se ciljevi, koji uključuju povećanje razine sigurnosti CARNetovih usluga, računalnih sustava i mreže, postižu sljedećim aktivnostima:

- prikupljanjem i analizom sigurnosnih događaja u CARNet mreži;
- provjerom sigurnosti aplikacija, komponenti i usluga CARNeta;
- provjerom ranjivosti mrežnih uređaja u jezgri CARNet mreže;
- uslugom izdavanja elektroničkih certifikata (TCS-om);
- provođenjem odredbi Programa sigurnosti;
- uvođenjem novih tehnologija sa sigurnosnog aspekta u informacijski sustav CARNeta.

Tijekom 2016. godine Nacionalni CERT u sklopu je tih aktivnosti:

- izdao 456 poslužiteljskih certifikata, od toga 16 *Extended Validation* (EV) certifikata te 23 klijentska certifikata;
- provodio penetracijska testiranja važnih CARNetovih usluga u sklopu implementacije programa sigurnosti u CARNetovim poslovnim procesima;
- provjeravao sigurnost usluga razvijenih u CARNetu ili za CARNet;
- certificirao aplikacije koje pristupaju sustavu “e-Matica”;
- sudjelovao u projektima GEANT 4-1 SA4/T1 i GEANT 4-2 SA2/T1;
- pružao potporu sigurnosnom dijelu projekta “e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)”;
- obavljao provjeru usklađenosti DNS poslovnog procesa s normom ISO 27001;
- uspostavio SIEM – sustav upravljanja informacijama i događajima.

2. Suradnja Nacionalnog CERT-a s institucijama izvan RH

Pored institucija **EU** i **NATO**, Nacionalni CERT surađuje s međunarodnim udruženjima CERT-ova **FIRST** *(Forum of Incident Response and Security Teams)* i **TI** *(Trusted Introducer)* čiji je akreditirani član.

2.1. Sudjelovanje u vježbi Cyber Europe 2016

Nacionalni CERT sudjelovao je u međunarodnoj vježbi Cyber Europe 2016 koju je organizirala Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA). Prva je faza započela u travnju 2016. godine, a druga se faza, u kojoj su stručnjaci za informacijsku sigurnost i ostala nadležna tijela rješavali scenarije računalno-sigurnosnih incidenata, održala u listopadu iste godine. Po prvi je puta u scenarij vježbe Cyber Europe bila uključena i simulacija medijske pokrivenosti, društvenih mreža i raznih tvrtki kako bi se što vjernije simulirala stvarna situacija *cyber* napada. Za uspješno rješavanje vježbe ključna je suradnja s drugim sudionicima, a moto Cyber Europe vježbi glasi "Zajedno smo jači", odnosno "Stronger together".

2.2. Sudjelovanje u vježbi Cyber Coalition 2016

Četvrtu godinu za redom Hrvatska akademska i istraživačka mreža - CARNet i njezin odjel za Nacionalni CERT aktivno su sudjelovali u najvećoj i najsloženijoj godišnjoj NATO vježbi zaštite računalnih sustava pod nazivom "Cyber Coalition 2016". U petodnevnoj vježbi koja je trajala od 28. studenog do 2. prosinca 2016. godine sudjelovalo je 27 NATO članica, brojne NATO partnerske zemlje te NATO i EU tijela. Kao i prethodnih godina, i ovog puta u provedbi vježbe sudjelovali su hrvatski partneri iz industrije i akademske zajednice. Kako bi se savladali složeni tehnički izazovi koji se pojavljuju pri rješavanju računalnih incidenata naglasak je stavljen na međusobnu komunikaciju i suradnju. Vježbom se rukovodilo iz NATO-vog centra izvrsnosti - *Co-operative Cyber Defence Centre of Excellence* (CCD COE) koji se nalazi u Tallinnu u Estoniji.

3. Suradnja i djelovanje Nacionalnog CERT-a unutar RH

3.1. Potpisan sporazum o poslovnoj suradnji sa ZSIS-om

U lipnju 2016. godine Nacionalni CERT potpisao je sporazum o poslovnoj suradnji sa Zavodom za sigurnost informacijskih sustava (ZSIS), središnjim državnim tijelom za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske. Kako je Nacionalni CERT zadužen za istovrsne poslove javnih informacijskih sustava, suradnja ovih dvaju tijela itekako je poželjna. Cilj sklapanja navedenog sporazuma je produbljivanje suradnje od zajedničkog interesa na području informacijske sigurnosti Republike Hrvatske, a time i podizanje cjelokupne razine nacionalne informacijske i kibernetičke sigurnosti.

3.2. Nacionalna strategija kibernetičke sigurnosti (NSKS)

U 2016. godini Nacionalni CERT radio je na provedbi mjera iz akcijskog plana za provedbu nacionalne strategije kibernetičke sigurnosti (NSKS). Kako je riječ o prvoj sveobuhvatnoj Strategiji u RH na 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 sudionika te učinkovitije koristilo postojeće resurse i bolje planiralo potrebu i ostvarenje novih resursa.

Mjere u kojima CARNet, odnosno odjel za Nacionalni CERT, aktivno sudjeluje kroz Nacionalnu strategiju kibernetičke sigurnosti podrazumijevaju:

- razvoj međusektorske suradnje nacionalnih regulatornih tijela i tijela odgovornih za područje informacijske sigurnosti i politike zaštite podataka te međusobnu koordinaciju i razmjenu iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira,
- analizu postojećeg stanja u provedbi mjera sigurnosti informacijskih sustava tijela javnog sektora,
- definiranje taksonomije (uključujući pojam značajnog incidenta), definiranje protokola za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima te uspostava platforme ili tehnologije za razmjenu podataka,
- prikupljanje podataka o incidentima od dionika,
- izvještavanje dionika unutar sektora o računalno-sigurnosnim incidentima,
- izdavanje upozorenja o sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje,
- izobrazbu zaposlenika na godišnjoj razini za potrebe ekspertize i specijalističke izobrazbe,
- izradu i objavljivanje preporuka o minimalnim sigurnosnim zahtjevima za davatelje i korisnike elektroničkih usluga,
- osmišljavanje i provođenje usklađene kampanje o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u RH o značaju kibernetičke sigurnosti,
- pravodobno obavještavanje javnosti putem medija o eventualnim nastancima računalno sigurnosnih incidenata koji se mogu lako multiplicirati i pogoditi veliki broj korisnika u kibernetičkom prostoru.

3.3. Djelovanje preko javnih medija i obraćanje javnosti

S ciljem podizanja svijesti o informacijskoj sigurnosti Nacionalni CERT djelovao je kroz sljedeće aktivnosti:

1. Izdao novu inačicu popularne brošure “Sigurnije na Internetu”
2. U travnju nastupio na HRT-u u emisiji “Potrošački kod” gdje se raspravljalo o problematici prijevara i uvreda na društvenim mrežama
3. U srpnju nastupio na HRT-u u emisiji “Potrošački kod” gdje se raspravljalo o problematici internetske kupovine i zaštite podataka kreditnih kartica
4. U rujnu nastupio na HRT-u u obrazovnoj emisiji za djecu i mlade “Školski sat” gdje se raspravljalo o zaštiti osobnih podataka na Internetu te o neprimjerenom ponašanju na Internetu
5. Održao niz predavanja na domaćim konferencijama i prezentacijama akademskoj zajednici, javnim i privatnim institucijama te široj javnosti, između ostalog “DIDS 2016”, “OWASP Croatia meetup”, “FSEC 2016”, “CUC 2016”, “Internet Security Days 2016”
6. U listopadu sudjelovao na Danu otvorenih vrata na Fakultetu prometnih znanosti kao dio programa “Danas studiram, sutra radim” gdje je prezentiran rad CARNeta (Nacionalnog CERT-a) s ciljem podizanja svijesti korisnika o sigurnosti informacijskih sustava u Republici Hrvatskoj, kao i o mogućnosti prijave sigurnosnih incidenata na području RH.

Isto tako mnogo informacija bilo je diseminirano putem *web* sjedišta Nacionalnog CERT-a, kojeg je u 2016. godini posjetilo 323 546 korisnika.

4. Suradnja i sudjelovanje na projektima

4.1. e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)

U sklopu projekta "e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)" uspostavlja se upravljanje sigurnosnim informacijama i događajima (eng. *Security Information and Event Manager* - SIEM) s ciljem sigurnosnog nadzora CARNetove mreže, CARNetovih kritičnih usluga te škola uključenih u projekt e-Škole. SIEM rješenje koje se implementira je *AlienVault* USM koje na temelju prikupljenih dnevničkih zapisa s različitih sustava u stvarnom vremenu omogućava detekciju, analizu, korelaciju i pohranjivanje relevantnih sigurnosnih događaja zabilježenih u računalno-mrežnoj infrastrukturi te u aplikacijama.

4.2. GEANT4

Nacionalni CERT u 2016. sudjelovao je u četvrtoj generaciji projekta GEANT - GEANT4. Projekt je sufinanciran sredstvima Europske unije, a za glavni cilj ima razvoj paneuropske akademske i istraživačke e-infrastrukture koja je prepoznata kao temelj za poticanje znanstvene izvrsnosti i interoperabilnosti. Nacionalni CERT sudjelovao je u aktivnostima vezanim uz uspostavu okvira za implementaciju sigurnosti u GEANTovoj infrastrukturi i uslugama, izradi okvira za sustavni razvoj, održavanje i unaprjeđivanje GEANTovih usluga (eng. *Software Management Framework*) te na poslovima sigurnosnih testiranja GEANTovih usluga. Projektne aktivnosti provodile su se u sklopu dvije servisne aktivnosti (eng. *Service Activity*) - SA4 i SA2. Uspostavljeni su mehanizmi kvalitativne i sigurnosne provjere novih usluga tijekom tranzicije usluga iz razvojnog okruženja u produkciju te periodičkih provjera produkcijskih usluga. U skladu s uspostavljenim okvirom obavljene su kvalitativne i sigurnosne provjere pet novih GEANTovih usluga koje su tijekom godine uspješno uključene u produkcijsko okruženje.

4.3. CEKOM

Nacionalni CERT 2016. godine predao je prijavu za EU projekt CEKOM (Centar kompetencija) u kojem će sudjelovati kao partner. Centar kompetencija - CEKOM - ima za cilj povećati konkurentnost hrvatskog gospodarstva poticanjem inovativnosti poslovnog sektora i suradnje sa znanstveno-istraživačkim institucijama u području kibernetičke sigurnosti upravljačkih sustava (uključujući i industrijske upravljačke sustave – eng. *Industrial Control System,* ICS). Nositelj projekta je tvrtka CS Computer Systems d.o.o., a CARNet, odnosno odjel za Nacionalni CERT uz Končar, FER i tvrtku Hrvatski operator prijenosnog sustava d.o.o. sudjeluje kao partner na projektu. U prvoj godini projekta predviđeno je da Nacionalni CERT opremi prijenosni laboratorij potreban za obradu incidenata vezanih uz upravljačke sustave, odnosno da nadogradi svoj postojeći labo-

ratorij sa specifičnim softverskim i hardverskim alatima potrebnim za forenziku zlonamjernog programa vezanog uz protokole i okruženje industrijskih sustava (za sada Nacionalni CERT posjeduje laboratorij u kojem je moguće analizirati zlonamjerni program „klasičnog“ tipa). Predviđeno trajanje projekta je tri godine, a u drugoj i trećoj godini predviđeno je da CARNetov odjel za Nacionalni CERT radi s alatima za penetracijsko testiranje i utvrđuje ranjivosti u laboratorijskim uvjetima te utvrđuje metode skeniranja i procjene ranjivosti ICS komponenti. U sklopu projekta testirat će se efikasnost alata pribavljenih za pokretni forenzički laboratorij Nacionalnog CERT-a te će se nadograditi mreže senzora *(honeypot)* za detekciju aktivnosti zlonamjernog sadržaja koji je prijetnja ICS sustavima.

4.4. CEF

U sklopu Connecting Europe Facility (CEF) Nacionalni CERT prijavio je EU projekt pod nazivom *„Increase of National CERT Capacities and Enhancement of Cooperation on National and European level – GrowCERT“*. U okviru projekta CEF kao jedna od glavnih aktivnosti ističe se podizanje svijesti o kibernetičkim prijetnjama te adekvatnim odgovorima na iste kroz radionice i razne marketinške aktivnosti. Na razinu kibernetičke sigurnosti u nacionalnom okviru djelovat će se osvještavanjem šire populacije, akademske zajednice te privatnog sektora o izvorima prijetnji, značaju socijalnog inženjeringa te o načinima na koji se mogu proaktivno zaštititi. Značajna je aktivnost i razvitak platforme za razmjenu statističkih podataka te platforme za razmjenu informacija vezanih uz sigurnosne incidente na razini Republike Hrvatske i Europske unije. Time bi se osigurala visoka razina usklađenosti sustava za razmjenu informacija vezanih uz sigurnosne prijetnje te pripadajućih statističkih pokazatelja, definiranih uvjetima što ih postavlja Nacionalna strategija kibernetičke sigurnosti. Isto tako projektom će se razviti nekoliko novih javnih usluga te internih servisa koji doprinose podizanju razine kibernetičke sigurnosti i ostvarivanju ciljeva iz Nacionalne strategije kibernetičke sigurnosti. Nabavom hardvera, softvera, licenci te razvitkom usluga i platformi povećat će se sposobnost CARNetovog Nacionalnog CERT-a da osigura neprekidan rad općih usluga. Ova bi aktivnost neposredno omogućila višu razinu sigurnosti kritične nacionalne informacijske infrastrukture kao što su vršna nacionalna .hr domena, **AAI@EDU.hr** identifikacija i autentikacija na koju se oslanja niz nacionalnih usluga i servisa vezanih uz obrazovanje (kao što su upisi u škole i na fakultete ili e-dnevnik) te CARNet infrastrukture za rukovanje povjerljivim informacijama na nacionalnoj razini. Projektom je također predviđena i aktivnost osposobljavanja i usavršavanja djelatnika Nacionalnog CERT-a na polju kibernetičke sigurnosti.

5. Stanje računalnih incidenata i statistike

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

Nacionalni CERT u 2016. godini zaprimio je i obradio ukupno 641 prijavu koja se može klasificirati kao računalni incident u nadležnosti Nacionalnog CERT-a.

Vodeći tipovi incidenata su ***web defacement*** (kompromitirano *web* sjedište s izmijenjenom početnom *web* stranicom), ***phishing* URL** i ***malware* URL**. S obzirom na to da navedena tri tipa incidenata, uz ***spam* URL**, zapravo predstavljaju kompromitirana web sjedišta, ako se gleda sumarno, broj otkrivenih kompromitiranih *web* sjedišta u odnosu na prošlu godinu pao je za 16%. Najznačajnija promjena u odnosu na prethodnu godinu rast je broja web defacementa, što je rezultat vanjskih (automatiziranih) izvora koji su to češće prijavljivali nego prošle godine.

Napadi uskraćivanjem usluge i dalje su prisutni. Napadači često traže plaćanje otkupnine kako bi obustavili svoje DDoS napade.

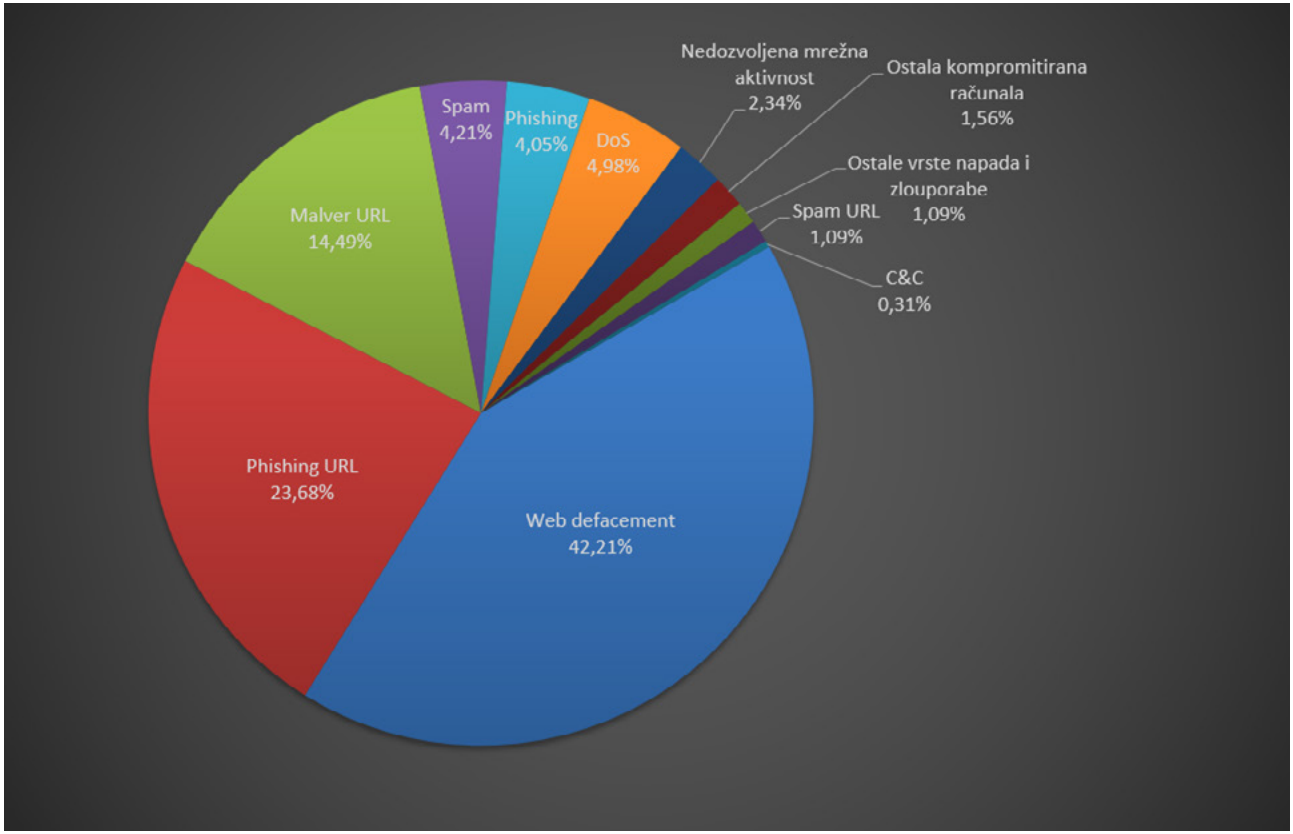
Tablica 2. Prikaz incidenata po tipu u 2016. godini:

TIP INCIDENTA	BROJ	
Web defacement	271	▲
Phishing URL	152	▼
Malware URL	93	▼
DoS	32	▼
Spam	27	▼
Phishing	26	▼
Nedozvoljena mrežna aktivnost	15	▲
Ostala kompromitirana računala	10	▲
Ostale vrste napada i zlouporabe	7	▼
Spam URL	7	▼
C&C	2	▼
UKUPNO	**642**	


Phishing
Spyware
Financial
Remote Admin
Trojans Horses
Identity Theft
Password
Crime
Virus Computer
Spam
Botnet
Rootkits
Social Network
E-Commerce
Update
Worms
Internet Scam
are
Username
Skimming

5.2. Raspodjela incidenata po tipu

Sljedeća tablica prikazuje omjere incidenata po tipu u 2016. godini, koji su zabilježeni u sustavu za obradu incidenata:

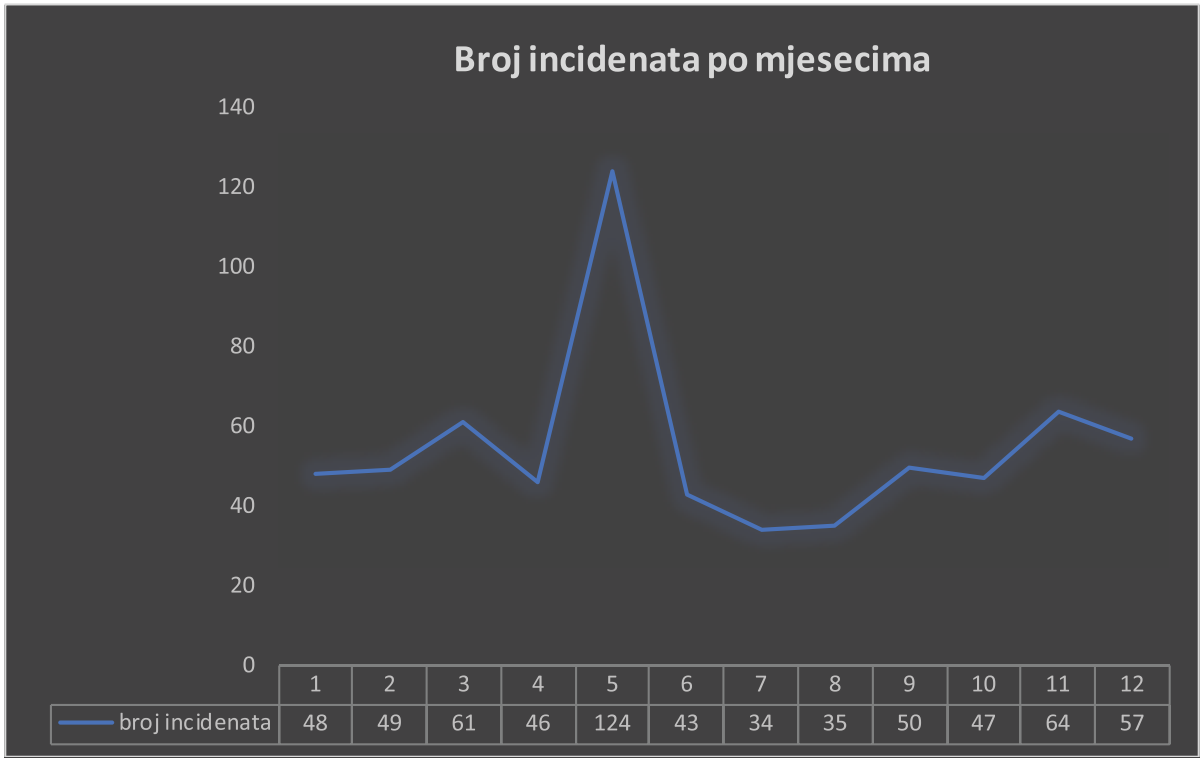


Grafikon 2. Raspodjela incidenata po tipu:

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 2016. godini

Sljedeća tablica prikazuje broj obrađenih incidenata na poslužiteljima na mjesečnoj bazi, koji su zabilježeni u sustavu za obradu incidenata:



Grafikon 3. Broj incidenata po mjesecima

5.4. Registrirani botovi u RH

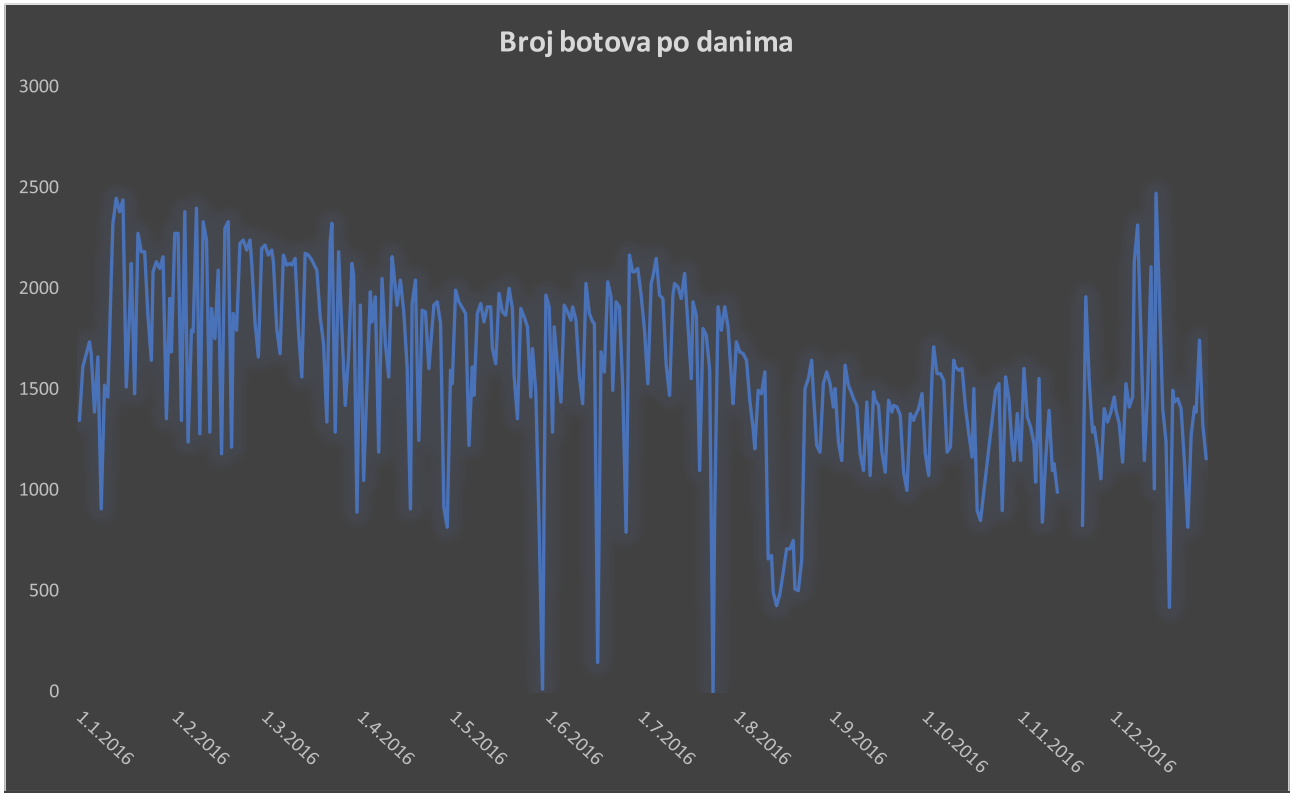
Nacionalni CERT primao je i statistički obrađivao podatke o *botovima* na računalima krajnjih korisnika. Podaci su prosljeđivani pripadajućim davateljima internetskih usluga i pružateljima usluga udomljavanja Internet stranica *(hosting provider)*. Iz grafikona koji prikazuje godišnji trend broja *botova* 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:

Conficker	**283 955**
Sality	40 872
ZeroAccess	27 757
Ponmocup	23 334
Nivdort	22 038
Downadup	19 370
Dorkbot	17 458
Palevo	16 886
Tinba	16 049
Mirai	12 102

Tablica 3. Suma zabilježenih *botova* prema tipu (vrsti zlonamjernog programa) tijekom 2016. godine:



Grafikon 4. Broj zabilježenih *botova* po danima

Srednja vrijednost broja *botova* po danu za 2016. godinu iznosila je 1.593,5.

6. Značajniji incidenti, otkrivene ranjivosti i događaji u 2016. godini

1. KVARTAL

U siječnju 2016. godine otkriven je komandni i kontrolni (command and control - C&C) poslužitelj Dridex *botneta* u mreži jednog hrvatskog ISP-a. Također, vanjski je partner prijavio kako je velik broj računala u Republici Hrvatskoj zaražen Qakbot zlonamjernim kodom čija je primarna namjena krađa povjerljivih podataka.

U istom mjesecu zabilježena je *phishing* kampanja na hrvatske korisnike **Gmaila**. Napadači su slali *phishing* poruke elektroničke pošte (u ime Google tima) koje su lažno obavještavale korisnike da je došlo do nadogradnje na poslužiteljima te se tražilo unošenje Gmail korisničkih podataka unutar *phishing* stranice.

Američka tvrtka iSight objavila je kako je ruska hakerska grupa **„Sandworm“** odgovorna za prekid struje u Ukrajini u prosincu 2015. Analizom je utvrđeno da su uz pomoć zlonamjernog softvera „Black Energy 3“ i „Kill Disk“, 23. prosinca 2015. prekinuli dovod električne energije za 80,000 korisnika na oko šest sati.

U veljači se dogodio DNS reflektirajući DDoS napad na poslužitelje u CARNetovoj mreži, *web* stranice Vlade RH (www.gov.hr) i na *web* sjedište www.predsjednica.hr.

1. ožujka objavljeno je kako je otkrivena ranjivost HTTPS poslužitelja, nazvana **DROWN**. Ranjivost se očituje u dva slučaja: ako poslužitelj uz TLS podržava i SSLv2 ili ako se isti javni ključ koristi na drugom poslužitelju koji podržava SSLv2 (tada je TLS poslužitelj ranjiv jer koristi isti javni ključ). Naime, poslužitelj koji podržava SSLv2 izlaže informacije koje se mogu iskoristiti kako bi se prisluškivala komunikacija TLS sesija. Isti dan je objavljeno kako je čak 33% HTTPS poslužitelja ranjivo na DROWN.

U ožujku se dogodio phishing napad u kojem je korištena *phishing* stranica jedne poznate hrvatske banke. Isti mjesec je otkrivena i nova *phishing* kampanja - elektroničkom poštom širile su se *phishing* poruke koje su u privitku sadržavale .zip datoteku unutar koje je zlonamjerna JavaScript datoteka. Radilo se o *crypto-ransomware* tipu zlonamjernog koda naziva **“Locky”** koji se u računalo korisnika ubacuje u slučaju pokretanja JavaScript datoteke koja s udaljenog *web* sjedišta dohvaća zlonamjerni kod i ubacuje ga na računalo. *Malware* potom šifrira podatke na računalu, nakon čega napadači ucjenjuju žrtvu da otkupi ključ kojim je moguće dešifrirati šifrirane podatke.

2. KVARTAL

U travnju je **WhatsApp**, poznata mobilna aplikacija za komunikaciju, implementirala „End-to-End“ šifriranje svih tekstualnih poruka, priloženih datoteka, poziva i grupnog dopisivanja.

Istraživači za računalnu sigurnost unaprijedili su **BREACH** *(Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)* napad star tri godine. BREACH napad iskorištava gzip/DEFLATE algoritam za sažimanje HTTP(S) prometa kojeg koriste mnogi *web* poslužitelji kako bi komunikaciju učinili efikasnijom. Mehanizam sažimanja otkriva informacije o šifriranim vezama. Starije inačice BREACH napada bile su efikasne za veze koje su koristile RC4 simetrični kriptografski algoritam toka, dok je novija inačica efikasna i kod veza koje koriste danas zastupljeniji TLS block ciphers kao što je AES.

U svibnju je nekoliko tvrtki i banaka unutar Republike Hrvatske ucjenjivano DDoS napadima. Neki DDoS napadi su se stvarno i dogodili.

8. lipnja 2016. na ilegalnom internetskom tržištu na prodaju je ponuđeno oko 32 milijuna korisničkih imena i približan broj lozinki društvene mreže **Twitter** za 10 Bitcoina. Korisnički podaci prikupljeni su pomoću zlonamjernog programa koji je bez znanja žrtve spremao korisnička imena i lozinke u *web* preglednicima “Google Chrome” i “Firefox” te ih slao napadaču. Kompromitirani računi većinom dolaze iz ruskog govornog područja.

14. lipnja 2016. godine NATO je *cyber* prostor proglasio zonom ratovanja. Razlog je tome što se „opasni napadi“ mogu izvršiti u kibernetičkom prostoru isto kao i u zraku, moru i zemlji, te time utjecati na suverenitet pojedine članice NATO saveza.

3. KVARTAL

U srpnju je parlament Europske Unije usvojio **NIS** direktivu *(The Directive on Security of Network and Information Systems)*. Zemlje članice imaju (od 6. srpnja) 21 mjesec da direktivnu ugrade u svoje zakonodavstvo i još 6 mjeseci kako bi identificirale operatore ključnih usluga. Direktiva definira potrebu za uređenjem mreže CSIRT-ova (država članica) kako bi se promovirala brza i učinkovita operativna suradnja te dijeljenje informacija u slučaju računalno-sigurnosnih incidenata.

Tijekom kolovoza otkriven je skup četiri ranjivosti nazvan **“QuadRooter”** koji pogađa čak 900 milijuna Android uređaja koji imaju ranjivi čip proizvođača Qualcomm. Ranjivosti su omogućavale napadačima preuzimanje kontrole nad mobilnim uređajem ako uspiju žrtvu natjerati da instalira zlonamjernu mobilnu aplikaciju (bez posebnih privilegija). Neki od poznatijih pogođenih uređaja su: Samsung Galaxy S7 i S7 Edge, Sony Xperia Z Ultra i OnePlus One.

U rujnu je predstavljena inicijativa **„NoMoreRansom“** od strane Europola, nizozemske policije i tvrtki Kaspersky Lab i Intel Security. Cilj inicijative je pomoći žrtvama *ransomwarea* u vraćanju datoteka bez da plate otkupninu, kao i edukacija krajnjih korisnika kako bi se spriječila zaraza opasnim kripto virusima.

Yahoo! je potvrdio kompromitaciju 500 milijuna korisničkih imena, adresa elektroničke pošte, telefonskih brojeva, datuma rođenja i šifriranih sigurnosnih pitanja i odgovora. Kompromitacija se dogodila 2014. godine, a početkom kolovoza 2016. godine haker pod nazivom *Peace*, na prodaju je ponudio 200 milijuna Yahoo! korisničkih računa.

Najveći zabilježeni **DDoS** napad intenziteta preko 1 Tbps izvršen je na poslužitelje poznatog francuskog pružatelja usluge udomljavanja internet stranica, **OVH**. Ovu vijest na Twitteru je objavio osnivač i CTO tvrtke, Octave Klaba. Napad je izvršen iskorištavanjem preko 152 000 *Internet of Things* (IoT) uređaja, uglavnom CCTV nadzornih kamera i video rekordera. Izvršena su dva uzastopna napada čiji je ukupni intenzitet dosegao više od 1 Tbps. Jedan od njih bio je intenziteta 799 Gbps što ga čini najvećim DDoS napadom ikad zabilježenim. Procjenjuje se da je svaki uređaj generirao intenzitet od 1 do 30 Mbps.

4. KVARTAL

U sklopu europskog mjeseca sigurnijeg interneta obnovljen je sadržaj *web* sjedišta **botfree.eu**. Inicijalno je napravljen kao dio europskog Cyber Security projekta ACDC (*Advanced Cyber Defence Centre*), projekta koji je bio aktualan od 2013. do 2015. godine s ciljem unaprjeđenja borbe protiv *botneta*. Fokus servisa ‘botfree.eu’ je pružanje pomoći *malware* i *botnet* žrtvama, ali i davanje savjeta o zaštiti protiv zlonamjernih kodova i ostalih *cyber* prijetnji poput *phishing* mail poruka i *ransomware* zlonamjernog softvera.

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

Kompromitirani su poslužitelji kompanije **FriendFinder Networks** koja se nalazi iza 49 000 *web* sjedišta za odrasle. Kompromitirano je 412 214 295 korisničkih računa, od toga 15 milijuna obrisanih korisničkih računa koji su još uvijek bili pohranjeni u bazu podataka. Prema tome, riječ je o najvećoj kompromitaciji u 2016. godini. Otkriveni su korisnički podaci za posljednjih 20 godina s ukupno šest domena. Kompromitirani osobni podaci uključivali su korisnička imena, adrese elektroničke pošte, datume prijava u sustav, jezika, lozinke i slično.

U prosincu je u koordiniranoj akciji srušena organizirana kriminalna mreža (*botnet* **Avalanche**). Akcija je trajala četiri godine, a uključivala je rad tužitelja i istražitelja iz trideset zemalja, FBI i Europol. Žrtve napada koje su koristile navedenu infrastrukturu nalaze se u čak 180 zemalja, a 221 poslužitelj je ugašen. Operacija je uključivala preuzimanje kontrole ili blokiranje rekordnih 800 tisuća domena. Procijenjeno je da je Avalanche uzrokovao gubitak stotina milijuna eura diljem svijeta.

7. Zaključak

Tijekom 2016. godine Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave sigurnosnih incidenta i umanjenja štete u slučaju njihovog nastanka. Nastavio je razvijati suradnju s institucijama izvan RH kao što su drugi CERT timovi i institucijama EU-a i NATO-a te s ostalim tijelima unutar RH, a sve u svrhu razvitka zajedničkih interesa u području informacijske sigurnosti.

Nacionalni CERT i u 2016. godini uspješno je sudjelovao u NATO CyberCoalition vježbi, gdje je RH sudjelovala u svojstvu igrača. Vještine djelatnika koji se bave digitalnom forenzikom i obradom incidenata morale su ponovno biti podignute na jedan još viši nivo. U međunarodnoj vježbi Cyber Europe 2016 stručnjaci za informacijsku sigurnost, i ostala nadležna tijela, rješavali su simulirane scenarije računalno sigurnosnih incidenata i time pokazali sposobnost uspješne suradnje s drugim sudionicima.

Sumarno, prema statistikama, može se zaključiti kako razina incidenata koji se odnose na broj registriranih *botova* konstantno pada, a u padu je i broj drugih vrsta incidenata. Posjećenost portala antibot.hr je tijekom 2016. godine dosegla brojku od 24 891 posjetitelja, što je u korelaciji s manjim brojem zabilježenih zaraženih računala krajnjih korisnika *(botova)*. Osvježenjem portala antibot.hr dodana je kategorija *"Ransomware"*, potkategorija s alatima za preglednike, nove poveznice za različite online servise te potkategorija "Korisni alati". Pada broj kompromitiranih *web* sjedišta u odnosu na prošlu godinu, i to za 16%. Najznačajnija promjena u odnosu na prethodnu godinu je rast broja *web* defacementa, što je rezultat veće suradnje s vanjskim izvorima, tj. veći je broj prijava iz vanjskih izvora u odnosu na prošlu godinu. Što se tiče većih pravnih subjekata, napadi uskraćivanjem usluge i dalje su prisutni, a često se za obustavljanje DDoS napada traži plaćanje otkupnine.

Zaključno, Nacionalni CERT u 2016. godini ostvario je značajne pomake na području nacionalne i međunarodne suradnje, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

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.

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

—