GODIŠNJI IZVJEŠTAJ NACIONALNOG CERT-A ZA 2020. GODINU

CERT.hr
surfaj sigurnije

CARNET
znanje povezuje

SADRŽAJ

1. O CARNET-OVOM NACIONALNOM CERT-U

Nacionalni CERT (**CERT.hr**) je odjel Hrvatske akademske i istraživačke mreže – **CARNET** osnovan 30. listopada 2007. godine prema **Zakonu o informacijskoj sigurnosti RH** (5. poglavlje) kao nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj.

CERT.hr se bavi incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj (odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru), osim tijela državne uprave za koje je nadležan Zavod za sigurnost informacijskih sustava (**ZSIS**). Osim toga, Nacionalni CERT se bavi incidentima sa znatnim učinkom prema **Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga** za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državna tijela i davatelje digitalnih usluga.

Usluge CERT.hr-a dostupne su široj javnosti. Djelovanje CERT.hr-a dijelom je financirano sredstvima koja osigurava Ministarstvo znanosti i obrazovanja, a drugi dio Europska unija kroz razne EU projekte.

Tijekom 2020. godine Nacionalni CERT provodio je svoje proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenata i smanjenja šteta pri njihovom nastanku.

1.1. PROAKTIVNE MJERE

Proaktivnim mjerama CARNET-ov Nacionalni CERT djeluje prije incidenata i drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprečavanja ili ublažavanja mogućih šteta.

Neke od proaktivnih mjera koje provodi Nacionalni CERT su:

- **sigurnosne preporuke** - svakodnevno izdavanje sigurnosnih preporuka za najpopularnije operativne sustave;
- **diseminacija informacija iz područja računalne sigurnosti** - izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti;
- **praćenje računalno-sigurnosnih tehnologija** - i davanje i objavljivanje tehničkih informacija o sigurnosnim alatima;
- **praćenje i objavljivanje novosti u vezi kibernetičke sigurnosti**;
- **provjera ranjivosti za ustanove članice CARNET mreže**;
- **izdavanje elektroničkih certifikata za ustanove članice CARNET-a**;
- **sigurnosna testiranja CARNET-ovih usluga i servisa te aplikacija koje pristupaju sustavu eMatica**;
- informiranje javnosti putem portala **www.antibot.hr** s ciljem pružanja pristupačnih i jednostavnih savjeta krajnjim korisnicima;
- **unapređenje svijesti o značaju računalne sigurnosti** - organiziranje i provedba aktivnosti podizanja svijesti o kibernetičkoj sigurnosti;
- **edukacija i obuka o računalnoj sigurnosti**;
- **održavanje predavanja i webinara o sigurnosti na internetu**;
- sudjelovanje u televizijskim i radijskim emisijama;
- sudjelovanje na predavanjima u sklopu konferencija i radionica.

ALATI	3
DOKUMENTI	4
NOVOSTI	107
UKUPNO PREPORUKA	3682
BROJ PROVJERA RANJIVOSTI	215
BROJ IZDANIH ELEKTRONIČKIH CERTIFIKATA	1555

Broj izvršenih proaktivnih mjera u 2020. godini

1.2. REAKTIVNE MJERE

Reaktivnim mjerama odgovara se na incidente u Republici Hrvatskoj te na druge događaje koji mogu ugroziti kibernetičku sigurnost javnih informacijskih sustava u Republici Hrvatskoj. Neke od reaktivnih mjera koje provodi Nacionalni CERT su:

- **postupanje s računalno-sigurnosnim incidentima** - obrada incidenata (svi korisnici u Hrvatskoj, uključujući korisnike CARNET-a);
- **koordinacija rješavanja značajnijih incidenata** - obrada incidenata sa znatnim učinkom sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga;
- **sigurnosna upozorenja**;
- prikupljanje podataka o kompromitiranim računalima i njihovim aktivnostima s izvora na internetu te njihova analiza;
- prikupljanje i analiza podataka o napadima dobivenih iz sustava ili senzora;
- Abuse služba CARNET mreže.

2. STANJE RAČUNALNIH INCIDENATA I STATISTIKE

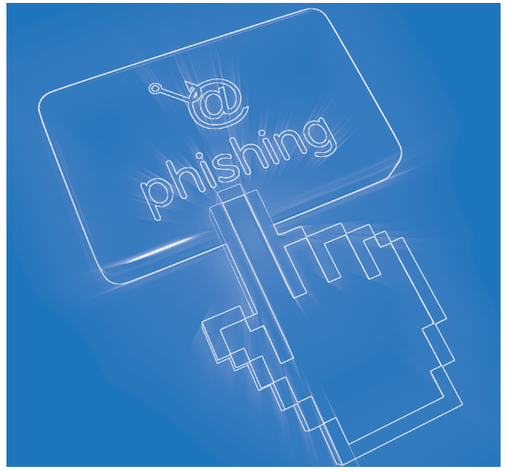
2.1. STATISTIKA O OBRAĐENIM INCIDENTIMA

Nacionalni CERT je tijekom 2020. godine zaprimio i obradio ukupno 1710 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tipovi incidenata su ***phishing URL, phishing i pogađanje zaporki***.

Najznačajnija promjena u odnosu na prošlu godinu je općenito velik broj prijavljenih incidenata. Korištenjem OSINT metoda (eng. *Open Source Inteligence*) za otkrivanje računalno-sigurnosnih incidenata na web sjedištima pod nadležnošću Nacionalnog CERT-a, ali i stalnim aktivnostima podizanja svijesti javnosti o ugrozama koje dolaze s interneta, u odnosu na 2019. godinu Nacionalni CERT je zaprimio i obradio 66% incidenata više.

Velika promjena odnosi se i na rast broja incidenta pogađanje zaporki koji je u 2020. godini došao na 3. mjesto, po prvi puta u top 3 incidenta. Razlog tome je povećanje suradnje s domaćim pružateljima usluge udomljavanja Internet stranica (*hosting providerima*) i stranim CERT timovima koji nam prijavljuju takve incidente.

S obzirom na to da ***web defacement, phishing URL, malware URL i spam URL*** zapravo predstavljaju kompromitirana web sjedišta, ako se gleda sumarno, broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu povećao se za visokih 58% što je također rezultat korištenja OSINT metoda za otkrivanje računalno-sigurnosnih incidenata.



TIP INCIDENTA	BROJ	TREND
PHISHING URL	446	▲
PHISHING	277	▲
POGAĐANJE ZAPORKI	205	▲
WEB DEFACEMENT	188	▲
MALWARE URL	132	▲
HOAX	116	▲
SUSTAV ZARAŽEN ZLONAMJERNIM KODOM	83	▲
POKUŠAJ ISKORIŠTAVANJA RANJIVOSTI	59	▲
SCAM	45	▲
SPAM	35	▼
KORISNIČKI RAČUN	29	▲
DOS - VOLUMETRIČKI NAPAD	27	▲
SPAM URL	21	▲
PRIJEVARE	13	▼
C&C	12	▲
SKENIRANJE	12	▲
ISPAD USLUGE (ENG. OUTAGE)	5	–
OSTALO	2	▼
DOSTUPNOST	1	–
DOS - NAPAD NA APLIKACIJSKOM SLOJU	1	–
ZLONAMJERNO RUDARENJE KRIPTOVALUTE (ENG. CRYPTOJACKING)	1	–
UKUPNO	**1710**	▲

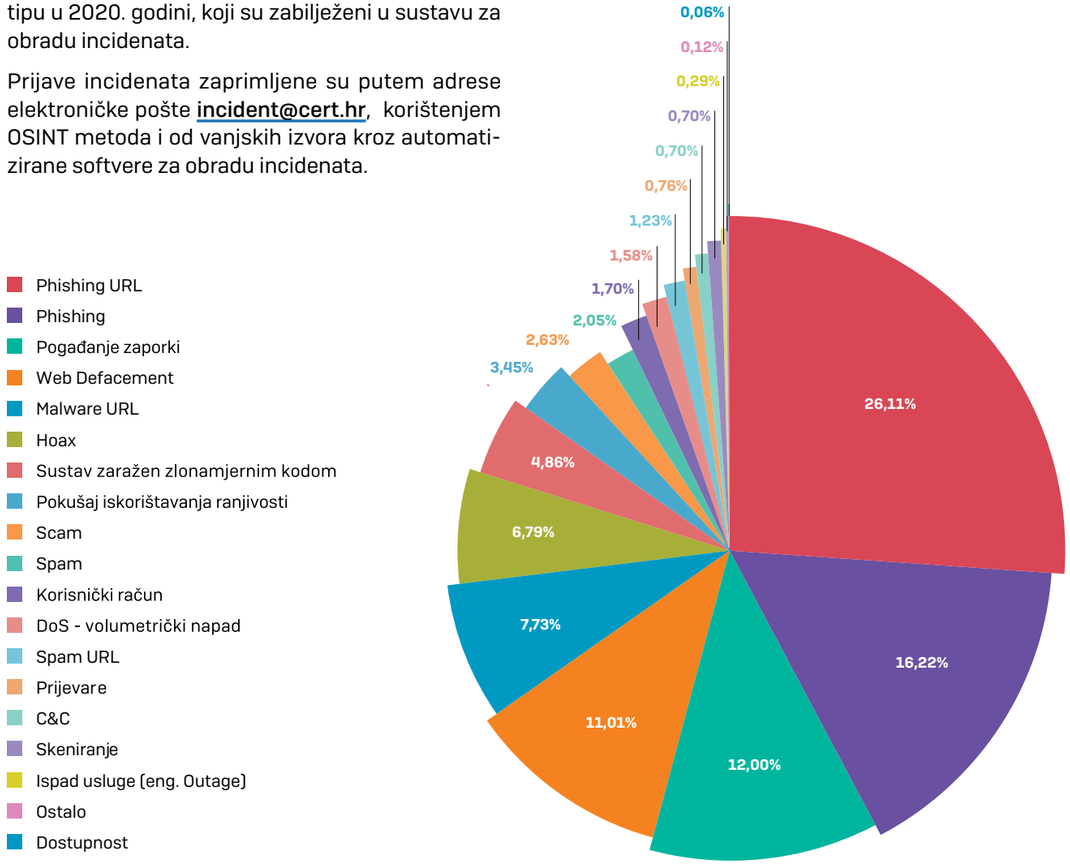
Prikaz incidenata po tipu u 2020. godini

Prema trendu kretanja vrsta incidenata vidimo da su gotovo sve kategorije incidenata u porastu, što je rezultat velikog broja prijava općenito (zbog povećanja suradnje i puno aktivnosti vezanih uz vidljivost samog Nacionalnog CERT-a). Pad broja kategorije "Ostalo" je rezultat uspostave Nacionalne taksonomije računalno-sigurnosnih incidenata koja dobro opisuje kategorije i podkategorije u koje se pojedina prijava može klasificirati. Taksonomija je "živi" dokument i ovisno o opisu pojedinog incidenta s vremenom će sve manje incidenata biti u kategoriji "Ostalo".

2.2. RASPODJELA INCIDENATA PO TIPU

Sljedeći grafikoni prikazuju omjere incidenata po tipu u 2020. godini, koji su zabilježeni u sustavu za obradu incidenata.

Prijave incidenata zaprimljene su putem adrese elektroničke pošte **incident@cert.hr**, korištenjem OSINT metoda i od vanjskih izvora kroz automatizirane softvere za obradu incidenata.



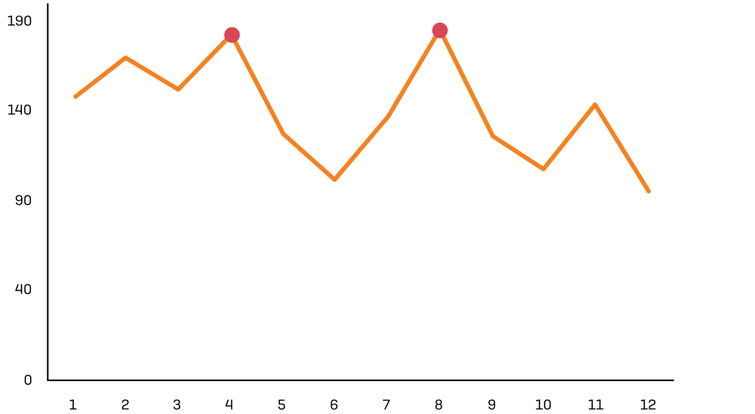
Raspodjela incidenata po tipu u 2020. godini

2.3. TRENDOVI POJAVA INCIDENATA NA POSLUŽITELJIMA U 2020. GODINI

Sljedeći grafikon prikazuje broj obrađenih incidenata na poslužiteljima na mjesečnoj osnovi, koji su zabilježeni u sustavu za obradu incidenata.

Na grafičkom prikazu vidljiva su dva skoka u broju incidenata: u travnju i kolovozu. Prvi skok zabilježen je radi povećanog broja incidenata zbog velikog broja *phishing* kampanja vezanih uz COVID-19. U tom razdoblju je velik broj država bio u *„lockdownu"* i poslovanje se kod velikog broja korisnika prebacilo u model rada od kuće, što je napadačima dalo dodatnu motivaciju za kreiranjem phishing kampanja. Kod većine ***phishing* poruka** pošiljatelji su se predstavljali kao Svjetska zdravstvena organizacija (eng. *World Health Organization – WHO*) ili ministarstvo zdravstva pojedine države. **CSIRT Network** je bio u *„Alert"* stanju suradnje te je redovno održavao sastanke, sastavljao izvještaje i upozoravao na računalno-sigurnosne incidente pojedine države članice Europske unije.

Razlog povećanja broja incidenata u kolovozu je korištenje OSINT metoda kojima je otkriven veći broj zlonamjernih stranica i kompromitiranih web sjedišta s izmijenjenim izgledom i sadržajem web stranica. Nacionalni CERT je poslao prijave svim nadležnim pružateljima usluga udomljavanja Internet stranica.



1	2	3	4	5	6	7	8	9	10	11	12	MJESEC
151	171	154	183	131	106	139	186	130	122	146	101	BROJ INCIDENATA

Broj incidenata na poslužiteljima u 2020. godini po mjesecima

2.4. REGISTRIRANI BOTOVI U REPUBLICI HRVATSKOJ

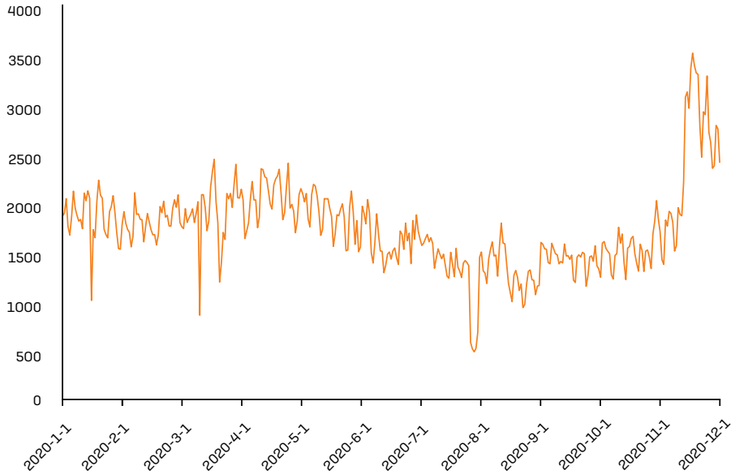
Nacionalni CERT primao je i statistički obrađivao podatke o *botovima* na računalima krajnjih korisnika. Podaci su prosljeđivani nadležnim davateljima internetskih usluga i pružateljima usluga udomljavanja internetskih stranica (eng. *hosting provider*). Iz grafikona koji prikazuje godišnji trend broja *botova* vidljivo je da se u Hrvatskoj broj registriranih zaraženih računala neznatno smanjuje u odnosu na prethodnu godinu. Broj otkrivenih *botova* prikazan ovim statističkim podacima temelji se na vanjskim izvorima koji dostavljaju podatke Nacionalnom CERT-u i ne odražava stvaran broj zaraženih korisničkih računala, no prikazuje trend i daje okvir stvarnog stanja.

U tablici u nastavku prikazano je deset najčešće prijavljivanih *botova* prema tipu (vrsti zlonamjernog sadržaja) u 2020. godini, koji su bili proslijeđeni davateljima internetskih usluga.

Zbroj zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2020. godine iznosi 633 284, što je smanjenje od 5.6% u odnosu na 2019. godinu.

ANDROMEDA	259882
CONFICKER	70893
NECURS	49870
AVALANCHE-ANDROMEDA	28301
ANDROID.HUMMER	27421
GAMUT	24282
MIRAI	17909
WROKNI	15439
QSNATCH	14706
SALITY	12156

Top 10 botova prema tipu u 2020. godini



Broj zabilježenih botova po danima u 2020. godini

Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću ispod 2000 *botova* dnevno, što je bio slučaj i prošle godine. Godišnji trend broja *botova* - Srednja vrijednost broja botova po danu za 2020. godinu iznosila je 1.730,28 što je smanjenje za nešto više od 100 *botova* u odnosu na 2019. godinu.

3. ZNAČAJNIJI INCIDENTI, OTKRIVENE RANJIVOSTI I DOGAĐAJI

1. KVARTAL

#476 incidenata #C&C poslužitelj #Zeus i Loki botnet #Afrodita ransomware

U prvom kvartalu 2020. godine obrađeno je **476** računalno-sigurnosnih incidenata. U **siječnju** je zaprimljeno nekoliko prijava *phishing* poruka u kojima se napadač predstavljao kao jedna od hrvatskih tvrtki. Poruka je sadržavala zlonamjerni prilog. Analizom je utvrđeno da nakon preuzimanja i pokretanja izvršna datoteka krade pristupne podatke s kompromitiranog korisničkog računala te ih šalje na udaljeni FTP poslužitelj. Kasnije tog mjeseca zaprimljena je prijava o otkrivenom zlonamjernom sadržaju smještenom kod jednog hrvatskog pružatelja usluge udomljavanja Internet stranica. Na web sjedištu je bio postavljen upravljački C&C poslužitelj koji je sadržavao web panel sučelja za *Zeus* i *Loki* **botnet**. Zatražen je sadržaj baze podataka C&C poslužitelja kako bi se ustanovilo koja su kompromitirana korisnička računala komunicirala sa zlonamjernim poslužiteljem. Krajem siječnja zabilježen je povećan broj lažnih ucjenjivačkih poruka kojima napadač pokušava iznuditi novčanu dobit od žrtve. Pošiljatelj kod ovakvih poruka lažira "From" polje na način da je pošiljateljeva adresa jednaka onoj na čiju se adresu šalje ucjenjivačka poruka. Pokušaji prijevare na ovakav način su učestali u zadnjih nekoliko godina, no potrebno je neprestano podizati svijest o ovakvim ugrozama stoga je Nacionalni CERT izdao **upozorenje** za širu javnost na svojim stranicama.

Sredinom **veljače** zabilježena je veća *phishing* kampanja usmjerena prema hrvatskim korisnicima. Poruke su sadržavale zlonamjerni privitak koji s .com domene preuzima zlonamjernu .dll datoteku. Radilo se o novoj inačici Afrodita *ransomwarea* za koju u tom trenutku još nije bio poznat *dekriptor*.

Sredinom **ožujka** pojavili su se računalno-sigurnosni incidenti vezani uz COVID-19 pandemiju. Zabilježena je *phishing* kampanja vezana uz COVID-19 u kojoj se napadač predstavlja kao Svjetska zdravstvena organizacija. Pošiljatelj je lažirao „*From*" polje poslane poruke koja je sadržavala i zlonamjerni privitak. Analizom je utvrđeno da nakon preuzimanja i pokretanja izvršna datoteka krade pristupne podatke s kompromitiranog korisničkog računala te ih šalje napadaču u obliku elektroničke poruke putem SMTP protokola. Izdano je **upozorenje** na web sjedištu i društvenim mrežama Nacionalnog CERT-a, kao i **poziv na povećan oprez** po pitanju računalne sigurnosti za vrijeme trajanja COVID-19 pandemije.

Za vrijeme pripreme rada od kuće prijavljen je DDoS napad na web sjedište login.aaiedu.hr koje je smješteno na web poslužitelju Sveučilišnog računskog centra (Srce), a koji je uzrokovao poteškoće u radu svih sustava za koje je potrebna prijava preko navedenog servisa. U napadu su iskorištene adrese javno dostupnih proxy servisa za ostvarivanje velikog broja TCP konekcija. Napadi su se ponovili nekoliko puta u narednim danima no uspješno su mitigirani.

2. KVARTAL
#420 incidenata #CoViper #infostealer

U drugom kvartalu 2020. godine obrađeno je **420** računalno-sigurnosnih incidenata. U **travnju** se nastavilo aktivno praćenje računalno-sigurnosnih incidenata vezanih uz COVID-19 pandemiju. Zabilježeno je nekoliko *phishing* kampanja sa zlonamjernim privitkom u kojima se sadržaj poruke u različitim mjerama odnosio na COVID-19. Zlonamjerni sadržaj u privitku je uglavnom bio namijenjen za krađu osjetljivih korisničkih podataka. Zaprimljena je obavijest koja je sadržavala indikatore kompromitacije zlonamjernog softvera koji je tematski vezan za COVID-19, kasnije prozvan „CoViper". Krajem travnja tri poznatije hrvatske banke prijavile su phishing kampanje usmjerene na njihove korisnike. U dva slučaja je bio cilj zaraziti korisnikovo računalo zlonamjernim kodom, a u jednom slučaju radilo se o *phishingu* s ciljem krađe korisnikovih pristupnih podataka.

Tijekom **svibnja** zabilježene su *phishing* kampanje sa zlonamjernim privitkom u kojima se sadržaj poruke u različitim mjerama odnosio na COVID-19, no u nešto manjem broju nego prethodni mjesec. Od vanjskog izvora zaprimljena je prijava o kompromitiranim računima koji su pod nadležnošću Nacionalnog CERT-a. Nacionalni CERT je poslao prijave tvrtkama i korisnicima čiji su računi kompromitirani i uputili ih na izmjenu lozinki. Radi se o podacima s računala zaraženih *„infostealer"* zlonamjernim sadržajem.

U **lipnju** je zaprimljena prijava o dvije lažne stranice na kojima se neovlašteno nalazio sadržaj kopiran sa stranica tijela javne vlasti. Na jednoj od stranica se predstavljao kao autorizacijska infrastruktura. Na stranicama su se nalazile poveznice do Google obrazaca na kojima su traženi osobni podaci korisnika (uključujući i lozinku).

3. KVARTAL
#455 incidenata #DNS server ranjivost #C&C #Emotet #lažne web trgovine

U trećem kvartalu 2020. godine obrađeno je **455** računalno-sigurnosnih incidenata. Otkrivena je kritična ranjivost na Windows DNS (eng. Domain Name System) poslužiteljima. Windows poslužitelji koji su konfigurirani tako da se koriste kao DNS poslužitelji izloženi su riziku iskorištavanja ove ranjivosti. Uspješno iskorištavanje ove ranjivosti napadačima može omogućiti izvršavanje proizvoljnog izvršnog koda u kontekstu lokalnog sistemskog korisničkog računa na poslužitelju. Nacionalni CERT je poslao obavijest svim korisnicima kod kojih je otkriven javno dostupan Windows DNS poslužitelj. Otkriven je upravljački panel (C&C) botneta na web sjedištu kod hrvatskog pružatelja usluge udomljavanja internetskog sadržaja. Nacionalni CERT zatražio je sadržaj baze unutar koje se nalaze podaci o zaraženim računalima s kojima je komunicirao C&C i poslao obavijest svim korisnicima s preporukom za uklanjanje zlonamjernog sadržaja.

U **rujnu** je bila aktivna *phishing* kampanja vezana uz COVID-19, a napadač se predstavljao kao Ministarstvo zdravlja. *"From"* polje je bilo lažirano te je glasilo Ministarstvo zdravlja Hrvatska <covid-19@zdravlje.gov.hr>. U privitku poruke elektroničke pošte nalazila se .zip datoteka u kojoj se nalazio zlonamjerni LokiBot infostealer sadržaj.

Korištenjem **OSINT** metoda otkriven je veći broj kompromitiranih web sjedišta s izmijenjenim izgledom i sadržajem web stranica. Na stranicama se nalazio i određeni broj poveznica do postavljenog zlonamjernog programskog koda na kompromitiranom web sjedištu. Nacionalni CERT je poslao prijave svim nadležnim pružateljima usluga udomljavanja internetskog sadržaja.

Cyber Crime odjel pri MUP-u dostavio je Nacionalnom CERT-u podatke o IP adresama uređaja koji su bili meta napada zlonamjernog koda Emotet. Nacionalni CERT poslao je obavijest davateljima internetskih usluga u čijoj su nadležnosti dostavljene IP adrese.

Zaprimljeno je nekoliko novih prijava za „.com.hr" domene na kojima su se nalazile lažne web trgovine. Slučaj je prijavljen Cyber Crime odjelu pri MUP-u te su zlonamjerne domene onesposobljene.

Od vanjskog CERT-a zaprimljena je informacija o većem broju IP adresa u RH koje su bile meta napada zlonamjernog koda. Od vanjskog CERT-a zaprimljena je informacija o većem broju IP adresa u RH koje su bile meta napada zlonamjernog koda Emotet. Nacionalni CERT poslao je obavijest davateljima internetskih usluga u čijoj su nadležnosti dostavljene IP adrese.

4. KVARTAL

#359 incidenata #ucjenjivačke poruke #Cit0Day

U četvrtom kvartalu 2020. godine obrađeno je **359** računalno-sigurnosnih incidenata. Otkriven je nastavak *phishing* kampanje iz listopada putem koje se širi Emotet zlonamjerni sadržaj. Nacionalni CERT je ažurirao **upozorenje** na svojim stranicama s novim prikupljenim informacijama. Sadržaj poruke elektroničke pošte povezan je s pandemijom COVID-19. Nacionalni CERT je poslao prijave na sve nadležne adrese kako bi se što prije spriječila daljnja distribucija *phishing* poruka i spriječilo širenje.

Krajem **prosinca** zabilježen je povećan broj lažnih ucjenjivačkih poruka kojima napadač pokušava iznuditi novčanu dobit od žrtve. Metoda kojom napadač pokušava ostvariti financijsku dobit se temelji na objavljivanju navodnih osjetljivih snimaka žrtve koja je primila ucjenjivačku poruku ako žrtva ne izvrši uplatu u Bitcoin vrijednosti od 750 eura. Kako bi poruku učinio što uvjerljivijom, napadač je lažirao adresu pošiljatelja kako bi bila istovjetna adresi primatelja. Nacionalni CERT poslao je prijave davatelju usluga s čijeg su se poslužitelja distribuirale poruke. Dodatno je objavljeno **upozorenje** za širu javnost na web sjedištu i društvenim mrežama Nacionalnog CERT-a. U jednom od najvećih slučajeva curenja podataka u povijesti više od 23 000 baza podataka postalo je javno dostupno. Za kolekciju baza se vjeruje kako je potekla s privatnog hakerskog foruma Cit0Day.in kojeg mnogi napadači koriste kako bi prikupili što veći broj korisničkih imena, adresa elektroničke pošte i čak lozinki u obliku čistog teksta. Sama kolekcija sastoji se od više od 226 milijuna jedinstvenih korisničkih računa. CARNET-ov Nacionalni CERT analizom je utvrdio kako je u Cit0Day kolekciji sadržano više od 47 000 korisničkih računa koji završavaju nastavkom .hr, od čega je za čak više od 24 000 korisnika lozinka dostupna u čistom tekstualnom obliku. Nacionalni CERT je **informirao javnost** o curenju podataka.

4. USLUGE CARNET-OVOG NACIONALNOG CERT-A

4.1. CERT ETA (DNSBL SUSTAV)

cert eta

Uz postojeći Spamtrap sustav koji uspješno prikuplja i analizira neželjenu poštu, razvijen je i sustav DNSBL (eng. *Domain Name Server Blacklist*) ili RBL sustav (eng. *Real Time Blacklist*) koji je u 2020. godini unaprijeđen i preimenovan u uslugu CERT ETA. Svrha CERT ETA usluge je smanjivanje količine neželjene pošte koju šalju pošiljatelji iz Hrvatske i regije (tzv. *spameri*), a koji često nisu obuhvaćeni poznatim globalnim listama. CERT ETA nije zamjena za poznate liste kao što su *Spamhaus, SpamCop, Sorbs* i sl. Usluga je dostupna na poveznici https://www.cert.hr/cert_eta/

4.2. CERT EPSILON (CVE SEARCH)

cert epsilon

Nova usluga CERT Epsilon korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa korištenijih operativnih sustava. Uz to, korisnicima omogućava brže pretraživanje poznatih ranjivosti prema specifičnim kriterijima kao što su proizvođač, CWE oznaka te ID oznaka. Ova će usluga zamijeniti trenutnu uslugu "Sigurnosne preporuke" koja korisnicima informacije distribuira putem mailing lista i stranice cert.hr.

Usluga je namijenjena svim korisnicima, a pogotovo onima koji rade u području kibernetičke sigurnosti te im je potrebna sažeta informacija o poznatim ranjivostima proizvođača i proizvoda koje su sami odabrali u obliku personalizirane poruke elektroničke pošte.

Također, informacije o ranjivostima moguće je podijeliti prema CVSS (eng. *Common Vulnerabilities Scoring System*) ocjeni što korisniku dopušta da sadržaj svojeg izvještaja kroji sukladno svojim prioritetima. Izvještaj u obliku poruke elektroničke pošte sadrži popis poznatih ranjivosti te poveznice do detaljnijih informacija o istima, a u slučaju izmjene informacija o pojedinačnoj ranjivosti u NVD (eng. *National Vulnerability Database*) bazi, korisniku se o njima šalje informacija. Usluga je dostupna na poveznici https://epsilon.cert.hr/

4.3. PLATFORMA ZA RAZMJENU INFORMACIJA O INCIDENTIMA I PRIJETNJAMA (PIXI)

Kako bi se spriječio incident i ubrzao proces njegova zaustavljanja i rješavanja, Nacionalni CERT je u 2020. godini nastavio s razvojem platforme PiXi za razmjenu informacija o računalno-sigurnosnim prijetnjama i incidentima. Ujedno se radi na proširenju korištenja platforme na operatore ključnih usluga i davatelje digitalnih usluga kako bi se osiguralo njihovo neometano poslovanje, a time i sigurnost usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti u Hrvatskoj poput bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture i poslovnih usluga za državna tijela.

4.4. SIGURNOST CARNET USLUGA

Tijekom 2020. godine služba za sigurnost usluga i infrastrukture CARNET-ovog Nacionalnog CERT-a provodila je sljedeće aktivnosti s ciljem povećanja razine sigurnosti CARNET-ovih usluga i infrastrukture:

- prikupljanje i analiza sigurnosnih događaja u CARNET mreži;
- provjera sigurnosti aplikacija, komponenata i usluga CARNET-a;
- usluga izdavanja elektroničkih certifikata (TCS-om);
- provođenje odredaba Programa sigurnosti;
- uvođenje novih tehnologija sa sigurnosnog a pekta u informacijski sustav CARNET-a;
- redovita provjera ranjivosti (eng. *Vulnerability Scanning*) ustanova članica CARNET mreže

Tijekom 2020. godine Nacionalni CERT je u sklopu tih aktivnosti:

- provodio penetracijska testiranja važnih CARNET-ovih usluga u sklopu implementacije Programa sigurnosti u CARNET-ove poslovne procese;
- provodio provjeru ranjivosti i provjeru usklađenosti sa standardima (*policy compliance*) CORE mrežnih uređaja CARNET-a
- provjeravao sigurnost usluga razvijenih u CARNET-u ili za CARNET;
- certificirao aplikacije koje pristupaju sustavu "e-Matica";
- radio na potpori sigurnosnih aspekata projekta"e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće".
- radio na projektu izrade sigurne SDDC (eng. *Software Defined Data Centre*) platforme

4.4.1. PROVJERA RANJIVOSTI

Nacionalni CERT nudi uslugu redovite provjere ranjivosti (eng. *Vulnerability Scanning*) ustanova članica CARNET mreže. Redovita provjera ranjivosti obavlja se periodički svaka tri mjeseca, a koristi je 57 ustanova iz sustava prosvjete, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže. U 2020. godini provedeno je ukupno 215 provjera ranjivosti.

Stručnjaci Nacionalnog CERT-a redovne provjere ranjivosti provode korištenjem specijaliziranih alata i samo s određenih računala s istim IP adresama. Rezultati te provjere šalju se odgovornim osobama ustanova u obliku izvještaja koji sadrži listu pronađenih sigurnosnih propusta i upute za njihovo rješavanje koje korisnicima mogu pomoći pri uspješnijem održavanju njihovih mreža.

4.4.2. TRUSTED CERTIFICATE SERVICE - TCS

CARNET-ov Nacionalni CERT nudi uslugu izdavanja elektroničkih certifikata (*Trusted Certificate Service – TCS*). Od travnja 2020. godine u suradnji s organizacijom **GÉANT** (prije DANTE i TERENA), CARNET nudi novu uslugu izdavanja elektroničkih certifikata. Izdavatelj certifikata je tvrtka **Sectigo Limited** (umjesto dosadašnje tvrtke **DigiCert**) s kojom je GÉANT zajednica sklopila ugovor.

Vrste certifikata koje CARNET nudi su poslužiteljski certifikati, klijentski S/MIME certifikati, Code Signing certifikati, Document Signing certifikati, Grid certifikati za eScience projekte te Extended Validation (EV) certifikati. U 2020. godini izdano je ukupno 1555 certifikata, što je čak 904 certifikata više nego prošle godine.

Što se tiče poslužiteljskih certifikata, njih je izdano ukupno 1231 u 2020. godini što je vrlo veliki porast u odnosu na 2019. godinu (izdano je 664 više poslužiteljskih certifikata nego prošle godine). U 2020. godini izdano je i 318 klijentskih certifikata.

5. SURADNJA I DJELOVANJE NACIONALNOG CERT-A NA MEĐUNARODNOJ RAZINI

Pored institucija EU-a i NATO-a, Nacionalni CERT surađuje s i članom je sljedećih organizacija:

CSIRT mreža - uspostavljena NIS Direktivom, a čine ju CSIRT-ovi država članica EU, CERT-EU i ENISA te djeluje s ciljem doprinosa razvoju povjerenja između država članica i promicanju brze i učinkovite operativne suradnje.

FIRST - (Forum of Incident Response and Security Teams) međunarodna konfederacija CSIRT-ova koji surađuju i zajedno rješavaju računalno-sigurnosne incidente te promoviraju programe prevencije.

TF-CSIRT - (Task Force CSIRT) radna skupina koja promiče suradnju i koordinaciju između CSIRT-a u Europi i susjednim regijama, istovremeno uspostavljajući veze s relevantnim organizacijama na globalnoj razini i u drugim regijama.

TI - (Trusted Introducer) program koji predstavlja pouzdanu okosnicu infrastrukturnih usluga timova i održava listu poznatih, akreditiranih i certificiranih timova prema njihovoj pokazanoj i provjerenoj razini zrelosti. Jedan je od tri elementa koji čine jezgru TF-CSIRT portfelja uz Sastanke radne skupine i TRANSITS. CERT.hr je akreditirani član od 2010. godine.

5.1. VJEŽBA CYBER COALITION 2020

Hrvatska akademska i istraživačka mreža - CARNET i njezin odjel za Nacionalni CERT aktivno su sudjelovali u trinaestoj po redu NATO vježbi zaštite NATO i nacionalnih računalnih sustava pod nazivom „Cyber Coalition 2020". U petodnevnoj vježbi koja je trajala od 16. do 20. studenog 2020. godine sudjelovalo je preko 1000 stručnjaka iz područja kibernetičke sigurnosti. Saveznici i partneri su zajedno vježbali kako bi održali visoku razinu kibernetičke sigurnosti zemalja članica NATO-a. Vježba, između ostalog, obuhvaća obranu od zlonamjernog sadržaja (eng. *malware)* i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri iz Hrvatske, a čiji je koordinator bio CARNET. Akademsku zajednicu u vježbi su predstavljali Fakultet elektrotehnike i računarstva Zagreb, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Učilište Algebra i Pravni fakultet u Osijeku. Sudjelovalo je i 10 subjekata iz privatnog sektora (SPAN d.o.o., DIVERTO d.o.o., Microsoft Hrvatska, INsig2 d.o.o., INFIGO IS d.o.o., CS COMPUTER SYSTEMS d.o.o., APATURA d.o.o., Eduron IS, KONČAR KET d.d., Zavod za informatiku Osijek). Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti – *Cooperative Cyber Defence Centre of Excellence* (CCD COE) – koji se nalazi u Tallinnu u Estoniji.

5.2. CSIRT MREŽA

Mreža CSIRT-ova (eng. *CSIRTs Network*) nastala je temeljem Direktive o mrežnoj i informacijskoj sigurnosti (NIS direktiva) koju je donijela Europska unija. NIS direktiva donesena je s ciljem postizanja visoke razine sigurnosti mreže i informacijskih sustava unutar EU, doprinosa razvoju povjerenja među državama članicama te promicanja brze i učinkovite operativne suradnje. Godišnje se održe tri sastanka Mreže na kojima sudjeluju predstavnici CERT-ova zemalja članica, ENISA-e te Europske Komisije. Hrvatsku na sastancima zastupa delegacija koju čine stručnjaci iz CARNET-ovog odjela za Nacionalni CERT i CERT-a Zavoda za sigurnost informacijskih sustava (ZSIS). Na sastancima su predstavljeni rezultati radnih grupa koje su oformljene unutar CSIRT mreže, a koje za cilj imaju unaprjeđenje suradnje, komunikacije i razmjene informacija među CSIRT-ovima Europske unije, poboljšanje operativnih procedura, podizanje razine zrelosti pojedinog CSIRT-a te razmjenu znanja i razvoj alata koji se koriste u CSIRT zajednici. Osim ranije spomenutog, na sastancima se redovito izvještava o aktivnostima ENISA-e, Europske Komisije, napretku razvoja Europske platforme za razmjenu informacija o računalno-sigurnosnim incidentima – MeliCERTes te o detaljima kibernetičkih vježbi koje se održavaju na EU razini ili ciljano za članove CSIRT mreže. Od 1. siječnja 2020. do 30. lipnja 2020. godine Hrvatska je, uz Rumunjsku i Finsku, bila dio predsjedavajuće trojke CSIRT mreže. Za vrijeme hrvatskog presjedanja Vijećem EU sastanak CSIRT mreže održao se u Zagrebu, no zbog COVID-19 pandemije prvi puta održan je u virtualnom izdanju. Uspješna i dobra organizacija potaknula je nastavak trenda pa su se tako svi idući sastanci održali online, a ovakav oblik sastajanja zadržat će se do okončanja pandemije i dok putovanja u druge zemlje ne budu u potpunosti omogućena.

5.3. DSI GOVERNANCE BOARD

Nacionalni CERT od 2018. godine aktivno sudjeluje u radu odbora CEF Cyber DSI Governance Board koji je uspostavljen unutar europskog CEF (eng. *Connecting European Facility*) programa sufinanciranja za projekte koji se provode u okviru implementacije Europske strategije kibernetičke sigurnosti. Nastavkom aktivnosti projekta Grow2CERT, Nacionalni CERT podržava i implementira usluge i servise nadogradnje i poboljšanja razmjene informacija o kibernetičkim prijetnjama i incidentima na europskoj razini te se pridružuje ostalim europskim projektima na zajedničkoj platformi MeliCERTes koja je ušla u drugu fazu razvoja s projektom SMART 2018/1024. Odbor ima upravljačku ulogu za sve projekte financirane iz CEF programa za kibernetičku sigurnost, usmjerava i vodi voditelje projekata, predstavlja i služi interesima EU kroz praćenje i usmjeravanje suradnje na zajedničkoj platformi, sudjeluje u procesima donošenja odluka po pitanju strategija, politika i aktivnosti unutar CEF programa te izvještava o projektima. Predstavnici Nacionalnog CERT-a sudjelovali su na dva radna sastanka odbora.

5.4. CTF INTERNATIONAL CYBEREX 2020

Predstavnici CARNET-ovog Nacionalnog CERT-a po prvi su puta sudjelovali u International **CyberEx-u**, **CTF natjecanju** u organizaciji OAS-a (*Organization of American States*), INCIBE (*Spanish National Cybersecurity Institute*) i CNPIC-a (*Spanish National Centre for Infrastructure and Cybersecurity*), čiji je cilj jačanje sposobnosti odgovora na računalno-sigurnosne incidente. Natjecanje se održalo 10. rujna 2020. goditne te je trajalo od 16 do 24 sata po našem vremenu. Natjecanje je bilo CTF jeopardy tip CTF natjecanja. Za natjecanje su se smjeli prijaviti isključivo nacionalni CERT-ovi i CSIRT zajednice, te su organizatori odabrali 81 tim koji se natjecao. Mladi tim iz Nacionalnog CERT-a osvojio je impresivno 11. mjesto. Zadaci su bili iz područja kriptografije, digitalne forenzike, reverznog inženjerstva, web sigurnosti i sličnih područja. Više informacija o natjecanju dostupno je na:

https://www.incibe-cert.es/en/international-cyberex

6. SURADNJA I DJELOVANJE NACIONALNOG CERT-A NA NACIONALNOJ RAZINI

6.1. SPORAZUM O POSLOVNOJ SURADNJI S MUP-OM

U 2020. godini nastavlja se suradnja na prevenciji i rješavanju računalnih incidenata i drugih oblika kibernetičkog kriminaliteta između MUP-a i CARNET-a (Nacionalnog CERT-a). Sporazumom koji je obnovljen još krajem 2017. godine nastavlja se suradnja s ciljem očuvanja sigurnosti kibernetičkog prostora Republike Hrvatske. S obzirom na činjenicu da suvremeni način borbe protiv kibernetičkog kriminaliteta, kao osnovni preduvjet uspješnosti, podrazumijeva dijeljenje informacija između relevantnih institucija i visoku razinu tehničkih predznanja, MUP i CARNET suglasno su osigurali međusobnu suradnju kako bi uvijek bili spremni na računalno-sigurnosne izazove kojih je svakim danom sve više.

6.2. SPORAZUM O POSLOVNOJ SURADNJI S FER-OM

CARNET-ov Nacionalni CERT nastavlja poslovnu suradnju s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu, Laboratorijem za sustave i signale (LSS) Zavoda za elektroničke sustave i obradu informacija FER-a. Tijekom 2020. godine kao rezultat suradnje objavljene su recenzije s uputama za ukupno 3 alata te je napisano 4 dokumenta na teme iz područja kibernetičke sigurnosti. Recenzija alata ***Postman*** namijenjena je uglavnom programerima i ostalim zainteresiranim stranama koji se bave sigurnosnim testiranjima aplikacija. Recenzija i upute alata ***Rubber Ducky*** namijenjene su općoj populaciji te na zanimljiv način prikazuju kako se koristi jedan od najpoznatijih USB alata. Dokumenti „***Reverzni inženjering Android aplikacija***“, „***Sigurnost HTTP REST API-ja***“, „***Hardverska strana socijalnog inženjeringa***“ i „***Savjeti za zaštitu osobnih uređaja***“ teme su namijenjene svima koji žele znati više o kibernetičkoj sigurnosti. Također, portal **antibot.hr** je sadržajno osvježen te usmjeren prema krajnjim korisnicima koji traže brze, jednostavne i pristupačne savjete kako podići razinu sigurnosti. Povodom Dana sigurnijeg interneta u veljači organiziran je interaktivni webinar “**Na digitalnom tragu**” na kojem je prisustvovalo 500 ljudi. Posebno valja izdvojiti organizaciju i provedbu prvog CTF natjecanja za srednjoškolce pod nazivom „Hacknite“ tijekom listopada u sklopu aktivnosti vezanih uz obilježavanje Europskog mjeseca kibernetičke sigurnosti. Za potrebe natjecanja razvijeni su vrlo zanimljivi i izazovni sadržaji koji su izazvali snažnu potporu svih sudionika, a pogotovo učenika srednjih škola. Organiziranjem natjecanja svim zainteresiranim učenicima dana je prilika za učenje o kibernetičkoj sigurnosti. Natjecanje je bilo vrlo uspješno te će se sigurno organizirati i narednih godina.

6.3. SUDJELOVANJE U RADU TIJELA IZ NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI

Tijekom 2020. godine Nacionalni CERT nastavio je aktivno sudjelovati radu nacionalnih relevantnih tijela proizašlih iz **Nacionalne strategije kibernetičke sigurnosti**: **Nacionalnog vijeća za kibernetičku sigurnost** i **Operativno-tehničke koordinacije za kibernetičku sigurnost**. Uz praćenje provedbe Strategije i Akcijskog plana ovim međuresornim tijelima povjeravaju se i određene zadaće vezane uz upravljanje u kibernetičkim krizama. Sjednice navedenih tijela održavaju se jednom mjesečno (osim u iznimnim situacijama kada je moguće sazvati izvanrednu sjednicu).

6.4. ZAKON I UREDBA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

Tijekom 2020. godine Zavod za sigurnost informacijskih sustava i Nacionalni CERT nastavili su s obavezama koje im kao nadležnim CSIRT-ovima proizlaze iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Istim je Zakonom Nacionalni CERT proglašen nadležnim CSIRT-om za sve operatore ključnih usluga iz sektora bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, poslovnih usluga za državna tijela te davatelja digitalnih usluga. Osim toga, CARNET u Zakonu ima ulogu samog operatora ključne usluge (DNS usluga) kao i ulogu Tehničkog tijela za ocjenu sukladnosti. U 2020. godini, u suradnji sa Središnjim državnim uredom za razvoj digitalnog društva (SDURDD) provedena je prva ocjena sukladnosti sa Zakonom u CARNET-u i Srcu. Modul "Prijava incidenta prema ZKS-u" može se pronaći na web sjedištu **www.cert.hr**.

6.5. SURADNJA S HRVATSKOM UDRUGOM BANAKA

Nacionalni CERT je i u 2020. godini sudjelovao na mjesečnim sastancima Odbora za sigurnost Hrvatske udruge banaka. Djelokrug rada Odbora je organiziranje zajedničkih aktivnosti radi unapređenja informacijske sigurnosti, razvoja sustava upravljanja rizicima nastalih zloupotrebom informacija i informacijskih kanala te pripremanje i davanje inicijative za formiranje pravne i zakonske regulative informacijske sigurnosti u Hrvatskoj. Međusektorska suradnja vrlo je važna u borbi protiv kibernetičkih incidenata. Suradnja s Hrvatskom udrugom banaka započela je i ranije kroz zajedničke mjere iz Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, radnu skupinu iz projekta GrowCERT, no pojavila se i dodatna potreba za jačanjem suradnje zbog Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Sektor bankarstva jedan je od pet sektora za koji je Nacionalni CERT nadležni CSIRT sukladno Zakonu. Na sastancima se izvještava o trendovima i eventualnim aktualnim ugrozama u području kibernetičke sigurnosti, a zainteresirane banke mogu se obraditi Nacionalnom CERT-u kako bi zaprimale tjedne izvještaje o ranjivim servisima.

HRVATSKA UDRUGA BANAKA
CROATIAN BANKING ASSOCIATION

6.6. OBILJEŽAVANJE EUROPSKOG MJESECA KIBERNETIČKE SIGURNOSTI

CARNET-ov Nacionalni CERT i ove je godine aktivno obilježio Europski mjesec kibernetičke sigurnosti. Tijekom listopada 2020. godine proveden je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti, s naglaskom na mrežnu i informacijsku sigurnost te promociju sigurnijeg korištenja interneta za sve korisnike.

Nacionalni CERT preuzeo je ulogu nacionalnog koordinatora za provedbu Europske kampanje za podizanje svijesti o kibernetičkoj sigurnosti tijekom listopada te je ažurirao sadržaj na stranici https://cybersecuritymonth.eu/countries/croatia.

Pod sloganom "Kibernetička sigurnost je zajednička odgovornost" teme na kojima je 2020. godine bio naglasak su digitalne vještine, kibernetička higijena, digitalni trag, internet prevare te siguran rad od kuće. Sukladno navedenim temama pripremljene su četiri infografike na hrvatskom jeziku koje su prezentirane široj javnosti, dva najavna spota za infografike, dva kratka animirana filma o internet prevarama i digitalnim kompetencijama i šest blic filmova - isječaka s naglascima i ključnim porukama za korisnike interneta o njihovoj zaštiti i odgovornom korištenju internetskih usluga.

Infografiku "Digitalni trag" zaposlenici Nacionalnog CERT-a su samostalno izradili i ponudili ostalim članicama EU na korištenje. Tekst inforgrafike je preveden na ostale jezike i objavljen u tri europske zemlje.

Na društvenim stranicama @CERT.hr i @HRCERT do početka listopada objavljivane su zanimljive činjenice iz područja kibernetičke sigurnosti. Najzahtjevnija i najveća aktivnost kojom se obilježio Europski mjesec kibernetičke sigurnosti je "Hacknite", prvo hrvatsko CTF natjecanje za srednjoškolce o kojem možete pročitati u sljedećem poglavlju.

EUROPSKI MJESEC KIBERNETIČKE SIGURNOSTI

6.7. HACKNITE – PRVO HRVATSKO CTF NATJECANJE ZA SREDNJOŠKOLCE

HACKNITE.hr
CARNET CERT.hr

U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je prvo hrvatsko CTF natjecanje za srednjoškolce koje se provodilo 17. i 18. listopada 2020. godine. Natjecanju su mogli pristupiti samo prijavljeni timovi (ukupno šest osoba – prijavitelj i pet članova tima) s dobivenim korisničkim podacima za pristup natjecanju. Pravo sudjelovanja imali su svi učenici srednjih škola u Republici Hrvatskoj stariji od 16 godina uz mentorstvo svojih profesora kao Prijavitelja timova.

Natjecanje je bilo organizirano u obliku CTF-a (*Capture the Flag*), a cilj je bio proširiti svijest o važnosti primjene sigurnosnih mjera te izbjegavanju i ispravljanju mogućih sigurnosnih propusta u programskom kôdu, postavkama ili nekoj drugoj komponenti računalnog sustava.

U natjecanju je sudjelovao 31 srednjoškolski tim iz 16 gradova i 23 srednje škole. Pobjednički tim bio je Tim ELPROS iz Elektrotehničke i prometne škole Osijek.

Učenici su imali prilike puno naučiti, a čime su se iskazali je odlična suradnja između timova i međosobno pomaganje, iako su se nalazili na "suparničkim" stranama. Reakcije na natjecanje su bile vrlo pozitivne te se nadamo da će se i narednih godina natjecanje ovakvog tipa uspješno organizirati i da će učenici koji nisu uspjeli igrati ove godine priliku dobiti u idućem mjesecu kibernetičke sigurnosti.

6.8. DJELOVANJE PUTEM JAVNIH MEDIJA I OBRAĆANJA JAVNOSTI

1/2020 – sudjelovanje u emisiji HRT-a "Glas potrošača" na temu sigurnosti potrošača na internetu

2/2020 – davanje izjave za HRT na temu internetskih ucjena

2/2020 - održan webinar za u sklopu obilježavanja Dana sigurnijeg interneta nazvan "Na digitalnom tragu"

3/2020 - sudjelovanje u emisiji HRT-a "Potrošački kod" na temu kibernetičke sigurnosti i rada u digitalnom okruženju

4/2020 – davanje izjave za Radio Sljeme na temu kibernetičkih prijetnji vezanih uz COVID 19

4/2020 – sudjelovanje u Dnevniku HRT-a na temu kibernetičke sigurnosti za vrijeme rada od kuće te *phishing* porukama vezanima uz COVID 19 pandemiju.

10/2020 - sudjelovanje na konferenciji CSC20 (Cyber Security Conference) u Osijeku s temom "Kibernetička sigurnost u ustanovama - Praktični savjeti i primjeri dobre prakse"

10/2020 - gostovanje na okruglom stolu u sklopu CSC20 konferencije na temu "Iskustva i izazovi provedbe Zakona o kibernetičkoj sigurnosti"

11/2020 - tri interaktivna izlaganja na konferenciji CUC20 na teme "Sigurnost u online okruženju", "Popularizacija i učenje o kibernetičkoj sigurnosti kroz igrifikaciju" i "TCS - Trusted Certificate Service"

11/2020 – Gostovanje na više različitih nacionalnih televizija (HRT, Nova TV, RTL) na temu curenja podataka te zaštite korisničkih podataka

— Informiranje javnosti putem web sjedišta Nacionalnog CERT-a (**www.cert.hr**) – 137 224 posjetitelja u 2020. godini. Korištenjem novog sustava za praćenje posjetitelja web sjedišta bilježimo značajan porast u odnosu na 2019. godinu, a posebno valja izdvojiti situacije kada su objavljivana upozorenja prilikom čega je promet značajno premašivao prošlogodišnje brojke

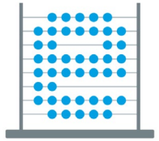
— Informiranje javnosti putem društvenih mreža Facebook (**@CERT.hr** - 1739 pratitelja) i Twitter (**@HRCERT** – 1142 pratitelja)

— Dano je više od 15 intervjua i izjava za časopise te tiskane i digitalne medije, npr. Poslovni lider, 24 sata, Indeks, Večernji list, Jutarnji list, T-portal

7. PROJEKTI

7.1. E-ŠKOLE

U 2020. godini CARNET-ov Nacionalni CERT započeo je s provedbom projekta "**e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće**". Radi se o II. fazi projekta, dok je I. faza (pilot projekt) završena 31. kolovoza 2018. godine. Opći cilj II. faze programa je podizanjem digitalne zrelosti škola doprinijeti digitalnoj transformaciji obrazovnih i administrativnih procesa u obrazovnom sustavu, te tako osposobiti učenike za život i rad u 21. stoljeću. Projektni rezultati ostvarit će se kroz projektne elemente i podelemente, a odjel za Nacionalni CERT aktivno je uključen u elemente "Sigurnosti" s ciljem postizanja adekvatne razine sigurnosti CARNET mrežne infrastrukture, infrastrukture podatkovnih centara, sigurnost ustanova i javno dostupnih usluga i aplikacija. Provodi se sveobuhvatna procjena usluga i aplikacija razvijenih unutar projekta kako bi se ostvarila njihova spremnost za postavljanje u produkcijsku okolinu. S projektnim partnerom **ICENT** (Inovacijski centar Nikola Tesla) provode se istraživačke aktivnosti s ciljem poboljšavanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola.



e-Škole

7.2. GROW2CERT

Nacionalni CERT je u 2020. godini nastavio s provedbom projekta sufinanciranog sredstvima Europske unije putem Instrumenta za povezivanje Europe (eng. CEF – *Connecting Europe Facility*) pod nazivom **Grow2CERT** – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti (eng. *Increasing maturity of National CERT for stronger cooperation in cybersecurity community*). Cilj projekta je povećati pripravnost Nacionalnog CERT-a za odgovor na kibernetičke prijetnje i incidente. Projektom se nastavlja razvoj platforme PiXi za razmjenu informacija o računalno-sigurnosnim prijetnjama i incidentima razvojem i integracijom dodatnih komponenti koje će omogućiti interakciju s MeliCERTes-om. Ujedno se proširuje korištenje platforme na operatore ključnih usluga i davatelje digitalnih usluga kako bi se osiguralo njihovo neometano poslovanje, a time sigurnost usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti u Hrvatskoj poput bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture i poslovnih usluga za državna tijela. Nacionalni CERT nastavlja s provedbom aktivnosti s ciljem podizanja svijesti opće javnosti o kibernetičkoj sigurnosti putem digitalne kampanje, objava na društvenim mrežama i organiziranja kvizova, okruglih stolova i drugih događanja posvećenih temama kibernetičke sigurnosti tijekom Europskog mjeseca kibernetičke sigurnosti. Poseban naglasak stavljen je na „kibernetičku higijenu", odnosno održavanje visoke razine sigurnosti korisnika interneta uz odgovorno korištenje suvremenih informacijsko-komunikacijskih tehnologija. **Od 1. siječnja 2020. do 30. lipnja 2020. godine Hrvatska je, uz Rumunjsku i Finsku, bila dio predsjedavajuće trojke CSIRT mreže. Za vrijeme hrvatskog predsjedanja Vijećem EU sastanak CSIRT mreže održao se u Zagrebu, no zbog COVID-19 pandemije prvi puta održan je u virtualnom izdanju**. Opseg projekta čini osam različitih aktivnosti. Uz upravljanje projektom i komunikaciju i vidljivost, ostale aktivnosti odnose se na nadogradnju nacionalne platforme i pripremu za nove interakcije / korištenje komponenti MeliCERTes-a, aktivnosti podizanja svijesti, povećanje razine zrelosti Nacionalnog CERT-a na temelju SIM3 kriterija, poboljšanje kapaciteta osoblja CERT-a i drugih nacionalnih tijela koja sudjeluju u provedbi mjera kibernetičke sigurnosti te nabava opreme i licenci za podizanje ukupne razine kibernetičke sigurnosti. Projekt u vrijednosti većoj od milijun eura provodit će se do kraja listopada 2021. godine.

grow2cert

Sufinancira Europska unija
Instrument za povezivanje Europe

7.3. CEKOM

Nacionalni CERT kao partner sudjeluje u EU projektu **CEKOM** (Centar kompetencija). Cilj trogodišnjeg projekta je 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.

7.4. CYBER EXCHANGE

U studenom 2018. godine započeo je projekt **„CyberExchange"** u okviru Instrumenta za povezivanje Europe – *Connecting Europe Facility* (CEF). Nositelj projekta je udruženje CZ.NIC iz Češke, a u projektu sudjeluje 10 država Europske unije (Austrija, Hrvatska, Češka, Grčka, Latvija, Luksemburg, Malta, Poljska, Rumunjska i Slovačka). Radi se o dvogodišnjem projektu s ciljem jačanja suradnje između nacionalnih i državnih CSIRT-ova/CERT-ova. CyberExchange je pokrenut radi poboljšanja odaziva na sve učestalije prijetnje kibernetičkoj sigurnosti te naglašava važnost prekogranične suradnje u njihovom suzbijanju. Osim toga, važna je i stručnost osoba koje rade u području kibernetičke sigurnosti stoga se provodi razmjena djelatnika CERT-ova/CSIRT-ova tijekom koje individualni članovi pojedinih timova imaju priliku razmijeniti iskustva te unaprijediti svoju stručnost. Projektom se također stavlja fokus na implementaciju softverskih alata koje su razvili timovi uključeni u projekt kako bi se koristili na dobrobit cijele sigurnosne zajednice. Tijekom 2019. godine Nacionalni CERT sudjelovao je u čak tri razmjene: Nacionalni CERT posjetio je CERT Latvija i obrnuto na temu povećanja zrelosti CERT-ova te je CERT Austrija posjetio Nacionalni CERT na puna dva tjedna po temi provjere ranjivosti, penetracijskog testiranja, obrade incidenata i podizanja svijesti korisnika. U 2020. godini planirana je razmjena u Poljsku gdje bi djelatnici Nacionalnog CERT-a razvijali sposobnosti analize zlonamjernog sadržaja, no razmjena je odgođena do kraja pandemije koronavirusa. Iz istog razloga trajanje projekta je produženo do kraja lipnja 2021., po potrebi i dulje.

Cyber Exchange

Sufinancira Europska unija
Instrument za povezivanje Europe

8. ZAKLJUČAK

Tijekom 2020. godine CARNET-ov Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenta i smanjenja štete u slučaju njihovog nastanka.

Prema statistikama može se zaključiti kako je razina prijavljenih incidenata u porastu pa je tako obrađeno 66% incidenata više nego prošle godine. To možemo pripisati većoj vidljivosti Nacionalnog CERT-a u javnosti i stalnim aktivnostima podizanja svijesti javnosti o ugrozama koje dolaze s interneta, širenju suradnje s drugim CERT-ovima, hosting providerima i ISP-evima kao i korištenju OSINT metoda (eng. *Open Source Intelligence*) kojima su otkrivena kompromitirana web sjedišta. Zbog korištenja OSINT metoda broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu povećao se za čak 58%. Što se tiče broja registriranih botova vidi se blagi pad, no broj botova po danu se najčešće kreće nešto ispod 2000 što ne predstavlja razliku u odnosu na prethodne godine. Velika promjena odnosi se i na rast broja incidenta pogađanje zaporki koji je u 2020. godini došao na 3. mjesto, dok do sada nikad nije bio u top 3 incidenta.

U 2020. godini javnosti su predstavljene dvije nove usluge – CERT ETA i CERT EPSILON. Svrha CERT ETA usluge je smanjivanje količine neželjene pošte koju šalju pošiljatelji iz Hrvatske i regije (tzv. spameri), a koji često nisu obuhvaćeni poznatim globalnim listama. Usluga CERT Epsilon je nova usluga CARNET-ovog Nacionalnog CERT-a koja korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa nekih korištenijih operativnih sustava i u potpunosti zamjenjuje "Sigurnosne preporuke" u 2021. godini.

CARNET-ov Nacionalni CERT nastavio je razvijati suradnju s institucijama izvan Republike Hrvatske, kao što su drugi CERT timovi, s institucijama EU-a i NATO-a te s ostalim tijelima unutar Republike Hrvatske, a sve u svrhu razvitka zajedničkih interesa u području kibernetičke sigurnosti. Tijekom 2020. godine uspješno je sudjelovao u NATO-ovoj Cyber Coalition vježbi, gdje je Republika Hrvatska sudjelovala u svojstvu igrača. Vježba je, između ostalog, obuhvaćala obranu od zlonamjernog sadržaja (eng. *malware*) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri iz Hrvatske. Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti.

Predstavnici CARNET-ovog Nacionalnog CERT-a po prvi su puta sudjelovali u International CyberEx-u, CTF natjecanju čiji je cilj jačanje sposobnosti odgovora na računalno sigurnosne incidente. Zadaci su bili iz područja kriptografije, digitalne forenzike, reverznog inženjerstva, web securitya i sličnih područja. Mladi tim iz Nacionalnog CERT-a osvojio je impresivno 11. mjesto.

CARNET-ov Nacionalni CERT i ove je godine aktivno obilježavao Europski mjesec kibernetičke sigurnosti. Tijekom listopada 2020. godine Nacionalni CERT proveo je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti, s naglaskom na mrežnu i informacijsku sigurnost te promociju sigurnijeg korištenja interneta za sve korisnike. Nacionalni CERT preuzeo je i ulogu nacionalnog koordinatora za provedbu Europske kampanje za podizanje svijesti o kibernetičkoj sigurnosti tijekom listopada. U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je prvo hrvatsko CTF natjecanje za srednjoškolce koje se provodilo 17. i 18. listopada 2020. godine. U natjecanju je sudjelovao 31 srednjoškolski tim iz 16 gradova i 23 srednje škole.

Javnost je o aktivnostima informirana putem web sjedišta Nacionalnog CERT-a (**www.cert.hr**) – 137 224 posjetitelja u 2020. godini, a posebno valja izdvojiti situacije kada su objavljivana upozorenja prilikom čega je promet značajno premašivao prošlogodišnje brojke. Informirana je javnost i putem društvenih mreža Facebook (**@CERT.hr** - 1739 pratitelja) i Twitter (**@HRCERT** – 1142 pratitelja). Odrađeno je više od 15 intervjua i izjava za časopise te tiskane i digitalne medije, npr. Poslovni lider, 24 sata, Indeks, Večernji list, Jutarnji list, T-portal a i snimljeno je nekoliko reportaža za HRT, Novu TV i RTL.

CARNET-ov Nacionalni CERT aktivno se uključio u projekt "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće". Odjel za Nacionalni CERT bit će aktivno uključen u element "Sigurnost" s ciljem postizanja adekvatne razine sigurnosti CARNET mrežne infrastrukture, infrastrukture podatkovnih centara, sigurnost ustanova i javno dostupnih usluga i aplikacija. Provest će se sveobuhvatna procjena usluga i aplikacija razvijenih unutar projekta kako bi se ostvarila njihova spremnost za postavljanje u produkcijsku okolinu. S projektnim partnerom ICENT (Inovacijski centar Nikola Tesla) provest će se istraživačke aktivnosti u cilju poboljšavanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola.

Nacionalni CERT je u 2020. godini nastavio s provedbom projekta sufinanciranog sredstvima Europske unije putem Instrumenta za povezivanje Europe (eng. CEF – *Connecting Europe Facility*) pod nazivom Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti. Cilj projekta je povećati pripravnost Nacionalnog CERT-a za odgovor na kibernetičke prijetnje i incidente. Između ostalog, projektom se nastavlja razvoj platforme PiXi za razmjenu informacija o računalno-sigurnosnim prijetnjama i incidentima na nacionalnoj razini.

Zaključno, Nacionalni CERT je u 2020. godini ostvario značajne pomake na području nacionalne i međunarodne suradnje, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

9. MALI POJMOVNIK RAČUNALNO-SIGURNOSNIH INCIDENATA

Nacionalni CERT obrađuje incidente ako se jedna od strana uključenih u incident nalazi u .hr domeni ili u hrvatskom IP adresnom prostoru. U nastavku se nalazi kratak opis incidenata koji se spominju u ovom izvještaju.

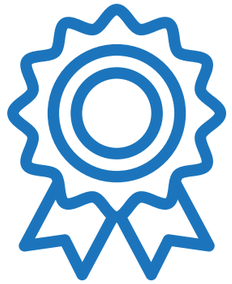
POJAM	KRATKI OPIS
Bot/Botnet	Zaraženo računalo/mreža zaraženih računala
C&C	Komandni i kontrolni poslužitelj koji upravlja mrežom zaraženih računala
Phishing	Masivno zasipanje velikog broja osoba porukama u kojima se na prijevaru traži odavanje tajnih podataka
Spam	Neželjena elektronička poruka poslana zbog namjere oglašavanja raznog propagandnog sadržaja, ili u svrhu phishing napada, ili kao sredstvo distribucije poveznica do zlonamjernog softvera
Malware	Zlonamjerni softver namijenjen infiltraciji računala bez znanja njegovog vlasnika, odnosno korisnika
Web Defacement	Izmjena izgleda stranica web sjedišta
Ransomware	Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala.
Phishing URL	Poveznica do lažne *web* stranice koja oponaša legitimnu stranicu na kompromitiranom *web* sjedištu s ciljem krađe povjerljivih korisničkih podataka
Malware URL	Poveznica do zlonamjernog sadržaja na kompromitiranom web sjedištu
Spam URL	*Spam* sadržaj na kompromitiranom web sjedištu koji se distribuira kroz *spam* poruke
DoS	Napad uskraćivanja usluge
Spyware	Vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole
Backdoor alati	Alati koji omogućuju drugom korisniku da se služi žrtvinim računalom dok je žrtva spojena na internet, bez znanja žrtve
SQL injection napadi	Napad umetanjem SQL koda koji iskorištava ranjivosti na sloju baze podataka
Brute force napadi	Testiranje svih kombinacija slova, brojeva i posebnih znakova s ciljem otkrivanja zaporki

GDJE NAS SIGURNO MOŽETE NAĆI?

Ovisno o tome kako možemo pomoći - za opće informacije nazovite na **01 6661 650** ili pišite na ncert@cert.hr, računalno-sigurnosne incidente prijavite na incident@cert.hr,a za upite medija kontaktirajte nas na **press@carnet.hr**. Sve ostale informacije o Nacionalnom CERT-u nalaze se na adresi www.cert.hr.

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

NACIONALNI CERT U BROJKAMA



1231
Poslužiteljski elektronički certifikati

318
Klijentski elektronički certifikati

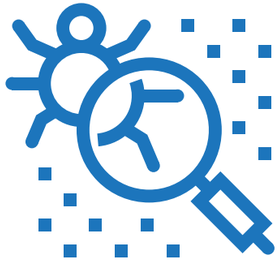
3682
Sigurnosne preporuke

5
Certificiranje CARNET aplikacija koje pristupaju sustavu „e-Matica“

137 224
Posjeta portalu **www.cert.hr**

1739
Broj pratitelja na Facebook **@CERT.hr**

1142
Broj pratitelja na Twitter **@HRCERT**



633 284
Broj registriranih botova

1710
Obrađenih sigurnosnih incidenata

215
Provjera ranjivosti

46
Analiza prijavljenih sigurnosnih događaja u CARNET mreži

16
Provjera sigurnosti CARNET aplikacija, komponenata i usluga

107
Objavljene novosti

11
Broj objavljenih upozorenja

4
Broj objavljenih dokumenata

3
Broj objavljenih alata

Hrvatska akademska
i istraživačka mreža – CARNET
Josipa Marohnića 5, 10000 Zagreb, Hrvatska
tel: +385 1 6661 616, mail: ured@carnet.hr

Podrška:
tel: +385 1 6661 555
mail: helpdesk@carnet.hr