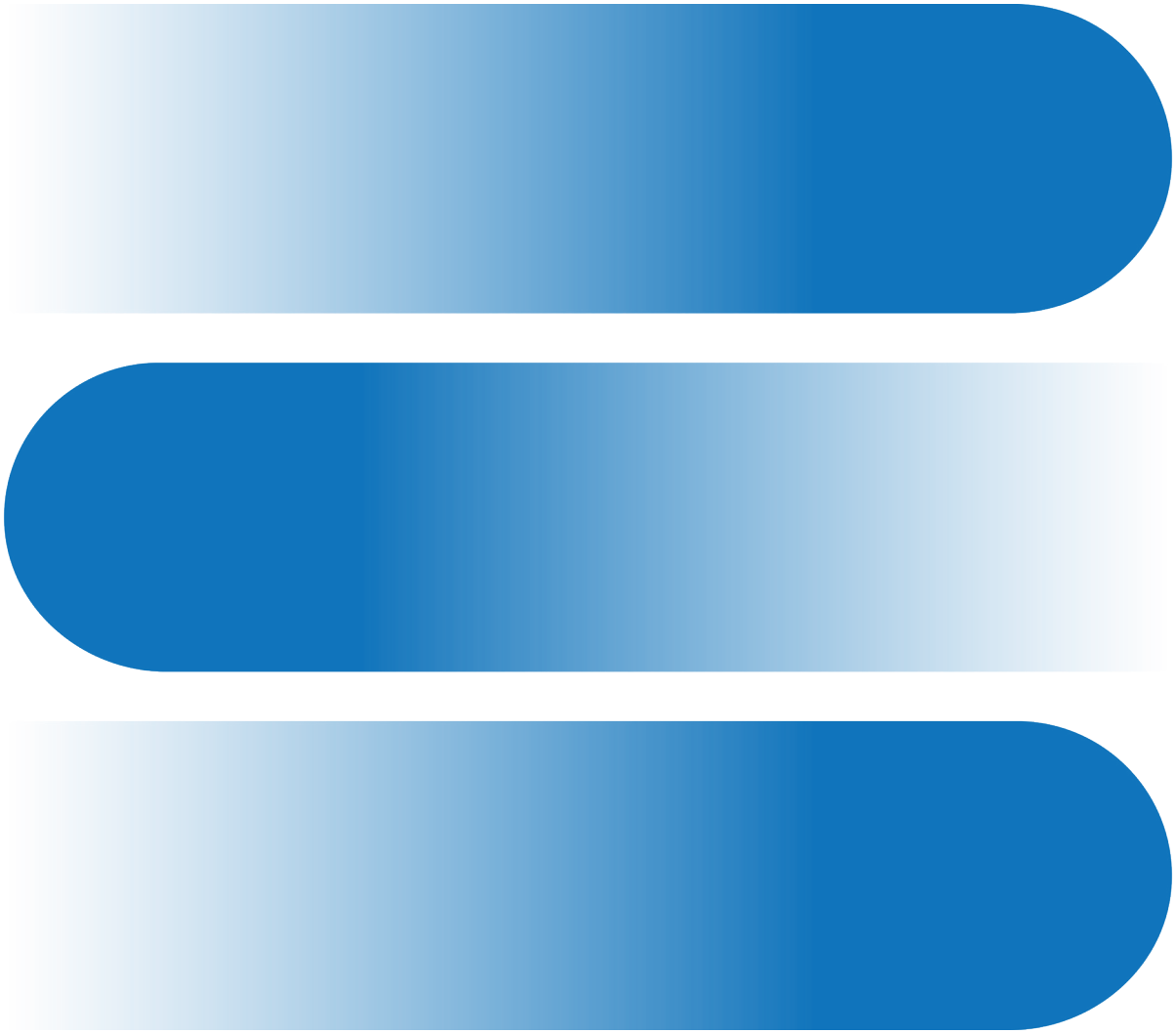
CARNET

CERT.hr
surfaj sigurnije

Godišnji izvještaj Nacionalnog CERT-a za 2019. godinu

Sadržaj



1 Usluge Nacionalnog CERT-a

Nacionalni CERT (eng. *Computer Emergency Response Team*) odjel je Hrvatske akademske i istraživačke mreže – CARNET, čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj. Nacionalni CERT bavi se 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 bavi se incidentima sa znatnim učinkom prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, poslovnih usluga za državna tijela i davatelje digitalnih usluga.

Nacionalni CERT osnovan je 30. listopada 2007. godine kada je Upravno vijeće CARNET-a prema obvezama Zakona o informacijskoj sigurnosti donijelo izmjene Statuta kojima je uspostavljen Odjel za Nacionalni CERT. Nakon ustrojstva Nacionalnog CERT-a započinje uspostava hijerarhijski ustrojene infrastrukture CERT timova koja je nužna za preventivno djelovanje i učinkovitu koordinaciju pri rješavanju računalno-sigurnosnih incidenata vezanih uz informacijsko-komunikacijske sustave.

Tijekom 2019. 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 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:

- svakodnevno izdavanje sigurnosnih preporuka za najpopularnije operativne sustave;
- izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti;
- izdavanje i objavljivanje tehničkih informacija o sigurnosnim alatima;
- praćenje i objavljivanje novosti u vezi kibernetičke sigurnosti;
- provjera ranjivosti ustanova članica CARNET mreže;
- provjera ranjivosti drugih korisnika u Republici Hrvatskoj, prema dogovoru;
- informiranje javnosti putem portala www.antibot.hr s ciljem suzbijanja *botova*;
- sudjelovanje u televizijskim i radijskim emisijama;
- sudjelovanje na predavanjima u sklopu konferencija i radionica;
- održavanje predavanja i webinara o sigurnosti na internetu.

Broj izvršenih proaktivnih mjera u 2019. godini

Alati	12
Dokumenti	12
Novosti	109
Ukupno preporuka	2 999
Broj provjera ranjivosti	222
Broj izdanih elektroničkih certifikata	631

Portal antibot.hr

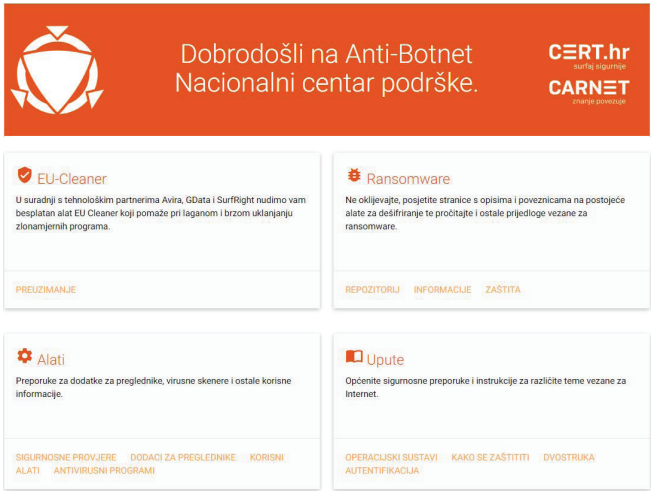
Nacionalni centar potpore **Antibot** krajnjim korisnicima omogućuje bolju detekciju i uklanjanje zlonamjernih programa s njihovih računala. U 2019. godini portal Antibot posjetilo je 34 375 korisnika.

EU-Cleaner

U suradnji s tehnološkim partnerima Avira, Gdata i SurfRight, Antibot nudi mogućnost besplatnog preuzimanja alata ***EU Cleaner*** koji pomaže pri laganom i brzom uklanjanju zlonamjernih programa.

Ransomware

U posebnoj kategoriji ***Ransomware*** mogu se pronaći sve bitne informacije i savjeti vezani uz *ransomware*, kao i poveznice na alate za dešifriranje datoteka u slučaju otkrivanja ključa. Jednom tjedno zainteresiranoj javnosti prenose se novosti o zlonamjernom *ransomware* sadržaju.



Alati

Kategorija **Alati** na jednom mjestu nudi vrlo koristan pregled antivirusnih programa u besplatnoj ili naplatnoj inačici, dodataka koji nadopunjavaju *web* preglednike s ciljem povećanja sigurnosti računala te poveznica za preuzimanje istih, preporuka za vanjske sigurnosne provjere, poput provjera *phishing* stranica ili zlonamjernih programa, te korisnih alata koji krajnjem korisniku mogu poslužiti u svakodnevnom korištenju računala, tableta ili pametnih telefona (donosi poveznice za preuzimanje različitih alata kao što su alati za izradu sigurnosnih kopija, spremanje lozinki i mnogi drugih). Pomoću senzora instaliranih unutar većih ISP-eva i fakulteta u Hrvatskoj, CARNET (Nacionalni CERT) može detektirati aktivne zlonamjerne domene kojima pristupaju zaražena korisnička računala.

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.

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.

1.2. Reaktivne mjere

Reaktivnim mjerama djeluje 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:

- obrada incidenata (svi korisnici u Hrvatskoj, uključujući korisnike CARNET-a);
- obrada incidenata sa znatnim učinkom sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga;
- 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.

Statistički podaci provedenih reaktivnih mjera u 2019. godini nalaze se u **poglavlju 5: Stanje računalnih incidenata i statistike.**

DNSBL

Uz postojeći Spamtrap sustav koji uspješno prikuplja i analizira neželjenu poštu, Nacionalni CERT je razvio i sustav DNSBL (eng. *Domain Name Server Blacklist*) ili RBL sustav (eng. *Real Time Blacklist*). Svrha DNSBL liste je smanjivanje količine neželjene pošte koju šalju pošiljatelji iz Hrvats ke i regije (tzv. *spameri*), a koji često nisu obuhvaćeni poznatim globalnim listama. DNSBL lista nije zamjena za poznate liste kao što su *Spamhaus, SpamCop, Sorbs* i sl. Usluga je razvijena u sklopu projekta GrowCERT i namijenjena je korisnicima u Hrvatskoj, a dostupna je od svibnja 2018. godine.

1.3. Sigurnost CARNET usluga

U sklopu Odjela za Nacionalni CERT djeluje Služba za sigurnost usluga i infrastrukture CARNET mreže koja uz Službu za obradu incidenata provodi aktivnosti s ciljem povećanja razine sigurnosti CARNET-ovih usluga, računalnih sustava i cjelokupne mreže, a to su:

- analiza prijavljenih sigurnosnih događaja u CARNET mreži;
- provjera sigurnosti aplikacija, komponenata i usluga razvijenih u CARNET-u ili za CARNET uz provođenje penetracijskih testiranja prema Programu sigurnost;
- certificiranje aplikacija koje pristupaju sustavu "e-Matica";
- izdavanje elektroničkih certifikata (TCS-om);
- uvođenje novih tehnologija sa sigurnosnog aspekta u informacijski sustav CARNET-a;
- pripreme za potporu sigurnosnom dijelu projekta "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće"

Broj provedenih aktivnosti u 2019. godini

Analiza prijavljenih sigurnosnih događaja	62
Provjera sigurnosti aplikacija, komponenata i usluga	18
Certificiranje aplikacija koje pristupaju sustavu „e-Matica"	6
Izdani poslužiteljski certifikati	567
▪ EV - Extended Validation	28
▪ Klijentski certifikati	33

2 Suradnja i djelovanje Nacionalnog CERT-a na međunarodnoj razini

Pored institucija EU-a i NATO-a, Nacionalni CERT surađuje s međunarodnim udruženjima CERT-ova FIRST (eng. *Forum of Incident Response and Security Teams*) i TI (eng. *Trusted Introducer*), čiji je akreditirani član. Zavod za sigurnost informacijskih sustava (ZSIS) je uz Nacionalni CERT predstavnik Hrvatske u mreži europskih CERT timova "CSIRT Network".

2.1. Vježba Cyber SOPEx 2019

Agencija Europske unije za mrežnu i informacijsku sigurnost - ENISA (eng. *European Network and Information Security Agency*) je 15. svibnja 2019. godine organizirala kibernetičku vježbu "Cyber SOPEx" s ciljem poboljšanja suradnje između CSIRT-ova (eng. *Computer Security Incident Response Team*). CERT timovi u scenarijima postupaju prema procedurama za obradu incidenata (eng. *SOP – Standard Operating Procedures*). Ovo je bila druga vježba takvog tipa. U vježbi je, uz Nacionalni CERT, sudjelovalo 52 člana europske mreže CSIRT-ova iz 26 zemalja EU. Scenarij vježbe se temeljio na kibernetičkim napadima prije i za vrijeme izbora za Europski parlament. Vježbom se, osim suradnje, poticao i kreativni pristup rješavanju računalno-sigurnosnih incidenata. "Cyber SOPEx" je prvi korak u seriji ENISA-inih vježbi kojima je fokus na podizanju svijesti dionika vježbe o pojedinoj situaciji, dijeljenju informacija, razumijevanju uloga i odgovornosti unutar tima te korištenju alata potrebnih za uspješno rješavanje incidenata. Dugogodišnji cilj ovog projekta je poboljšanje operativne suradnje u području kibernetičke sigurnosti unutar Europske unije.

2.2. Vježba Cyber Coalition 2019

Hrvatska akademska i istraživačka mreža - CARNET i njezin odjel za Nacionalni CERT aktivno su sudjelovali u dvanaestoj po redu NATO vježbi zaštite NATO i nacionalnih računalnih sustava pod nazivom „Cyber Coalition 2019". U petodnevnoj vježbi koja je trajala od 2. do 6. prosinca 2019. 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. Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti – *Cooperative Cyber Defence Centre of Excellence* (CCD COE) – koji se nalazi u Tallinnu u Estoniji.

2.3. Vježba NATO CMX 2019

CARNET i njegov odjel za Nacionalni CERT sudjelovali su u simulacijskoj vježbi upravljanja u krizama Organizacije Sjevernoatlantskog ugovora (eng. *Crisis Management Exercise* – CMX19) kao član Nacionalne upravljačke skupine za pripremu i provedbu. Vježba se provodila od 9. do 15. svibnja 2019. godine. Cilj vježbe bio je testiranje sposobnosti komunikacije unutar zemlje, ali i između partnera te sposobnosti donošenja odluka vezanih uz strateška vojno-politička pitanja.

2.4. Counter Hybrid Threats seminar

Od 3. do 5. rujna 2019. godine po prvi se puta u Hrvatskoj održao NATO seminar *"Counter Hybrid Threats"*. Seminar je namijenjen zemljama članicama NATO saveza i partnerima kako bi bili spremni odgovoriti na prijetnje 21. stoljeća. Seminar priprema NATO-ovo zapovjedništvo za specijalne operacije (NSHQ - NATO *Special Operations Headquarters*) s ciljem razvoja međusektorske suradnje i rješenja za borbu protiv hibridnih prijetnji. Kibernetički neovlašteni pristupi i incidenti jedno su od šest područja hibridnih prijetnji. Cilj seminara je međusektorska prezentacija problema, poteškoća, istraživanja i preporuka iz područja hibridnih prijetnji. NATO u suradnji s Ministarstvom obrane Republike Hrvatske radi na pripremama za održavanje Regionalnog seminara ovog tipa planiranog za 2020. godinu.

2.5. 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 Zavoda za sigurnost informacijskih sustava (ZSIS) i CARNET-ovog odjela za Nacionalni CERT. 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 2019. do 30. lipnja 2020. godine Hrvatska je, uz Rumunjsku i Finsku, dio predsjedavajuće trojke CSIRT mreže. Za vrijeme hrvatskog predsjedanja Vijećem EU sastanak CSIRT mreže održat će se u Zagrebu, a tijekom 2019. godine radilo se na pripremama za navedeni sastanak na kojem će sudjelovati oko 80 sudionika.

2.6. MeliCERTes Stakeholder Expert Group

Nacionalni CERT sudjelovao je u radu radne skupine MeliCERTes, oformljene u okviru trogodišnjeg CEF projekta SMART 2015/1089, za razvoj platforme za razmjenu informacija u CSIRT mreži. Platforma za razmjenu informacija o računalno-sigurnosnim incidentima objedinjava skupine alata slobodnog softvera koje većinom koriste europski CSIRT-ovi kako bi se postigla brža razmjena informacija o računalnim prijetnjama i računalno-sigurnosnim incidentima. Tijekom 2019. predstavnici Nacionalnog CERT-a sudjelovali su na sastancima radne skupine na kojima se raspravljalo o trenutnim i budućim potrebama u radu MeliCERTes platforme kroz tri aspekta: tehnički, pravni i potrebna podrška. Nacionalni CERT je sudjelovao u predstavljanju i testiranju razvijenih funkcionalnosti te u pregledu napisanog kôda. U 2019. godini Nacionalni CERT je instalirao MeliCERTes platformu na vlastitoj infrastrukturi te se tako povezao sa zajednicom CSIRT-ova i unaprijedio razmjenu informacija na EU razini.

2.7. DSI Governance Board

Nacionalni CERT aktivno sudjeluje u DSI programu (eng. *Cybersecurity Digital Service Infrastructures*) koji je uspostavljen unutar CEF fondova (eng. *Connecting Europe Facility*). Cilj CEF Cybersecurity DSI Governance Board programa je pružanje podrške CSIRT-ovima zemalja članica Europske unije u povećanju njihovih kapaciteta i suradnji s drugim timovima kroz mehanizme za razmjenu informacija. Mehanizmi za suradnju na operativnoj razini razvijaju se u projektu SMART 2015/1089, a CSIRT-ovi bi ih koristili na dobrovoljnoj bazi kako bi podržali zadatak povjeren CSIRT mreži prema NIS direktivi. Predstavnici Nacionalnog CERT-a sudjelovali su na radnim sastancima.

3 Suradnja i djelovanje Nacionalnog CERT-a na nacionalnoj razini

3.1. Sporazum o poslovnoj suradnji s MUP-om

U 2019. 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.

3.2. Sporazum o poslovnoj suradnji s FER-om

CARNET-ov Odjel za 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. Rezultati suradnje tijekom 2019. godine su: objava 12 dokumenata vezanih uz razne teme iz područja kibernetičke sigurnosti, 12 recenzija sigurnosnih alata i 51 novost o zlonamjernom *ransomware* sadržaju. Materijali se objavljuju na *web* sjedištima www.cert.hr i www.antibot.hr, a namijenjeni su obrazovanju i širenju znanja zainteresirane javnosti iz područja kibernetičke sigurnosti. U okviru poslova vezanih za provjeru sigurnosti računalnih programa, LSS na zahtjev CARNET-a izvršava provjeru sigurnosti računalnih aplikacija.

3.3. Vježba Kibernetički štit 2019

U organizaciji Samostalnog sektora za informacijske i komunikacijske sustave MORH-a te Glavne planske skupine 27. ožujka 2019. godine održana je vježba Koordinacije za sustav domovinske sigurnosti pod nazivom „Kibernetički štit 2019“ u kojoj je CARNET sudjelovao u ulozi igrača. Vježba je okupila članove Koordinacije na čelu s potpredsjednikom Vlade i ministrom obrane Damirom Krstičevićem, a u ulozi promatrača nazočili su i predstavnici drugih institucija. Radilo se o simulacijskoj vježbi temeljenoj na scenariju kibernetičkog napada u kojoj su ključni donositelji odluka na nacionalnoj razini okupljeni u Koordinaciji za sustav domovinske sigurnosti imali mogućnost provjeriti funkcioniranje sustava upravljanja u kriznim situacijama. U odnosu na “Kibernetički štit 2018”, vježba iz 2019. je pokazala kako su, zahvaljujući novom Zakonu o kibernetičkoj sigurnosti, uspostavljene značajne mjere kibernetičke sigurnosti te su prepoznati operatori ključnih usluga, kriteriji za utvrđivanje incidenta koji ima znatan učinak, obveze nadležnih tijela, postupak rješavanja incidenta koji ima znatan učinak te naposljetku i postupak izvješćivanja. Glavni cilj ovogodišnje vježbe bio je podizanje svijesti o kibernetičkoj sigurnosti s posebnim naglaskom na operatore ključnih usluga, davatelje digitalnih usluga, nadležna sektorska tijela te jedinstvenu nacionalnu kontaktnu točku i tijela nadležna za prevenciju i zaštitu od incidenata.

IZVOR: hrvatski-vojnik.hr

3.4. Nacionalna strategija kibernetičke sigurnosti (NSKS)

U 2019. godini Nacionalni CERT nastavio je rad 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. Nacionalni CERT aktivno sudjeluje u radu Nacionalnog vijeća za kibernetičku sigurnost (NVKS) i Operativno-tehničke koordinacije za kibernetičku sigurnost (OTKKS), tijelima osnovanim odlukom Vlade polovicom 2016. godine s ciljem provedbe Nacionalne strategije kibernetičke sigurnosti i Akci-

jskog plana za provedbu Strategije. Sjednice NVKS-a i OTKKS-a održavaju se jednom mjesečno, osim u iznimnim slučajevima ako postoji potreba za sazivanjem izvanrednih sjednica. U 2019. godini sjednice NVKS-a i OTKKS-a održavale su se redovito.

U 2019. godini Nacionalni CERT je aktivno sudjelovao u provedbi mjera iz Akcijskog plana kroz daljnji razvoj međusektorske suradnje nacionalnih regulatornih tijela i tijela odgovornih za područje kibernetičke sigurnosti i politike zaštite podataka te međusobnoj koordinaciji i razmjeni iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira; na ažuriranju Nacionalne taksonomije računalno-sigurnosnih incidenata; definiranju protokola za razmjenu anonimiziranih podataka te uspostavi platforme za razmjenu podataka; izvještavanju dionika unutar sektora o računalno-sigurnosnim incidentima te periodičnom izvještavanju Nacionalnog vijeća za kibernetičku sigurnost o trendovima, stanju i značajnim incidentima iz prethodnog razdoblja; izdavanju upozorenja o sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje; daljnjoj izobrazbi zaposlenika; te na osmišljavanju i provedbi kampanja podizanja svijesti svih korisnika o značaju kibernetičke sigurnosti.

U 2019. godini započelo je prvo ažuriranje Nacionalne strategije kibernetičke sigurnosti i pripadajućeg Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti.

3.5. Zakon i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

Tijekom 2019. 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. Zakon je donesen u srpnju 2018. godine, a proizlazi iz obveza Hrvatske kao članice EU-a za prijenos NIS direktive (Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije) u nacionalno zakonodavstvo. U skladu s navedenim Zakonom i Uredbom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, operatori ključnih usluga i davatelji digitalnih usluga dužni su, bez neopravdane odgode, obavještavati nadležni CSIRT o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. 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. Nakon što su 2018. godine nadležni CSIRT-ovi (Zavod za sigurnost informacijskih sustava i Nacionalni CERT) donijeli Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga, u listopadu 2019. godine izdali su dokument "Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti". Radi se o neobvezujućoj preporuci koju su navedena dva tijela izdala kao tehnička tijela za ocjenu sukladnosti prema Zakonu. Dokument služi kao implementacijski vodič za operatore ključnih usluga prilikom ostvarivanja sukladnosti s mjerama

sigurnosti propisanim u drugom dijelu Uredbe, ali istodobno i kao vodič za nadležna sektorska tijela, tehnička tijela za ocjenu sukladnosti, vanjske i interne revizore koji će provoditi nadzor ili ocjenjivanje sukladnosti kod operatora ključnih usluga o čemu se sve informacije mogu pronaći na web sjedištu www.cert.hr pod kategorijom „Prijava incidenta prema ZKS-u".

3.6. Suradnja s Hrvatskom udrugom banaka

Nacionalni CERT od 2019. godine sudjeluje 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

3.7. Djelovanje putem javnih medija i obraćanja javnosti

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

- 2/2019 – sudjelovanje u emisiji HRT-a "Dobro jutro Hrvatska" na temu "Dan sigurnijeg interneta
- 2/2019 - održan webinar za dan sigurnijeg interneta na temu "Važnost edukacije o kibernetičkoj sigurnosti"
- 2/2019 - sudjelovanje u emisiji "Pametna ploča" Radio Sljemena na temu "Dan sigurnijeg interneta"
- 2/2019 - započela nacionalna kampanja podizanja svijesti o kibernetičkoj sigurnosti "Veliki hrvatski naivci"
- 3/2019 - održane četiri radionice u sklopu projekta GrowCERT s ciljem podizanja svijesti o kibernetičkoj sigurnosti – dvije za akademsku zajednicu i dvije za poslovni sektor
- 3/2019 - "Veliki hrvatski naivci" koji su nastali u suradnji agencije Señor i CARNET-a osvojili zlato i broncu na Nacionalnom kreativnom natjecanju IdejaX
- 3/2019 - sudjelovanje u programu obilježavanja Svjetskog dana prava potrošača pod nazivom "Pametno s pametnim tehnologijama - Zaštita potrošača u digitalnom svijetu"
- 4/2019 - gostovanje u emisiji "Potrošački kod" HRT-a vezano uz prijevare na internetu
- 9/2019 - sudjelovanje na IV. Školi modernih tehnologija s predavanjem "#SurfajSigurnije"
- 10/2019 - obilježen Europski mjesec kibernetičke sigurnosti: kibernetička riječ dana putem Facebook profila te su održane dvije radionice za akademsku zajednicu

- 10/2019 - održano predavanje u Vrbovcu u sklopu 13. tjedna cjeloživotnog učenja pod nazivom "#SurfajSigurnije"
- 10/2019 - sudjelovanje na okruglom stolu na konferenciji "CSC2019 - Cyber Security Conference" u Osijeku po temi "Zakon o kibernetičkoj sigurnosti – iskustva i izazovi"
- 10/2019 - sudjelovanje na konferenciji "Dan korporativne sigurnosti" u Erste banci na temu novijih prijetnji i APT napada
- 10/2019 - sudjelovanje na okruglom stolu Hrvatskih dana sigurnosti Hrvatske udruge menadžera u sigurnosti
- 11/2019 - održana radionica za podizanje svijesti o kibernetičkoj sigurnosti na konferenciji CUC2019 pod nazivom "#SurfajSigurnije"
- 10/2019 - reportaža s konferencije MUP-a u povodu Europskog mjeseca kibernetičke sigurnosti
- 10/2019 - gostovanje u emisiji "Tema dana" HRT-a u sklopu Europskog mjeseca kibernetičke sigurnosti
- 11/2019 - sudjelovanje na konferenciji KOM2019 s predavanjem "Mreža europskih i nacionalnih sigurnosnih sustava – CERT-a"
- 11/2019 - predavanje povodom Mjeseca borbe protiv ovisnosti pod nazivom Moderne tehnologije – Izazovi za mlade u organizaciji Društva za socijalnu podršku
- Informiranje javnosti putem web sjedišta Nacionalnog CERT-a (www.cert.hr) – 289 947 posjetitelja u 2019. godini
- Podizanje svijesti korisnika o ugrozama na internetu putem edukativno informativnog portala u sklopu kampanje "Veliki hrvatski naivci" (www.naivci.hr) - 24 647 posjetitelja u 2019. godini
- Informiranje javnosti putem društvenih mreža Facebook (@CERT.hr - 1356 pratitelja) i Twitter (@ HRCERT – 969 pratitelja)
- Održan niz intervjua za časopise te tiskane i digitalne medije, npr. Poslovni lider, 24 sata, Indeks, Večernji list, Jutarnji list, T-portal
- Izdane tiskane brošure "SurfajSigurnije", letak za poslovne korisnike i letak za akademsku zajednicu
- Izdana digitalna izdanja brošura "Surfaj sigurnije na društvenim mrežama" i "Mali pojmovnik kibernetičke sigurnosti"

4 Projekti

4.1. GrowCERT

Nacionalni CERT i CARNET, potaknuti ostvarivanjem ciljeva Nacionalne strategije kibernetičke sigurnosti, 2019. godine zaključili su dvogodišnji projekt pod nazivom GrowCERT – Jačanje kapaciteta Nacionalnog CERT-a i poboljšanje suradnje na nacionalnoj i europskoj razini. Projekt u vrijednosti od gotovo 985 000 eura bio je sufinanciran sredstvima Europske unije putem Instrumenta za povezivanje Europe (*CEF – Connecting Europe Facility*). Projekt je doprinio jačanju nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o kibernetičkim incidentima i prijetnjama kibernetičkoj sigurnosti korištenjem novorazvijene platforme za prikupljanje podataka o sigurnosnim incidentima na nacionalnoj i europskoj razini. Ovim projektom željela se podići svijest opće populacije o kibernetičkim prijetnjama i primjerenim odgovorima na njih putem kampanje pod nazivom "Veliki hrvatski naivci" u kojoj je tijekom prve polovice 2019. godine proveden je niz marketinških i medijskih aktivnosti. U istom razdoblju organizirane su četiri radionice o kibernetičkoj sigurnosti za poslovni sektor i akademsku zajednicu. Projektom je omogućeno dodatno ulaganje u ljudske i tehničke kapacitete Nacionalnog CERT-a. Tijekom projekta Nacionalni CERT je razvio nove usluge: DNSBL sustav za blokiranje neželjene pošte (eng. *spam*), CVE *search* - sustav za distribuciju informacija o otkrivenim ranjivostima i alat za otkrivanje izmijenjenih izgleda stranica *web* sjedišta (eng. *web defacement*) te drugih zlonamjernih sadržaja u kibernetičkom prostoru u ovlasti Nacionalnog CERT-a. Razvijena je platforma PiXi za prikupljanje, analizu i razmjenu podataka o sigurnosnim incidentima i prijetnjama. U tom procesu sudjelovala je stručna radna skupina sastavljena od predstavnika različitih sektora (MORH, MUP, HANFA, HNB, HAKOM, Hrvatska udruga banaka, Zavod za sigurnost informacijskih sustava i akademska zajednica). Projekt je završio 30. lipnja 2019. godine te su rezultati projekta predstavljeni nacionalnoj, europskoj i međunarodnoj sigurnosnoj zajednici na brojnim konferencijama i sastancima.

grow-cert

U okviru kampanje "Veliki hrvatski naivci" izrađena je web stranica dostupna na www.naivci.hr

4.2. Grow2CERT

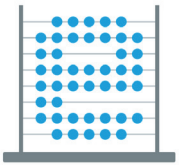
Nacionalni CERT je u studenom započeo s provedbom novog projekta sufinanciranog sredstvima Europske unije putem Instrumenta za povezivanje Europe (eng. *CEF – Connecting Europe Facility*) pod nazivom Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti (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 će se proširiti 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 će nastaviti 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. Posebno će se usmjeriti na „kibernetičku higijenu", odnosno održavanje visoke razine sigurnosti korisnika interneta uz odgovorno korištenje suvremenih informacijsko-komunikacijskih tehnologija. Opseg projekta čini osam različitih aktivnosti. Uz upravljanje projektom i komunikaciju i vidljivost, ostale aktivnosti odnose se na nadogradnju nacionalne platforme PiXi 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, organizacija sastanka CSIRT mreže u sklopu predsjedanja Hrvatske Vijećem Europske unije 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

4.3. e-Škole

U 2019. godini CARNET-ov odjel za Nacionalni CERT provodio je pripremne aktivnosti za projekt "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 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. Također će se provesti aktivnosti edu-

kacije s ciljem podizanja svijesti i aktivnog prenošenja znanja o kibernetičkoj higijeni, prepoznavanju kibernetičkih prijetnji i primjerenim odgovorom na moguću pojavu kibernetičkog incidenta, kao i istraživačke aktivnosti u cilju poboljšavanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola.



e-Škole

4.4. 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. Projekt podržava i MeliCERTes platformu te Centre za sigurniji internet. 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.

5 Stanje računalnih incidenata i statistike

5.1. Nacionalna taksonomija računalno-sigurnosnih incidenata

U 2019. godini ažurirana je "Nacionalna taksonomija računalno-sigurnosnih incidenata" koja je nastala godinu ranije kao jedna od mjera iz Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti. Razlog za ovako brzo ažuriranje je pojava novih prijetnji, kao i izmjene u nacionalnom zakonodavstvu.

Tako je na primjer uvedena potkategorija "Ispad usluge" koja se odnosi isključivo na dionike Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Od većih izmjena dodana je i kategorija "Zlonamjerno rudarenje kriptovalute (eng. *Cryptojacking*) koja se odnosi na neovlašteno korištenje CPU resursa korisničkog računala bez korisnikova znanja.

Ostale izmjene odnose se na manje promjene, uglavnom preciznije definiranje potkategorija incidenata. Kao i prva verzija, ažurirana taksonomija je rezultat suradnje Zavoda za sigurnost informacijskih sustava (ZSIS) i Nacionalnog CERT-a, a pri realizaciji podršku je pružila radna skupina sastavljena od predstavnika tijela različitih sektora, HAKOM-a, HNB-a, MORH-a, MUP-a, HANFA-e te stručnjaka s FER-a.

"Nacionalna taksonomija računalno-sigurnosnih incidenata" važna je jer daje definiciju pojma računalno-sigurnosnog incidenta te nudi ujednačene kriterije pri klasifikaciji računalno-sigurnosnih incidenata na nacionalnoj razini u svojim informacijskim sustavima i računalnim mrežama, a njome želimo stvoriti preduvjete da sva tijela i institucije koje će razmjenjivati informacije o računalno-sigurnosnim događajima to čine tako da su svim sudionicima u toj razmjeni u potpunosti jasni i kontekst i detalji o pojedinom događaju ili incidentu.

Važno je napomenuti i kako je navedena taksonomija „živi" dokument koji će se, u suradnji sa ZSIS-om i radnom skupinom, i dalje mijenjati ovisno o potrebama.

5.2. Statistika o obrađenim incidentima

Nacionalni CERT je tijekom 2019. godine zaprimio i obradio ukupno 1129 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a.

Vodeći tipovi incidenata su ***phishing***, ***phishing URL*** i ***web defacement*** (kompromitirano web sjedište s izmijenjenim izgledom ili sadržajem web stranice).

Najznačajnija promjena u odnosu na prošlu godinu je općenito velik broj prijavljenih incidenata. **U odnosu na 2018. godinu Nacionalni CERT obradio je 65% incidenata više**. To se, između ostalog, može pripisati i uspješno provedenoj kampanji "Veliki hrvatski naivci" u kojoj se prosječni korisnik interneta u Hrvatskoj bolje upoznao s djelovanjem Nacionalnog CERT-a kojem se mogu prijaviti računalno-sigurnosni incidenti. Osim toga, održano je nekoliko radionica s naglaskom na akademsku zajednicu i poslovni sektor, što je rezultiralo većim brojem individualnih prijava incidenata.

Velika promjena odnosi se i na pad broja web defacement incidenata koji je u 2019. godini pao na 3. mjesto.

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 8,5%.

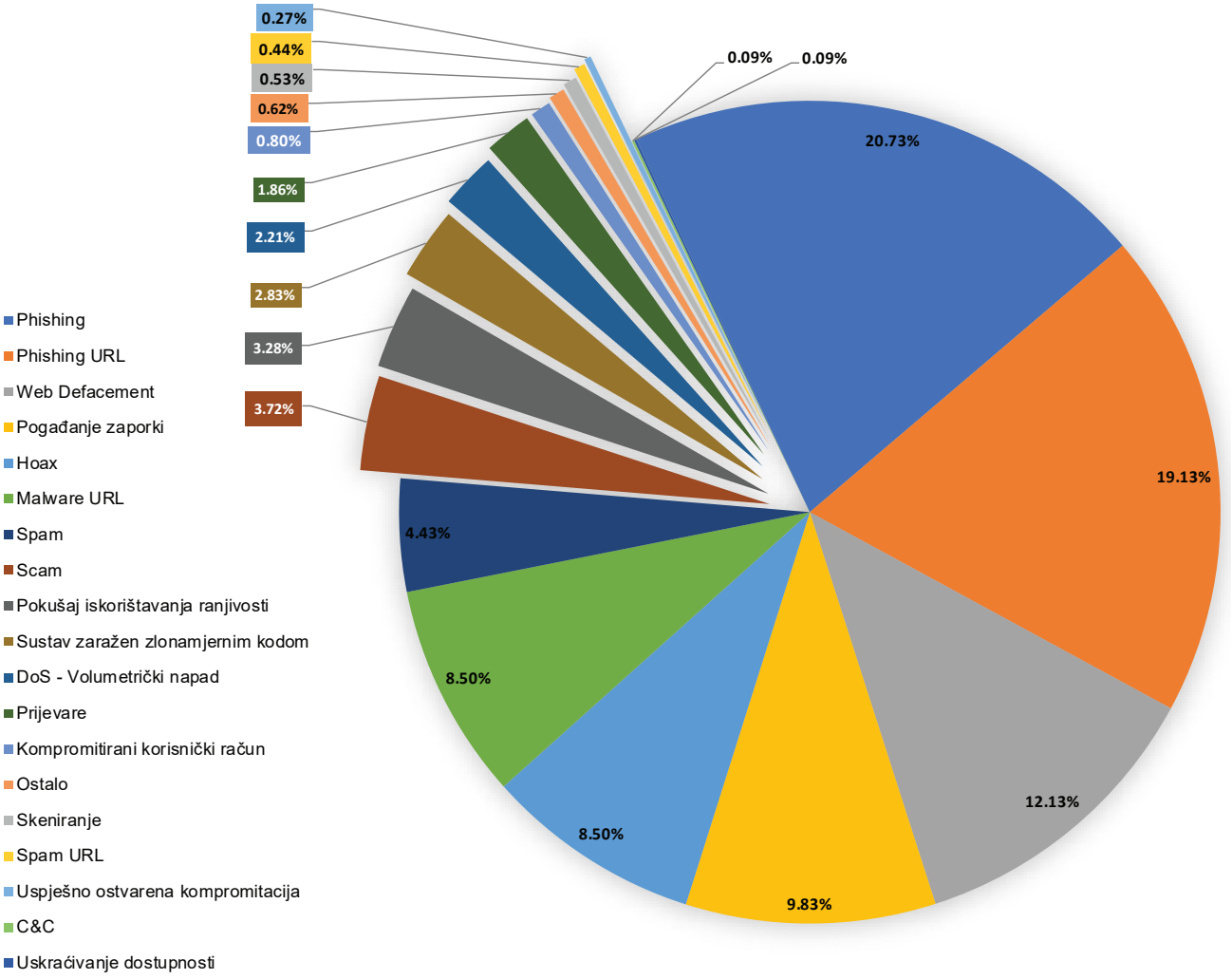
TIP INCIDENTA	BROJ	TREND
Phishing	234	▲
Phishing URL	216	▲
Web Defacement	137	▼
Pogađanje zaporki	111	▲
Hoax	96	▲
Malware URL	96	▲
Spam	50	▲
Scam	42	–
Pokušaj iskorištavanja ranjivosti	37	▲
Sustav zaražen zlonamjernim kodom	32	▲
DoS - Volumetrički napad	25	▲
Prijevare	21	▼
Kompromitirani korisnički račun	9	▲
Ostalo	7	▼
Skeniranje	6	–
Spam URL	5	▲
Uspješno ostvarena kompromitacija	3	–
C&C	1	▼
Uskraćivanje dostupnosti	1	–
UKUPNO	1129	▲

Prikaz incidenata po tipu u 2019. godini

5.3. Raspodjela incidenata po tipu

Sljedeći grafikoni prikazuju omjere incidenata po tipu u 2019. godini, koji su zabilježeni u sustavu za obradu incidenata.

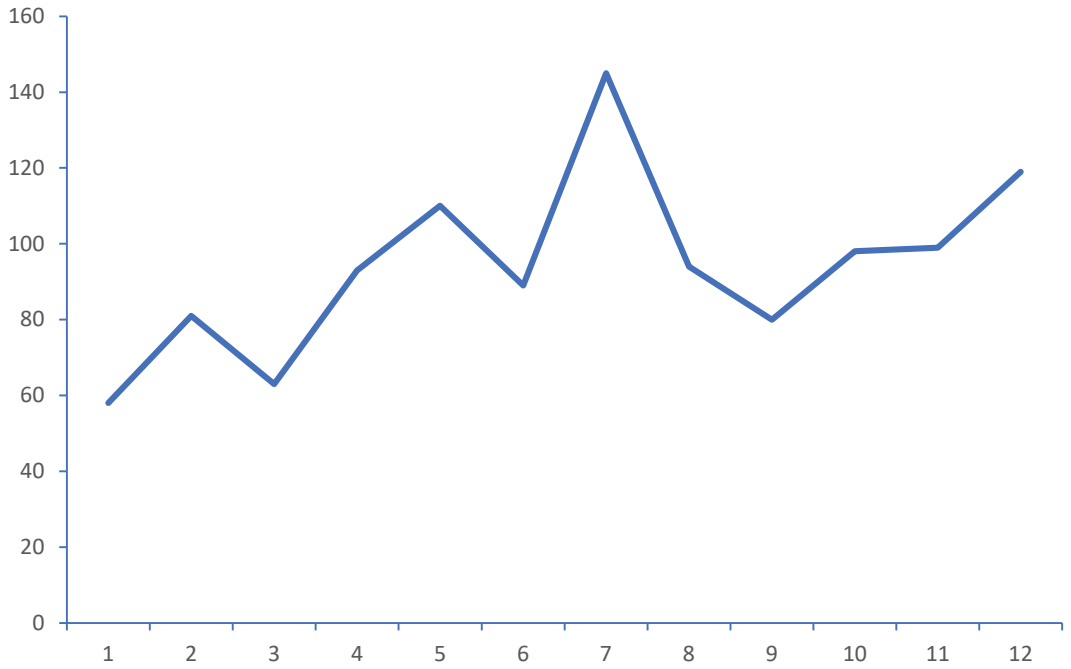
Incidenti su se prijavljivali putem e-mail adrese incident@cert.hr ili su prijave dobivene od vanjskih izvora kroz automatizirane softvere za obradu incidenata.



Raspodjela incidenata po tipu u 2019. godini

5.4. Trendovi pojava incidenata na poslužiteljima u 2019. godini

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



Broj incidenata koje je 2019. godine obradio Nacionalni CERT s prikazom po mjesecima

5.5. Registrirani *botovi* u Republici Hrvatskoj

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 internetskih stranica (*hosting provider*). Iz grafikona koji prikazuje godišnji trend broja *botova* vidljivo je da u Hrvatskoj broj registriranih zaraženih računala raste i više ih je u odnosu na prethodnu godinu. Broj otkrivenih *botova* prikazan ovim statistikama temelji se na vanjskim izvorima koji dostavljaju podatke Nacionalnom CERT-u i ne daje stvarni broj zaraženih korisničkih računala, no prikazuje trend i okvir stvarnog stanja.

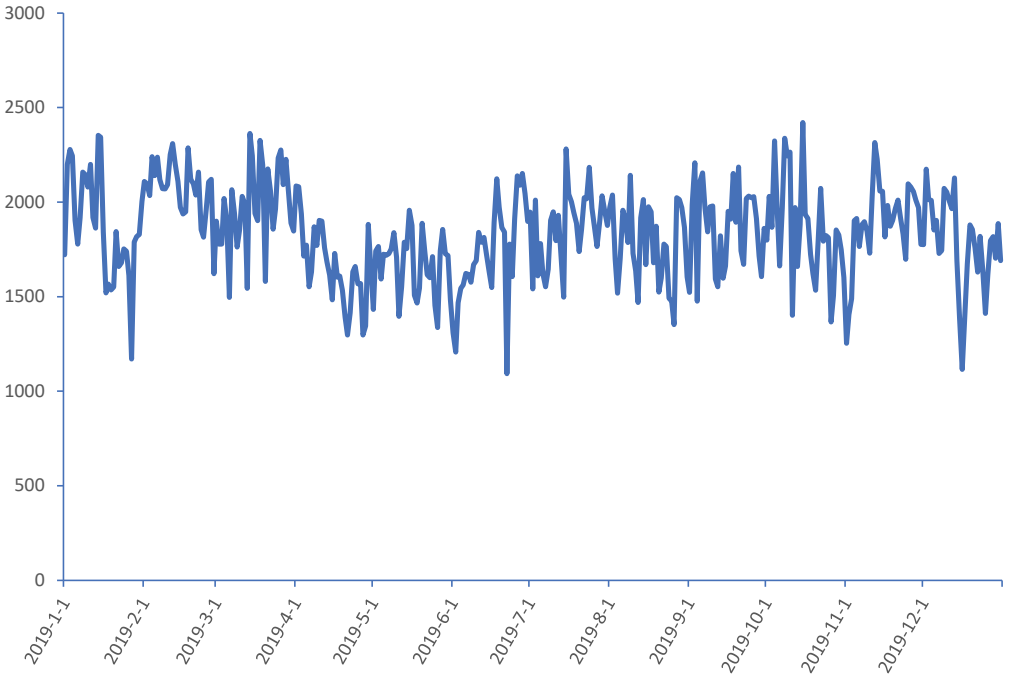
U tablici u nastavku prikazano je deset najčešće prijavljivanih *botova* prema tipu (vrsti zlonamjernog sadržaja) kroz 2019. godinu, koji su bili diseminirani davateljima usluge pristupa internetu.

andromeda	279 229
conficker	105 614
gamut	81 687
necurs	58 378
extortion	21 817
sality	20 986
mirai	16 583
malware-generic	11 287
stealrat	8 619
wrokni	8 144

Top 10 botova prema tipu u 2019. godini

Suma zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2019. godine iznosi 669 902, što je smanjenje od 10% u odnosu na 2018. godinu. Smanjenju broja *botova* pridonijela je nadogradnja izvora iz kojih se povlače podaci. Tom nadogradnjom postiglo se prepoznavanje istih "obitelji" zlonamjernog sadržaja (eng. *malware family*). Zlonamjerni sadržaj iz iste obitelji automatizirano se mapira, što rezultira "čišćom" slikom zlonamjernog sadržaja, odnosno sprječavanje pojave udvostručenih podataka.

Broj zabilježenih *botova* po danima u 2019. godini prikazan je u nastavku. Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću ispod 2000 *botova* dnevno, što nije bio slučaj prošle godine.



Godišnji trend broja botova - Srednja vrijednost broja botova po danu za 2019. godinu iznosila je 1.835,35 što je nešto manje od 200 botova u odnosu na 2018. godinu.

6 Značajniji incidenti, otkrivene ranjivosti i događaji

1. kvartal

- Početak godine obilježila su kaznena djela prijevare putem Facebook-a. Na stranicama Policijske uprave bjelovarsko-bilogorske objavljeno je upozorenje u kojem se korisnike poziva na oprez pri korištenju društvenih mreža. U šest mjeseci ova je Policijska uprava zabilježila dva slučaja prijevare ženskih osoba starosti oko 60 godina koje su uplatile veću svotu novaca nepoznatim počiniteljima koji su se lažno predstavljali na Facebook-u. Policijska uprava pozvala je građane da budu oprezni kod prihvaćanja prijatelja na Facebook-u jer je lažne profile vrlo lako napraviti, a posebice da ne nasjedaju na ovakve ili slične načine prijevara putem društvenih mreža.
- Početkom siječnja objavljena je vijest o curenju privatnih podataka njemačkih političara te se pokazalo koliko su ovakvi napadi opasni. Podaci su objavljivani na Twitter računu kojeg je pratilo nešto manje od 20 000 ljudi, no incident je dobio na značaju u trenutku kada su informacije prikupljene napadom objavljene na puno popularnijem Twitter računu koji je prethodno i probijen. Društvo snažno brine o pitanjima vezanima uz privatnost i nadzor, ali valja se zapitati na koji način kibernetički napadi utječu na vlade, političare i tvrtke. Iako se za napad na njemačke političare može reći kako je blizak vandalizmu, ostavio je traga na žrtvama.
- Sredinom siječnja zabilježena je *phishing* kampanja usmjerena na korisnike internet bankarstva jedne poznatije banke. Korisnici su zaprimali *phishing* e-mail koji je sadržavao poveznicu na lažnu stranicu internet bankarstva s ciljem prikupljanja osobnih podataka korisnika. Ubrzo nakon slanja prijava CERT-u države u kojoj je bila smještena stranica ista je uklonjena.
- Sredinom siječnja iz baze NASA-ine *web* aplikacije iscurili su podaci zaposlenika kao što su korisnička imena, imena i prezimena, adrese elektroničke pošte te imena projekata. Za curenje podataka zaslužna je jedna od inačica alata Jira, *web* aplikacije koju tvrtke koriste za praćenje promjena u projektima. U izvještaju Avinasha Jaina, sigurnosnog stručnjaka koji je otkrio curenje podataka, stoji kako je do greške u radu sustava došlo zbog krivo podešenih postavki vidljivosti. Ovaj je problem već dobro poznat, a temelji se na razlikovanju pojmova "Everyone" i "All users". Naime, pojam "Everyone" omogućava svim korisnicima interneta pristup povjerljivim podacima te Jain vjeruje kako je nesporazum oko ova dva pojma zaslužan za curenje podataka.
- Siječanj je bio težak mjesec i za Facebook. Naime, objavljeni su dokumenti koji su dio tužbe koja je podignuta protiv Facebooka 2012. godine. Ovaj je tehnološki div redovito dopuštao djeci da, bez

- znanja roditelja, kupuju online pogodnosti za igre na njihovoj platformi. Ovakvo što je moguće jer Facebook ne iziskuje od korisnika ponovnu prijavu svaki put kada želi kupiti neku virtualnu valutu. Iako su tada bila dostupna samo četiri dokumenta, Facebooku je naređeno da objavi još stotinjak stranica koje će dati više informacija o samoj tužbi.
- Krajem siječnja zabilježena je veća *phishing* kampanja usmjerena prema hrvatskim korisnicima. Korisnici su primali *CEO fraud* elektroničke poruke sa zlonamjernim privitkom (.iso ekstenzija) slane u ime jedne poznate hrvatske tvrtke (polje pošiljatelja i potpis su lažirani). Nacionalni CERT je iz dao upozorenje na web stranici i društvenim mrežama te poslao prijavu stranom operateru s čijeg poslužitelja su dolazile *phishing* poruke.
- Početak 2019. godine također je obilježila objava 2.2 milijarde korisničkih oznaka s lozinkama na javno dostupnim stranicama poput *torrenta* i hakerskih foruma. Podaci su prikupljeni iz raznih prethodnih curenja podataka poput Dropbox-a i LinkedIn-a. Sigurnosni stručnjak Troy Hunt identi-ficirao je prvi dio ove "mega" baze nazvane "*Collection #1*", a koju je objavio anonimni korisnik. Prema Huntu, ova je baza sadržavala 773 milijuna jedinstvenih korisničkih oznaka i lozinki. Međutim, sigurnosni su stručnjaci analizirali novu bazu podataka koja je nazvana "*Collections #2-5*", a koja sadrži 25 milijardi zapisa u 845 gigabajta. Ovi podaci se najviše koriste za slanje *phishing* i *hoax* poruka korisnicima te je važna svijest o ovakvim u-grozama kako bi se na vrijeme prepoznale.
- Kao dar za Valentinovo korisnici aplikacije za online upoznavanje *Coffee Meets Bagel* dobili su službenu obavijest o curenju njihovih podataka (adrese e-pošte i imena korisnika). Podaci su dio kompilacije prikupljenih korisničkih podataka koji su se prodavali na kriminalnim mjestima za trgovinu. U poruci e-pošte, koja sadrži obavijest o curenju korisničkih podataka, navodi se kako se radi o 6 milijuna korisničkih imena i adresa e-pošte, no kako nisu iscurile korisničke lozinke ni financijske informacije pošto se to ne pohranjuje unutar aplikacije.

2. kvartal

- Drugi kvartal 2019. godine bio je obilježen kibernetičkim napadima na korisnike u Hrvatskoj. Početkom travnja zabilježena je *phishing* kampanja koja je ciljala korisnike Hrvatske pošte. *Phishing* poruka je sadržavala poveznicu do lažne stranice sa zlonamjernim sadržajem. Nacionalni CERT poslao je prijavu stranom operateru preko čijeg je *mail* poslužitelja distribuirana *phishing* poruka. Poslana je prijava i registraru domene te pružatelju usluge udomljavanja *web* stranica preko koje se širio zlonamjerni sadržaj putem SMB protokola. Zlonamjerni sadržaj je uklonjen.
- Početkom travnja otkrivena je ranjivost MikroTik usmjerivača koje napadači koriste za čitanje korisničkih imena i lozinki administratorskih računa i za širenje zlonamjernog softvera za rudarenje kriptovaluta. Bilo je potencijalno ugroženih korisnika iz hrvatskog IP adresnog prostora te je Nacionalni CERT poslao prijave pružateljima internet usluge (*ISP - Internet Service Provider*) kako bi mogli poduzeti korake za sprječavanje iskorištavanja ranjivosti.
- Krajem travnja detektirana je zloupotreba javno dostupne *Cisco Smart Install* funkcionalnosti na preklopniku *Cisco Catalyst 3560* koja je za posljedicu imala neovlašteni upad u mrežu. Nacionalni CERT je poslao obavijest svim ISP-ovima koji imaju navedeni uređaj te ih savjetovao da onemoguće *Smart Install* funkcionalnost korištenjem "*no vstack*" naredbe u konfiguraciji samog preklopnika ili da se ograniči za interne potrebe.
- Nisu sve vijesti bile loše, početkom svibnja Europol je objavio da je ugasio dvije popularne trgovine na *dark web-u*, *Wall Street Market* i *Silkkitie* (poznata još i kao *Valhalla*). Gašenje je dio simultane

- globalne operacije usmjerene protiv internetskih *Dark web* stranica putem kojih se trguje drogom, ukradenim kreditnim karticama, zlonamjernim sadržajem i sličnim protuzakonitim dobrima. Policija je u zapadnoj Njemačkoj uhitila troje ljudi koji su navodno upravljali stranicom *Wall Street Market*, drugom najvećom internetskom *Dark web* trgovinom koja je imala više od milijun korisnika i 5 400 prodavača. Uz navedeno, operacija je uključivala i Europol, nizozemsku policiju te FBI, a u sklopu nje su uhićena i dva značajna dobavljača droge u Los Angelesu.
- Sredinom svibnja otkrivena je lažna stranica koja promovira alat za čuvanje lozinki (*password manager*), a zapravo širi zlonamjerni sadržaj. Stranica je dio veće mreže stranica koje dijele reklamni ili oglašivački softver kojeg predstavljaju kao besplatni alat. Mnogi korisnici reklamni ili oglašivački softver smatraju manjom prijetnjom od drugog zlonamjernog sadržaja. Mnogi reklamni ili oglašivački softveri sadrže trojance koji prikupljaju lozinke, alate za zlonamjerno rudarenje kriptovaluta, zlonamjerne *ransomware* sadržaje te sličan zlonamjerni sadržaj. Reklamni ili oglašivački softver se najčešće širi putem lažnih stranica koje se doimaju kao da šire legitiman sadržaj.
- Krajem svibnja otkriveno je kako su iz popularne društvene mreže Instagram četiri mjeseca curile informacije o korisnicima poput brojeva telefona i adresa elektroničke pošte. Kako navodi sigurnosni stručnjak David Stier, izvorni kod je omogućavao uvid u korisničke podatke prilikom svakog otvaranja stranice u pregledniku. Podaci koji su iscurili sadržavali su kontakt informacije tisuće korisničkih računa koji su pripadali više skupina korisnika, od privatnih do poslovnih. Propust je omogućio zlonamjernim korisnicima prikupljanje podataka s Instagrama što im je omogućilo stvaranje virtualnih imenika s detaljnim podacima tisuća korisnika Instagrama.
- Početkom lipnja zabilježen je povećan broj lažnih ucjenjivačkih poruka kojima napadač pokušava iznuditi novčanu dobit od žrtve. Gotovo uvijek u tekstu poruke ucjenjivač spominje posjedovanje žrtvine kompromitirane lozinke nekog internetskog servisa. Također, navodi da posjeduje snimke s web kamere žrtvinog računala kojoj je pristupio dok je žrtva navodno pregledavala web stranice pornografskog sadržaja. Pri tome prijeti objavom navodne "ponižavajuće" video snimke svim žrtvinim kontaktima koje je prikupio s Facebooka i e-maila. Premda se može dogoditi da poruka sadrži lozinku koju možda koristite ili ste koristili, to je vjerojatno zbog činjenice da postoje određeni servisi s bazom kompromitiranih lozinki.
- Krajem lipnja sigurnosni stručnjaci iz tvrtke ESET upozorili su korisnike na novu prevaru koja kruži popularnom aplikacijom za dopisivanje WhatsApp. Korisnici su počeli dobivati poruke u kojima stoje da im se, u sklopu desete obljetnice postojanja aplikacije, nudi posebna pogodnost. Točnije, u poruci stoji kako će svi korisnici koji odluče sudjelovati u promociji dobiti 1 TB besplatnog internetskog prometa. Kako bi ostvarili ovu "pogodnost", korisnici moraju pristupiti posebnoj poveznici, odgovoriti na par pitanja i poslati tu istu poruku na adrese 30 kontakata. Stručnjaci iz ESET-a smatraju kako je krajnji cilj napadača širenje reklamnog sadržaja bez pristanka korisnika što im je, na koncu, i uspjelo. Analiza je pokazala kako poveznica vodi do napadača koji su više puta sličnim metodama provodili phishing kampanju. Štoviše, napadači su putem iste domene pokrenuli više od 66 različitih kampanja, a posebnu je pažnju izazvala činjenica kako su se predstavljali kao poznati svjetski brendovi kao što su Adidas, Rolex i ostali.

3. kvartal

- Početkom srpnja aviokompanija *British Airways* dobila je kaznu od 183 milijuna funti zbog kršenje GDPR-a, odnosno curenja podataka koje im se dogodilo 2018. godine. Time je aviokompaniji *Britain's Information Commissioner's* Office (ICO) izdao najveću kaznu koja je do sada izdana zbog kršenja GDPR-a, i to zato što nisu uspjeli zaštititi osobne podatke od oko 500 000 korisnika za vrijeme curenja podataka. British Airways otkrila je osobne informacije i brojeve kreditnih kartica 380 000 korisnika u curenju podataka koje je trajalo više od dva tjedna. U vrijeme curenja podataka 2018. godine aviokompanija je potvrdila da su ukradeni podaci korisnika koji su svoje aviokarte kupovali online putem njihove službene stranice ba.com ili *British Airways* mobilne aplikacije između 21. kolovoza i 5. rujna. Kibernetički napad povezan je s hakerskom skupinom *Magecart*, jednom od najzloglasnijih hakerskih skupina specijaliziranih za krađu podataka o kreditnim karticama s web stranica koje nemaju visoku razinu sigurnosti.
- 6. srpnja još jedna gradska uprava u Sjedinjenim Američkim Državama je pokleknula pod kibernetičkim napadima i platila 130 000 američkih dolara kako bi povratila podatke koje je izgubila u napadu zlonamjernim *ransomware* sadržajem. Napad je primijećen prije no što se proširio na sva računala povezana s mrežom, no unatoč brzom djelovanju nešto manje od 7% prijenosnih računala je zaraženo, a napad je prouzročio gašenje dviju domena. Štoviše, *The News Dispatch* navodi kako službene adrese elektroničke pošte i službena internetska stranica gradske uprave nisu bile dostupne čak puna tri dana. Iako su se akciji spašavanja podataka priključile sigurnosne tvrtke i FBI, svi pokušaji su rezultirali neuspjehom te je na kraju isplaćena jamčevina koju su napadači tražili.
- Tvrtka koja surađuje sa Saveznom sigurnosnom službom Ruske Federacije (FSB) je bila žrtva hakerskog napada u sklopu kojega su objavljene informacije o tajnim projektima koji su razvijani za ovu sigurnosnu službu. Među objavljenim podacima posebno se ističu projekti kojima se želi otkriti identitet korisnika Tor mreže, prikupljati podatke o korisnicima društvenih mreža, ali nastojanja da se ruski dio interneta odvoji od ostatka svijeta. Prema navodima, tvrtku *Sytech* je 13. srpnja napala hakerska skupina *0v1ru$* koja je u sklopu napada na službene stranice tvrtke postavila sliku "*Yoba-face*", a presliku ekrana je objavila putem svojeg profila na društvenoj mreži Twitter kako bi dokazali da su ostvarili pristup poslužiteljima. *BBC Russia* navodi kako je u sklopu napada ukradeno gotovo 7,5 TB podataka koji otkrivaju informacije o nizu tajnih projekata koje je za potrebe FSB-a razvijala tvrtka *Sytech*. Ukradeni podaci su potom proslijeđeni hakerskoj skupini *DigitalRevolution* koja ih je poslala ruskim medijima.
- Krajem srpnja sigurnosni stručnjaci iz tvrtke *Data Group* otkrili su ranjivost u poslužiteljima koju su napadači iskoristili kako bi ostvarili pristup do podataka korisnika više lokalnih banaka u Brazilu. Iscurilo je oko 250 GB podataka vezanih uz korisnike više banaka, iako brazilska internetska stranica *The Hack*, koja je prva prenijela informacije o incidentu, navodi kako je najveći dio podataka vezan uz lokalnu tvrtku *Banco Pan* koja se nalazi u gradu Fortalezi u pokrajini Ceará. Podaci uključuju skenirane dokumente poput osobnih iskaznica

- te dokumenata koji su sadržavali adresu te niz povjerljivih podataka korisnika. Tvrtka *Banco Pan* se odmah ogradila od incidenta navodeći kako je njihov sustav siguran te da je za curenje podataka odgovorna partnerska tvrtka koja nudi usluge kredita za umirovljenike. U prilog ovoj tvrdnji ide činjenica kako su curenjem podataka pogođeni najviše korisnici ove starosne skupine.
- Sredinom kolovoza sigurnosni stručnjaci iz *Microsofta* otkrili su neobičnu *phishing* kampanju koja koristi "*error 404*" web stranice kako bi naveli korisnike na odavanje informacija o svojim Microsoft korisničkim računima. Kako bi izveli takvu prevaru, napadači registriraju domenu i umjesto da kreiraju pojedinu *phishing* stranicu na koje će preusmjeriti potencijalne žrtve, konfiguriraju "404" stranicu koja prikazuje lažnu login formu. To im omogućava neograničen broj *phishing* URL-ova sa samo jednom registriranom domenom. 404 stranice koje napadači koriste kako bi masovno prikupljali korisničke podatke su vrlo dobro prikrivene i djeluju kao legitimne *Microsoftove login forme*. *Phishing* forma kreirana je tako da prikuplja e-mail adrese, brojeve telefona i *Skype* korisnička imena, a kako korisnici ne bi posumnjali u legitimnost, nakon što prikupe željene podatke napadači preusmjere korisnika na Microsoftove legitimne stranice zamaskirane skraćenim URL-om.
- 23. kolovoza pružatelj usluge udomljavanja internet stranica (eng. *hosting provider*) *Hostinger* obavijestio je 14 milijuna svojih korisnika kako im je resetirao lozinke za prijavu nakon što je došlo do incidenta koji je zlonamjernim korisnicima omogućio pristup do baze podataka korisnika. *Hostinger* je pokrenuo resetiranje lozinki kako bi zaštitio svoje korisnike te je svima poslao upute kako da ponovno ostvare pristup svojim korisničkim računima. Iz *Hostingera* navode kako financijski podaci i sadržaj samih stranica nisu bili pogođeni, a posebno su istakli činjenicu kako se plaćanje vrši putem vanjskih tvrtki.
- Početkom rujna stranica koja se predstavlja kao službena stranica internetske usluge *PayPal* korisnike je navodila na preuzimanje nove inačice *Nemty* zlonamjernog *ransomware* sadržaja, a prema dostupnim informacijama napadači su se služili s više različitih kanala kako bi ga proširili. Specifično je kod ovog slučaja da se uz činjenicu kako se stranica doima kao legitimna stranica usluge *PayPal*, žrtvi jamči povrat novca u iznosu od tri do pet posto za svaku obavljenu transakciju. Sam dizajn stranice je odrađen na visokoj razini te je gotovo u potpunosti preslika legitimne stranice usluge *PayPal*. Što se samog zlonamjernog *ransomware* sadržaja *Nemty* tiče, on je već neko vrijeme prisutan, ali je u središte pozornosti stručnjaka za kibernetičku sigurnost došao tek u kolovozu 2019. godine, nakon što je Vitali Kremez objavio njegovu detaljnu analizu.
- Početak nove školske godine obilježila je velika *phishing* kampanja usmjerena na škole i obrazovne ustanove s ciljem kompromitacije korisničkih računa. Pošiljatelj lažne (*phishing*) poruke elektroničke pošte predstavlja se kao "Centar za pomoć e-poštom", a u poruci stoji upozorenje o premašenoj kvoti pohrane. Tijekom kampanje nekoliko korisničkih računa je uspješno kompromitirano te su iskorišteni za daljnje širenje *phishing* poruka. *Phishing* poruke sadržavale su umetnuti *phishing* URL za krađu osobnih podataka koji se često izmjenjivao. Nacionalni CERT je stranim operaterima prijavio svaki URL koji su po prijavi ubrzo i uklonjeni. Osim toga

- poslano je upozorenje svim školama i obrazovnim ustanovama kako bi se korisnike pozvalo na oprez.

4. kvartal

- *Phishing* kampanja na škole i obrazovne ustanove nastavila se i u listopadu. Kompromitirane korisničke račune, odnosno račune korisnika koji su nasjeli na *phishing* te upisali svoje korisničke podatke, napadači su iskorištavali za daljnje širenje phishing poruka. Tako su prijave pristizale i od CERT-ova drugih država u koje su se slale *phishing* poruke. Poduzete su sve potrebne mjere, a korisnike se i dalje upozorava da ne upisuju svoje korisničke podatke na stranice koje nisu pouzdane te da ne nasjedaju na *phishing* poruke.
- Sredinom listopada bila je aktivna *phishing* kampanja s ciljem kompromitacije korisničkog računala. Pošiljatelj poruke predstavljao se kao Porezna uprava, a poruke je slao s adrese elektroničke pošte informiranja@porezna-uprava.org. Poruka je naslovljena "Obavijest o primjeni", a u tekstu poruke se korisnika pozivalo na otvaranje *phishing* URL-a. *Phishing* URL nalazio se na lažnoj domeni "porezna-uprava.org" a nakon otvaranja zlonamjerne poveznice sadržane u poruci teksta na korisnički se uređaj automatski počinjala preuzimati izvršna datoteka. Nacionalni CERT korisnicima savjetuje oprez te brisanje zlonamjernih poruka iz sandučića elektroničke pošte.
- Skupina bolnica u američkoj saveznoj državi Alabami sredinom listopada objavila je kako je platila otkupninu nakon što je napad zlonamjernim *ransomware* sadržajem paralizirao njihove sustave. Nakon inicijalnih pokušaja, odlučili su se na plaćanje traženog iznosa u potpunosti, a iako nije poznato o kojoj je svoti riječ, osiguranje je pokrilo glavninu. Napad na bolnice u Alabami samo je jedan u mnoštvu incidenata koji su pogađali bolnice u Sjedinjenim Američkim Državama i Australiji koje su zbog posljedica napada bile primorane odgađati operacije i preglede, a značajan je udar doživio i njihov administrativni sustav. Ukratko, preuzimanje nalaza te naručivanje na preglede zbog posljedica napada nije bilo moguće, a period sanacije je trajao čak 10 dana.
- Krajem studenog objavljena je vijest o pronalasku baze podataka na nezaštićenom poslužitelju koja je sadržavala četiri terabajta podataka. Ukupno je riječ o 1,2 milijarde jedinstvenih zapisa. Iako je riječ o impresivnoj kolekciji, ona ne sadrži osjetljive podatke kao što su lozinke ili brojevi bankovnih kartica. Međutim, sadrži profile stotina milijuna korisnika u kojima se nalaze podaci kao što su brojevi telefona te veze do profila na društvenim mrežama, ali i 50 milijuna jedinstvenih telefonskih brojeva te čak 622 milijuna jedinstvenih adresa elektroničke pošte. Problematična je činjenica kako su zlonamjerni korisnici pristupom ovoj bazi dobili profile korisnika koje su mogli iskoristiti za daljnje napade. Ti profili sadrže sve informacije potrebne za izvršavanje napada te potpuno preuzimanje identiteta pogođenih žrtava što jasno ukazuje na vrijednost podataka, iako nije riječ o podacima koje u većini slučajeva klasificiramo kao osjetljive.

7 Zaključak

Tijekom 2019. godine Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenta i umanjenja štete u slučaju njihovog nastanka. 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.

Nacionalni CERT zaključio je svoj prvi samostalni projekt sufinanciran sredstvima Instrumenta za povezivanje Europe pod nazivom GrowCERT. Projektom se doprinijelo ispunjenju ciljeva Nacionalne strategije kibernetičke sigurnosti. Provedbom projekta doprinijelo se jačanju nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o kibernetičkim incidentima i prijetnjama kibernetičkoj sigurnosti korištenjem novorazvijene platforme za prikupljanje podataka o sigurnosnim incidentima na nacionalnoj i europskoj razini. U prvom kvartalu 2019. godine provedena je prva nacionalna kampanja podizanja svijesti opće populacije o kibernetičkoj sigurnosti pod nazivom "Veliki hrvatski naivci". Organizirane su radionice o kibernetičkoj sigurnosti za poslovni sektor i akademsku zajednicu. Projekt je završio 30. lipnja 2019. godine te su rezultati projekta predstavljeni nacionalnoj, europskoj i međunarodnoj sigurnosnoj zajednici na brojnim konferencijama i sastancima.

Nacionalni CERT je tijekom 2019. godine uspješno sudjelovao u NATO vježbama Cyber Coalition i CMX 2019 te u ENISA-inoj vježbi - "Cyber SOPEx".

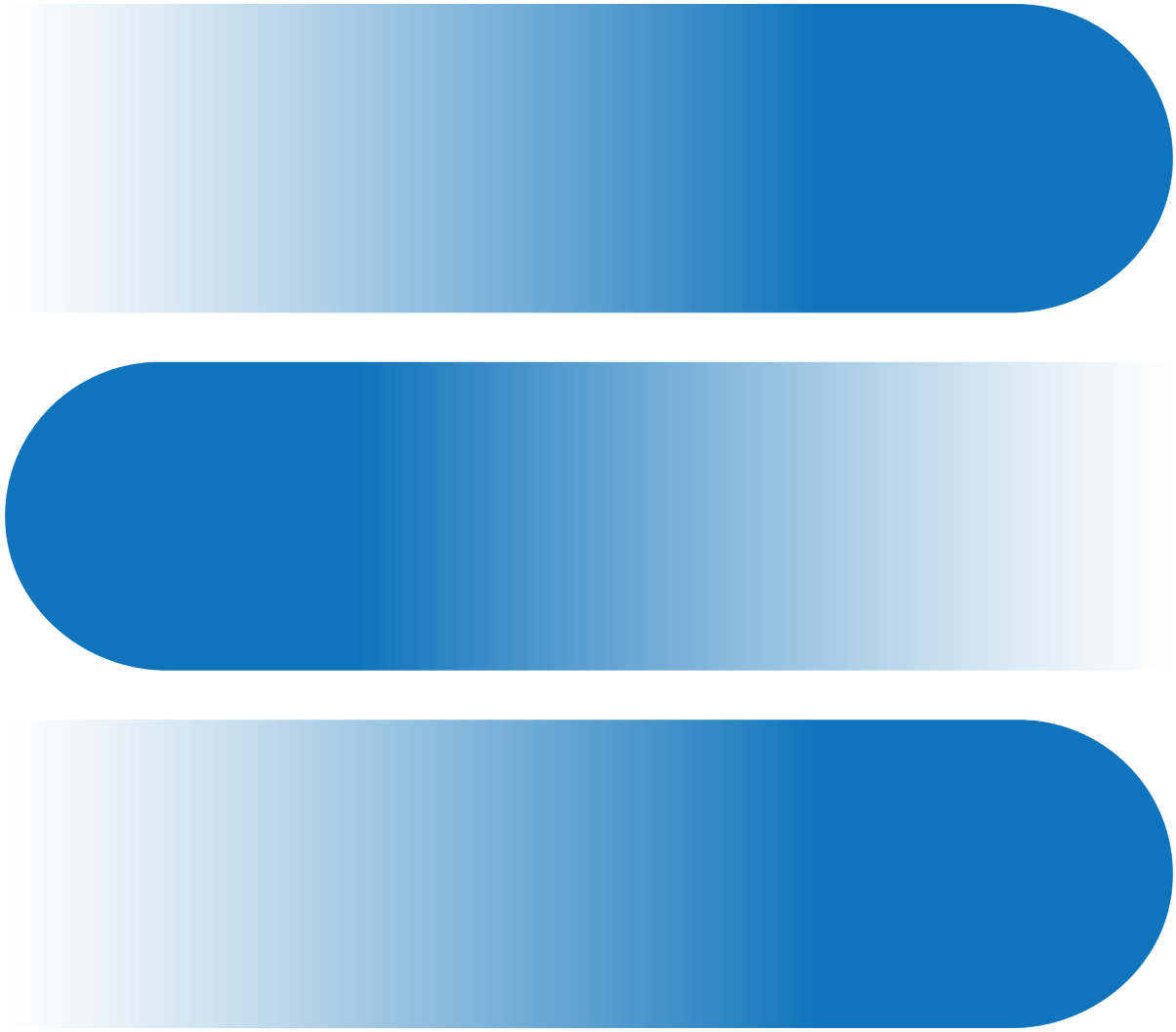
Sumarno, prema statistikama, može se zaključiti kako je broj registriranih *botova* u blagom padu što je rezultat nadogradnje izvora iz kojih se povlače podaci, odnosno prepoznavanje istih obitelji zlonamjernih sadržaja koje se potom mapiraju. Broj obrađenih prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a je u velikom porastu. To možemo pripisati rezultatima kampanje "Veliki hrvatski naivci" kojom je velik broj korisnika saznao da u Hrvatskoj postoji CERT kojem se mogu obratiti u slučaju pojave računalno-sigurnosnog incidenta. Osim toga, održane su radionice za akademsku zajednicu i poslovni sektor te oni više prijavljuju incidente nego prije. Posjećenost portala antibot.hr tijekom 2019. godine dosegla je brojku od 34 375 korisnika, dok je stranica cert.hr posjećena 289 947 puta. Broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu povećao se za 8,5%. Najznačajnija promjena u odnosu na prošlu godinu je općenito velik broj prijavljenih incidenata. U odnosu na 2018. godinu Nacionalni CERT obradio je 65% incidenata više. Velika promjena odnosi se i na pad broja *web defacement* incidenata koji je u 2019. godini pao na 3. mjesto, dok se do sada uvijek nalazio visoko na vrhu.

Zaključno, Nacionalni CERT je u 2019. 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.

8 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 pojmova 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?

CERT.hr
surfaj sigurnije

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

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
Skype: carnet_helpdesk
mail: helpdesk@carnet.hr

1/2020.