Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu

CERT.hr
surfaj sigurnije

Sadržaj

1 Usluge Nacionalnog CERT-a

Nacionalni CERT (eng. *Computer Emergency Response Team*) odjel je Hrvatske akademske i istraživačke mreže – CARNET, čija je osnovna zadaća obrada incidenata na internetu odnosno očuvanje informacijske 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 CERT ZSIS (CERT Zavoda za sigurnost informacijskih sustava).

U listopadu 2017. godine Nacionalni CERT obilježio je 10 godina djelovanja. 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. Do tada, jedini CERT u Republici Hrvatskoj bio je CARNET CERT koji je osnovan 1996. godine. 2013. godine Nacionalni CERT preuzima sve poslove koje je obavljao CARNET CERT. Tako je CARNET omogućio bolju brigu o sigurnosti javnih informacijskih sustava kroz djelatnost Nacionalnog CERT-a te pružio kvalitetniju uslugu korisnicima u sustavu znanosti i obrazovanja kroz aktivnosti tadašnjeg CARNET-ovog Odjela za računalnu sigurnost (2016. godine i taj je odjel pripojen Odjelu 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 sigurnosnih incidenata vezanih uz informacijsko komunikacijske sustave.

Tijekom 2017. godine Nacionalni CERT provodio je svoje proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave sigurnosnih incidenata i smanjenja šteta pri njihovom nastanku.

1.1. Proaktivne mjere

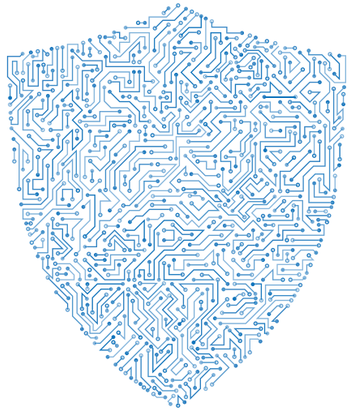
Proaktivnim mjerama Nacionalni CERT djeluje prije incidenata i drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprečavanja ili ublažavanja mogućih šteta. Neke od proaktivnih mjera koje provodi Nacionalni CERT su:

- 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 sa sigurnošću interneta;
- 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 2017. godini

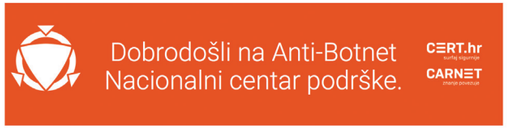
Alati	8
Dokumenti	5
Novosti	108
Ukupno preporuka	2 645
Broj provjera ranjivosti	224

Spam filter • Antivirus • Firewall



Portal antibot.hr

Nacionalni centar potpore **Antibot** krajnjim korisnicima omogućuje bolju detekciju i uklanjanje zlonamjernih programa s njihovih računala. U 2017. godini portal Antibot posjetilo je čak 62 455 korisnika, što je gotovo tri puta više u odnosu na 2016. godinu.



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 algoritma.

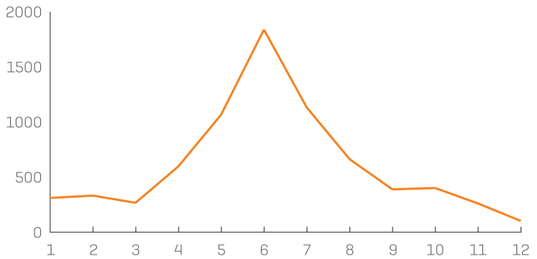
Alati

Kategorija **Alati** na jednom mjestu nudi vrlo koristan pregled antivirusnih programa u besplatnoj verziji ili verziji koja se naplaćuje, 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 mnogih 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.

Spam

Također se prikuplja i analizira neželjena elektronička pošta (spam) koja može sadržavati zlonamjerne URL-ove ili privitke. Takva elektronička pošta najčešće je prvi korak pri infekciji računala krajnjeg korisnika. Rezultati koji detaljno prikazuju neželjene elektroničke poruke (spam) sa zlonamjernim sadržajem nalaze se pod kategorijom **Spam**.



*Maliciozni sadržaj detektiran **spamtrap** senzorom u 2017. godini.*

Provjera ranjivosti

Nacionalni CERT nudi uslugu redovite provjere ranjivosti ustanova članica CARNET mreže. Redovita provjera ranjivosti obavlja se periodički svaka tri mjeseca, a rezultati se šalju odgovornim osobama ustanova u obliku izvještaja koji sadrži listu pronađenih sigurnosnih propusta i upute za njihovo rješavanje.

Uslugu redovite provjere ranjivosti koristi 56 ustanova iz sustava prosvjete, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže.

Stručnjaci Nacionalnog CERT-a provode i masovne provjere ranjivosti CARNET mreže. Automatiziranu masovnu provjeru velikog broja ustanova u kratkom vremenu omogućava softverska komponenta **SPORt** (sustav za pohranu, obradu i preuzimanje rezultata) razvijena u Nacionalnom CERT-u. SPORt omogućava dostavu izvještaja o pronađenim ranjivostima putem web sjedišta uz prethodnu prijavu administratora na ustanovi.

U lipnju 2017. godine obavljena je masovna provjera ranjivosti kojom je obuhvaćeno 980 ustanova spojenih stalnom vezom na CARNET mrežu, nakon čega je napravljena analiza rezultata te su rangirane ustanove prema razini pronađenih ranjivosti. Rezultati obavljenih provjera dali su uvid u sigurnosno stanje CARNET mreže te smjernice za daljnje planiranje s ciljem smanjenja broja ranjivosti.

1.2. Reaktivne mjere

Reaktivnim mjerama djeluje se na incidente u Republici Hrvatskoj te na druge događaje koji mogu ugroziti računalnu 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);
- prikupljanje podataka o kompromitiranim računalima i njihovim aktivnostima s izvora na internetu te njihova analiza;
- prikupljanje i analiza podataka o napadima dobivenih sa sustava ili senzora;
- Abuse služba CARNET mreže.

Statistički podaci provedenih reaktivnih mjera u 2017. godini nalaze se u **poglavlju 5: Stanje računalnih incidenata i statistike.**

1.3. Sigurnost usluga

Tijekom 2017. godine provodile su se aktivnosti unutar CARNET-ovog odjela za Nacionalni CERT koje su za cilj imale povećanje razine sigurnosti CARNET-ovih usluga, računalnih sustava i mreže, a to su:

- prikupljanje i analiza sigurnosnih događaja u CARNET mreži;
- provjera sigurnosti aplikacija, komponenata i usluga CARNET-a;
- provjera ranjivosti mrežnih uređaja u jezgri CARNET mreže;
- usluga izdavanja elektroničkih certifikata (TCS-om);
- provođenje odredaba Programa sigurnosti;
- uvođenje novih tehnologija sa sigurnosnog aspekta u informacijski sustav CARNET-a.

Tijekom 2017. godine Nacionalni CERT u sklopu je tih aktivnosti:

- izdao 464 poslužiteljskih certifikata, od toga 25 *Extended Validation* (EV) certifikata te 25 klijentskih certifikata;
- provodio penetracijska testiranja važnih CARNET-ovih usluga u sklopu implementacije programa sigurnosti u CARNET-ovim poslovnim procesima;
- provjeravao sigurnost usluga razvijenih u CARNET-u ili za CARNET;
- certificirao aplikacije koje pristupaju sustavu “e-Matica”;
- sudjelovao u projektu GEANT 4-2 SA2/T1
- pružao potporu sigurnosnom dijelu projekta “e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)”;
- nastavio rad na SIEM sustavu – sustavu upravljanja informacijama i događajima.

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** (*Forum of Incident Response and Security Teams*) i **TI** (*Trusted Introducer*), čiji je akreditirani član.

2.1. Vježba Cyber Coalition 2017

Petu godinu zaredom Hrvatska akademska i istraživačka mreža - CARNET i njezin odjel za Nacionalni CERT aktivno su sudjelovali u najvećoj i najsloženijoj godišnjoj NATO vježbi zaštite računalnih sustava pod nazivom "Cyber Coalition 2017". U petodnevnoj vježbi koja je trajala od 28. studenog do 1. prosinca 2017. godine sudjelovalo je 25 članica NATO-a, 3 partnerske zemlje NATO-a te tijela NATO-a i EU-a. Kao i prethodnih godina, i ovog puta u provedbi vježbe sudjelovali su hrvatski partneri iz gospodarskog sektora i akademske zajednice. Kako bi se svladali složeni tehnički izazovi koji se pojavljuju pri rješavanju računalnih incidenata, naglasak je stavljen na međusobnu komunikaciju i suradnju. Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti – *Cooperative Cyber Defence Centre of Excellence* (CCD COE) – koji se nalazi u Tallinnu u Estoniji.

2.2. Vježba NATO CMX

Nacionalni CERT sudjelovao je u simulacijskoj vježbi upravljanja u krizama Organizacije Sjevernoatlantskog ugovora (*Crisis Management Exercise* - CMX17) kao član Nacionalne upravljačke skupine za pripremu i provedbu. Vježba se provodila od 4. do 11. listopada 2017. godine. Cilj vježbe bio je testiranje sposobnosti komunikacije unutar zemlje, ali i između partnera te sposobnosti donošenja odluka vezanih uz strateška vojno-politička pitanja.

2.3. CSIRT mreža

Mreža europskih timova za obradu računalno-sigurnosnih incidenta (CSIRT – *Computer Security Incident Response Team*) održala je prvi formalni sastanak 22. i 23. veljače na Malti. Mreža CSIRT-ova 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. Na sastanku su uz predstavnike zemalja članica bili prisutni i predstavnici europskog CERT-a, ENISA-e te Europske Komisije. Hrvatsku je na sastanku zastupala dvočlana delegacija koju su činili stručnjaci iz CARNET-ovog odjela za Nacionalni CERT te Zavoda za sigurnost informacijskih sustava (ZSIS). Na sastanku su usvojeni poslovnik i zadaci Mreže te kratkoročni ciljevi koje bi Mreža trebala ostvariti u narednih 18 mjeseci.

2.4. MeliCERTes Stakeholder Expert Group

Nacionalni CERT sudjeluje u radu radne skupine MeliCERTes koja je oformljena za razvoj platforme za razmjenu informacija u Mreži CSIRT-ova. Platforma za razmjenu informacija o kibernetičko-sigurnosnim incidentima razvija se u sklopu trogodišnjeg CEF projekta SMART 2015/1089. Platforma će objedinjavati skupine alata slobodnog softvera koje većinom koriste europski CSIRT-ovi kako bi se postigla brža razmjena informacija o računalnim prijetnjama i incidentima.

2.5. Sponzorstvo članstvu u organizaciji FIRST

Nacionalni CERT kao primarni sponzor pomogao je kosovskom UBT-CERT-u u procesu apliciranja za pristupanje članstvu organizacije FIRST (*Forum of Incident Response and Security Teams*) koja udružuje svjetske CERT-ove.

3 Suradnja i djelovanje Nacionalnog CERT-a na nacionalnoj razini

3.1. Sporazum o poslovnoj suradnji s MUP-om

U listopadu 2017. godine obnovljen je Sporazum o suradnji na prevenciji i rješavanju računalnih incidenata i drugih oblika računalnog kriminaliteta između MUP-a i CARNET-a (Nacionalnog CERT-a). Sporazumom se nastavlja suradnja s ciljem očuvanja sigurnosti kibernetičkog prostora Republike Hrvatske. Suradnja je potrebna zbog masovne intenzivne uporabe računala i druge elektroničke opreme te interneta, sofisticiranih metoda zlouporaba informacijske tehnologije, iskorištavanja računalno-sigurnosnih slabosti, upotrebe zloćudnog softvera, mogućnosti ostvarivanja visokog stupnja anonimnosti, kao i drugih čimbenika kojima smo svjedoci u današnjem digitalnom dobu. S obzirom na činjenicu da suvremeni način borbe protiv računalnog 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, odnosno njegov Odjel za Nacionalni CERT, potpisao je sporazum o poslovnoj suradnji s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu, odnosno Laboratorijem za sustave i signale Zavoda za elektroničke sustave i obradu informacija FER-a. Temeljem sporazuma, Laboratorij za sustave i signale (LSS) Nacionalnom CERT-u mjesečno dostavlja materijale i prema zahtjevu izvršava usluge iz područja informacijske sigurnosti. LSS Nacionalnom CERT-u mjesečno dostavlja recenziju jednog alata i upute za njegovo korištenje te dva obrazovna materijala iz područja informacijske sigurnosti koji su namijenjeni obrazovanju zainteresirane javnosti. Materijali se objavljuju na web sjedištu *www.cert.hr,* a do sada su objavljeni dokumenti "DNSSEC", "Uvod u socijalni inženjering" i "Osnove privatnosti na internetu" te alat "Tor Browser". U okviru poslova vezanih za provjeru sigurnosti računalnih programa, LSS na zahtjev CARNET-a izvršava provjeru sigurnosti računalne aplikacije.

3.3. Vježba Paukova mreža 2017.

Od 25. do 28. travnja 2017. provedena je združena vojna vježba "PAUKOVA MREŽA 2017", u kojoj je sudjelovalo osamdesetak pripadnika Oružanih snaga Republike Hrvatske zajedno s predstavnicima Fakulteta organizacije i informatike iz Varaždina, Zavoda za sigurnost informacijskih sustava i Nacionalnog CERT-a (CARNET). Vojna vježba "PAUKOVA MREŽA 2017" prva je nacionalna vježba iz područja obrane od kibernetičkih napada na stacionarne i razmjestive komunikacijsko-informacijske sustave. Cilj je bio uvježbati procese donošenja odluke, tehničke i operativne procedure i razmjenu informacija sudionika vježbe u području obrane od kibernetičkih napada na stacionarne i razmjestive komunikacijsko-informacijske sustave. Vježbom su testirane sposobnosti sudionika za otkrivanje zloćudnih aktivnosti na komunikacijsko-informacijskim sustavima, provedba digitalne forenzike, ispitivanje funkcionalnosti zloćudnog koda, uklanjanje prijetnji i provedbu postupaka oporavka komunikacijsko-informacijskih sustava.

3.4. FSec2017 - konferencija o informacijskoj sigurnosti

Djelatnici Nacionalnog CERT-a sudjelovali su u rujnu na FSec2017 – konferenciji o informacijskoj sigurnosti u Varaždinu. Sedmu konferenciju zaredom organizirali su zaposlenici i alumni Fakulteta organizacije i informatike, volonteri i pripadnici Hrvatske zajednice otvorenog koda. CARNET je bio jedan od sponzora konferencije te je pružio infrastrukturnu podršku. Na konferenciji je sudjelovalo više od 300 sudionika iz Hrvatske, regije i svijeta, čime je potvrđeno kako se radi o najvažnijoj konferenciji o informacijskoj sigurnosti u Hrvatskoj i regiji. Predavači na konferenciji bili su predstavnici poznatih svjetskih i domaćih tvrtki i organizacija koje se bave informacijskom sigurnošću, a dolaze iz hakerske zajednice *Chaos Computer Club* i kompanija *Google*, *Cisco*, *Wire, Kaspersky ResetSecurity* itd. Predstavnik Nacionalnog CERT-a sudjelovao je u radu organizacijskog tima konferencije te kao panelist na okruglom stolu o stanju računalne sigurnosti u Hrvatskoj. U sklopu najave konferencije o informacijskoj sigurnosti FSec2017, Nacionalni CERT razgovarao je s doc. dr. sc. Tonimirom Kišasondijem s Fakulteta organizacije i informatike iz Varaždina, predsjednikom organizacijskog odbora i jednim od utemeljitelja konferencije, te objavio intervju u cijelosti na mrežnom sjedištu *www.cert.hr*.

Izvor: FSEC

3.5. Nacionalna strategija kibernetičke sigurnosti (NSKS)

U 2017. godini Nacionalni CERT radio je na provedbi mjera iz Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NSKS). Kako je riječ o prvoj sveobuhvatnoj Strategiji u RH na području kibernetičke sigurnosti, primarni je cilj Strategije prepoznavanje organizacijskih problema u njezinoj provedbi te širenje razumijevanja važnosti ove problematike u društvu. Poticanje koordinacije i suradnje svih državnih tijela i pravnih osoba s javnim ovlastima, ali i drugih sektora društva, nužno je kako bi se uspostavile nove funkcionalnosti, podigla učinkovitost rada relevantnih sudionika te učinkovitije koristilo postojeće resurse i bolje planiralo potrebu i ostvarenje novih resursa. Nacionalni CERT aktivno sudjeluje u radu Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost, tijelima osnovanim odlukom Vlade polovicom 2016. godine s ciljem provedbe Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Strategije.

Mjere u kojima Nacionalni CERT aktivno sudjeluje su:

- razvoj međusektorske suradnje nacionalnih regulatornih tijela i tijela odgovornih za područje informacijske sigurnosti i politike zaštite podataka te međusobna koordinacija i razmjena iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira;
- definiranje taksonomije (uključujući pojam značajnog incidenta), definiranje protokola za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima te uspostava platforme ili tehnologije za razmjenu podataka;
- razmjena prethodno anonimiziranih podataka o incidentima između sektorski nadležnih tijela korištenjem definirane taksonomije i protokola;
- izvještavanje dionika unutar sektora o računalno sigurnosnim incidentima te periodično izvještavanje Nacionalnog vijeća za kibernetičku sigurnost o trendovima, stanju i značajnim incidentima iz prethodnog razdoblja;
- izdavanje upozorenja o sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje;
- izobrazba zaposlenika na godišnjoj razini za potrebe ekspertize i specijalističke izobrazbe;
- izrada i objavljivanje preporuka o minimalnim sigurnosnim zahtjevima za davatelje i korisnike različitih elektroničkih usluga, kao i javno i komercijalno dostupnih bežičnih mreža (Wi-Fi) koje postaju masovno korištene, s ciljem zaštite krajnjih korisnika takvih usluga koji su široko zastupljeni u svim sektorima društva;
- osmišljavanje i provođenje usklađene kampanje o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u Republici Hrvatskoj, o značaju kibernetičke sigurnosti.

3.6. NIS direktiva

Kroz rad stručne radne skupine Nacionalnog vijeća za kibernetičku sigurnost za provedbu obveza Republike Hrvatske u području NIS direktive Europske unije, Nacionalni CERT sudjelovao je u pripremi prijedloga Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Donošenje takvog Zakona proizlazi iz obveza Hrvatske kao članice EU-a za prijenos NIS direktive u nacionalno zakonodavstvo. NIS direktiva, punog naziva Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava, donesena je 6. srpnja 2016. temeljem provedbe Europske strategije kibernetičke sigurnosti iz 2013. godine, a s ciljem osiguravanja zajedničke razine sigurnosti mrežnih i informacijskih sustava u svim državama članicama. NIS direktiva utvrđuje obvezu država članica o uvođenju mjera za visoku razinu zaštite kibernetičke sigurnosti u ključnim sektorima.

3.7. Djelovanje putem javnih medija i obraćanja javnosti

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

- 2/2017 – webinar „Socijalni inženjering – čovjek kao najveća ranjivost sustava“ povodom obilježavanja Dana sigurnijeg interneta;
- 2/2017 – izdan dokument “Ransomware – plati za svoje podatke” povodom obilježavanja Dana sigurnijeg interneta;
- 3/2017 – HRT emisija “Prometej” – prilog o prijevarama i uvredama na društvenim mrežama;
- 3/2017 – Fakultet elektrotehnike i računarstva – predavanje „Pregled stanja sigurnosti u RH iz perspektive Nacionalnog CERT-a“;
- 5/2017 – HRT emisija “Potrošački kod” – prilog o socijalnom inženjeringu i phishingu;
- 5/2017 – izjave zbog globalnog kibernetičkog incidenta *WannaCry* ransomware zlonamjernog sadržaja - Dnevnik Nove TV i Hrvatski Katolički Radio;
- 10/2017 – HRT Dnevnik – predstavljanje projekta GrowCERT;
- 12/2017 – Radio Dalmacija – izjava povodom čestih phishing kampanja usmjerenih na korisnike u Hrvatskoj;
- predavanja na domaćim skupovima za akademsku zajednicu, javne i privatne institucije i širu javnost – izdvajamo: “STO 2017”, “FSEC 2017”, “CUC 2017”;
- predavanja za učenike osnovnih škola o sigurnosti na internetu;
- informiranje javnosti putem web sjedišta Nacionalnog CERT-a (*www.cert.hr*) – 396 834 posjetitelja u 2017.

3 Projekti

4.1. GrowCERT

Nacionalni CERT i CARNET, potaknuti stvaranjem doprinosa ostvarivanju ciljeva Nacionalne strategije kibernetičke sigurnosti, pokrenuli su 1. srpnja 2017. godine 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 sufinanciran je sredstvima Europske komisije putem Instrumenta za povezivanje Europe (CEF – Connecting Europe Facility). Široj i stručnoj javnosti projekt je predstavljen na konferenciji za novinare 23. listopada. Provedbom projekta doprinosi 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. Ovim projektom želi se podići svijest o kibernetičkim prijetnjama te adekvatnim odgovorima na iste. Pripremljen je kreativni koncept za nacionalnu kampanju podizanja svijesti o kibernetičkoj sigurnosti što podrazumijeva veću sigurnost na internetu i društvenim mrežama te zaštitu osobnih podataka. Projektom je omogućeno dodatno ulaganje u ljudske i tehničke kapacitete Nacionalnog CERT-a kako bi se omogućio razvoj novih usluga, poput izrade nacionalnog popisa pošiljatelja neželjene elektroničke pošte (SPAM Blacklist), sustava za distribuciju informacija o otkrivenim ranjivostima i alata za otkrivanje izmijenjenih izgleda stranica web sjedišta (web defacement) i drugih zlonamjernih sadržaja u kibernetičkom prostoru u ovlasti Nacionalnog CERT-a. U okviru projekta sastavljena je stručna radna skupina za uspostavu platforme za razmjenu podataka. Pomoćnik ravnatelja za odjel Nacionalnog CERT-a imenovan je članom tijela CEF Cyber Security DSI Governance Board, a riječ je o Upravljačkom odboru programa Kibersigurnost infrastrukture za digitalne usluge u okviru CEF-a, koji osigurava neformalnu strukturu za smjernice na razini politike i pomoć CSIRT-ovima država članica u jačanju kapaciteta i provedbi dobrovoljnog mehanizma suradnje.

grow-cert

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

U sklopu projekta Nacionalni CERT održava sustav za upravljanje sigurnosnim informacijama i događajima (eng. *Security Information and Event Manager* - SIEM) s ciljem sigurnosnog nadzora CARNET-ove mreže, CARNET-ovih kritičnih usluga te škola uključenih u projekt e-Škole. SIEM rješenje koje se implementira je *AlienVault* USM koje na temelju prikupljenih dnevničkih zapisa s različitih sustava u stvarnom vremenu omogućava detekciju, analizu, korelaciju i pohranjivanje relevantnih sigurnosnih događaja zabilježenih u računalno-mrežnoj infrastrukturi te u aplikacijama. U 2017. godini cjelokupna infrastruktura SIEM-a preseljena je na novu lokaciju, odnosno u udaljeni podatkovni centar.

e-Škole

4.3. GEANT 4-2

Nacionalni CERT sudjelovao je u četvrtoj generaciji projekta GEANT – GEANT 4-2. Projekt je sufinanciran sredstvima Europske unije, a glavni cilj je razvoj paneuropske akademske i istraživačke e-infrastrukture koja je prepoznata kao temelj za poticanje znanstvene izvrsnosti i interoperabilnosti. Nacionalni CERT sudjelovao je u aktivnostima vezanim uz uspostavu okvira za implementaciju sigurnosti u GEANT-ovoj infrastrukturi i uslugama, izradi okvira za sustavni razvoj, održavanje i unaprjeđivanje GEANT-ovih usluga (eng. *Software Management Framework*) te na poslovima sigurnosnih testiranja GEANT-ovih usluga. Nacionalni CERT u 2017. godini sudjelovao je u servisnoj aktivnosti SA2/T1 (eng. *Service Transition and Software Management*). Uspostavljeni su mehanizmi kvalitativne i sigurnosne provjere novih usluga tijekom tranzicije usluga iz razvojnog okruženja u produkciju te periodičkih provjera produkcijskih usluga. U skladu s uspostavljenim okvirom obavljene su kvalitativne i sigurnosne provjere pet novih GEANT-ovih usluga koje su tijekom godine uspješno uključene u produkcijsko okruženje.

GÉANT

4.4. CEKOM

Nacionalni CERT kao partner sudjeluje u provedbi europskog projekta CEKOM (Centar kompetencija). Cilj 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 uz Nacionalni CERT kao partneri sudjeluju Končar, FER i tvrtka Hrvatski operator prijenosnog sustava d.o.o. U prvoj godini projekta predviđeno je da Nacionalni CERT opremi prijenosni laboratorij potreban za obradu incidenata vezanih uz upravljačke sustave, odnosno da nadogradi svoj postojeći labo-

computer systems

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

4.5. Cyber Exchange

U rujnu 2017. godine, kao partner nositelja projektnog prijedloga CZ.NIC-a iz Češke, u okviru Instrumenta za povezivanje Europe – Connecting Europe Facility (CEF), CARNET prijavljuje projektni prijedlog „Cyber Exchange" čiji je cilj povećanje znanja i kapaciteta nacionalnih i vladinih CSIRT-ova i CERT-ova jačanjem prekogranične suradnje, kao i jačanje sposobnosti za timsko suočavanje s naprednim prijetnjama. Uz Češku i Hrvatsku, u prijedlogu zajedničkog projekta sudjeluju i CSIRT-ovi ili CERT-ovi iz Austrije, Grčke, Latvije, Luksemburga, Malte, Poljske, Rumunjske i Slovačke.

4.6. Projekt SMART 2014/1079 – Preparatory activities for the launch of the CEF Core Service Platform for Cooperation Mechanisms for CERTs in the EU

U suradnji s tvrtkom Deloitte, Nacionalni CERT organizirao je 23. listopada nacionalnu radionicu pod nazivom Training & Awareness of the GDPR and the CSP (Core Service Platform) koja je okupila tridesetak predstavnika iz institucija i organizacija koje se bave kibernetičkom sigurnošću. Sudionici su imali priliku bolje se upoznati sa sadržajem GDPR-a – Opće uredbe o zaštiti osobnih podataka koja stupa na snagu 25. svibnja 2018. godine, te o CSP-u – europskoj platformi za razmjenu informacija o kibernetičko-sigurnosnim incidentima. Predavanje su održali stručnjaci iz tvrtke Deloitte angažirani na projektu SMART 2014/1079 financiranom od strane Europske komisije u svrhu provedbe pripremnih aktivnosti za pokretanje platforme CEF Core Service Platform za CERT-ove u Europskoj uniji.

4.7. Projekt SMART 2015/1089 - Establishment of a Core Service Platform between participating Member States and operation of cooperation mechanisms for Computer Emergency Response Teams

Nacionalni CERT aktivno sudjeluje u radu stručne skupine MeliCERTes koja je oformljena u svrhu razvoja platforme za razmjenu informacija u mreži CSIRT-ova. Platforma za razmjenu informacija o kibernetičko-sigurnosnim incidentima razvija se u sklopu trogodišnjeg CEF projekta, a objedinjavat će skupine alata slobodnog softvera koje većinom koriste europski CSIRT-ovi kako bi se postigla brža razmjena informacija o računalnim prijetnjama i incidentima.

5 Stanje računalnih incidenata i statistike

5.1. Najveći globalni računalni incident – WannaCry

Sredinom svibnja 2017. godine zabilježen je novi vrlo ozbiljan oblik prijetnje na internetu u obliku zlonamjernog ransomware programa – „Wannacry", koji iskorištava ranjivost u SMBv1 protokolu. Ovom prijetnjom bila su zahvaćena sva računala s operacijskim sustavom Windows na kojima nije bila instalirana zakrpa objavljena u ožujku u Microsoft Security Bulletinu s oznakom MS17-010.

Kako se radilo o globalnom incidentu, prvom ovakvog intenziteta, suradnja i razmjena informacija između tijela odgovornih za područje informacijske sigurnosti bila je od ključne važnosti za njegovo uspješno rješavanje. Informacije su se razmjenjivale na razini mreže europskih CSIRT-ova (*Computer Security Incident Response Teams Network*), a Nacionalni CERT surađivao je i sudjelovao na izvanrednom sastanku s tijelima unutar Hrvatske, kao što su UVNS (Ured vijeća za nacionalnu sigurnost) i OTKKS (Operativno-tehnička koordinacija za kibernetičku sigurnost).

Nacionalni CERT na ovu je prijetnju reagirao brzo i odgovorno te je poduzeo brojne aktivnosti kako bi se spriječilo širenje incidenta ili kako bi se smanjila šteta u slučaju infekcije. Neke od poduzetih aktivnosti su:

- informiranje šire javnosti o prijetnji putem TV emisija, e-mail poruka i svoje službene web stranice te odgovaranje na pitanja predstavnika medija;
- objava upozorenja i smjernica za zaštitu putem proaktivnih i reaktivnih mjera koje se mogu poduzeti te načina postupanja u slučaju infekcije;
- slanje obavijesti svim članicama CARNET mreže, telekom operaterima te javnim i privatnim tvrtkama s kojima surađuje Nacionalni CERT;
- suradnja sa sistemskim inženjerima i mrežnim odjelom unutar CARNET-a s ciljem sprečavanja širenja ransomwarea te analiza mreže s ciljem otkrivanja potencijalnih kompromitiranih računala.

5.2. Statistika o obrađenim incidentima

Nacionalni CERT je tijekom 2017. godine zaprimio i obradio ukupno 732 prijave koje se mogu klasificirati kao računalni incidenti u nadležnosti Nacionalnog CERT-a.

Vodeći tipovi incidenata su **web defacement** (kompromitirano web sjedište s izmijenjenom početnom web stranicom), **phishing URL** i **phishing**.

Najznačajnija promjena u odnosu na prošlu godinu je rast broja phishing incidenata, što je rezultat nekoliko učestalih phishing kampanja koje su ciljale korisnike u Hrvatskoj te su bile dobro pripremljene, uglavnom na jezično ispravnom hrvatskom jeziku. Kod većine kampanja napadač se predstavljao kao osoba nadređena meti napada.

Velika promjena odnosi se i na rast broja web defacement incidenata kojih je u 2017. godini bilo stotinu više u odnosu na 2016. To je rezultat alata razvijenog unutar Nacionalnog CERT-a koji povlači podatke o izmijenjenom izgledu web stranica iz vanjskih izvora.

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 %, što je rezultat vanjskih (automatiziranih) izvora koji su to češće prijavljivali.

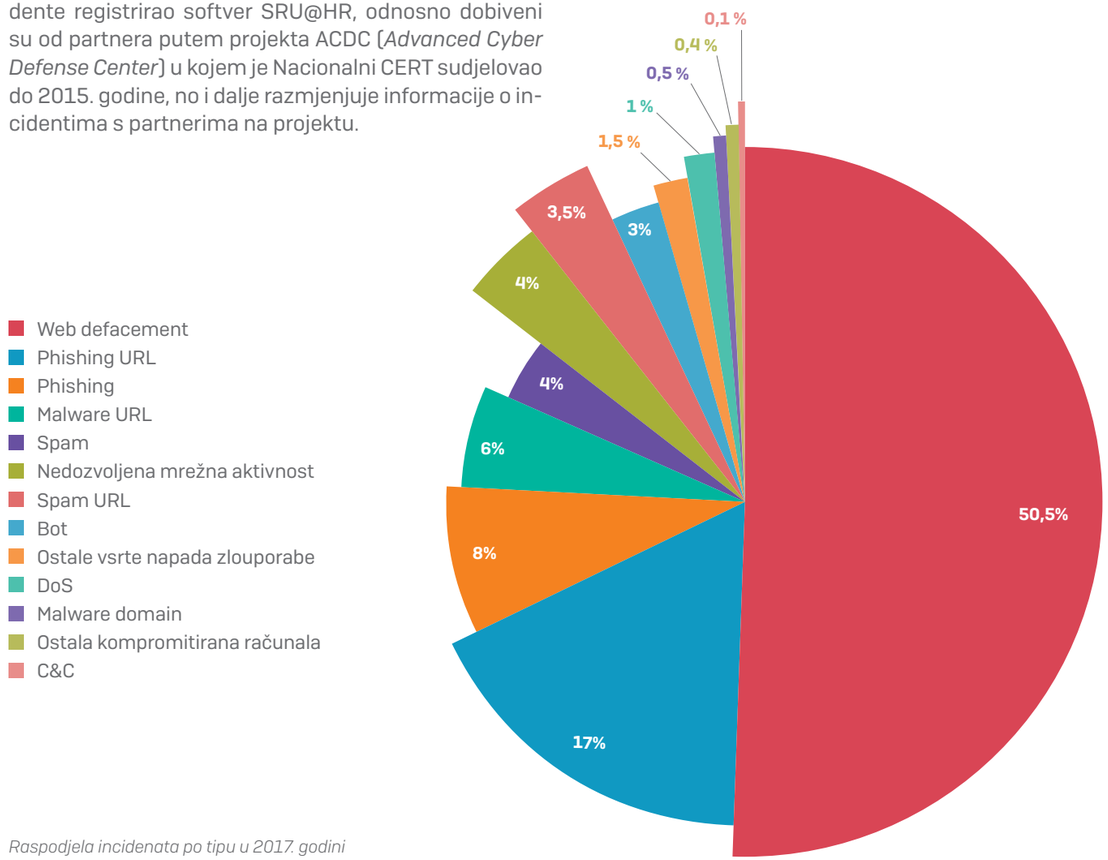
TIP INCIDENTA	BROJ	TREND
Web defacement	370	▲
Phishing URL	127	▼
Phishing	59	▲
Malware URL	42	▼
Spam	29	▲
Nedozvoljena mrežna aktivnost	28	▲
Spam URL	26	▲
Bot	20	▲
Ostale vrste napada i zlouporabe	12	▲
DoS	10	▼
Malware domain	4	▲
Ostala kompromitirana računala	3	▼
C&C	2	–
UKUPNO	732	▲

Prikaz incidenata po tipu u 2017. godini

5.3. Raspodjela incidenata po tipu

Sljedeći grafikon prikazuje omjere incidenata po tipu u 2017. godini, koji su zabilježeni u sustavu za obradu incidenata.

Prijavitelji incidenata, kao i prethodne godine, u većini slučajeva bili su izvan Republike Hrvatske, ili je incidente registrirao softver SRU@HR, odnosno dobiveni su od partnera putem projekta ACDC (*Advanced Cyber Defense Center*) u kojem je Nacionalni CERT sudjelovao do 2015. godine, no i dalje razmjenjuje informacije o incidentima s partnerima na projektu.

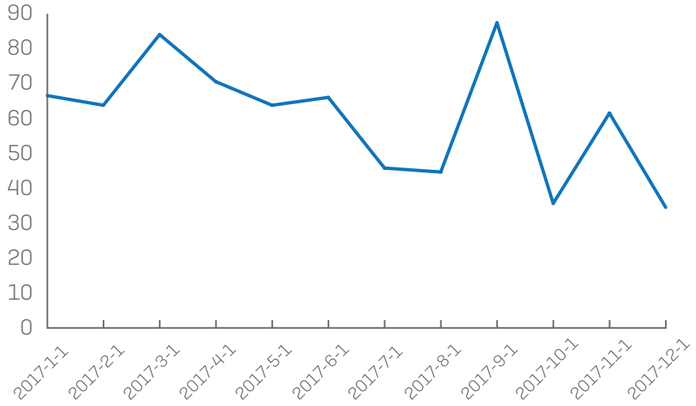


Raspodjela incidenata po tipu u 2017. godini

5.4. Trendovi pojava incidenata na poslužiteljima u 2017. godini

Sljedeći grafikon prikazuje broj obrađenih incidenata na poslužiteljima na mjesečnoj osnovi koje je Nacionalni CERT zabilježio i obradio u sustavu za obradu incidenata.

Najveći broj incidenata zabilježen je i obrađen u rujnu 2017. godine, njih 85. Najmanji broj incidenata zabilježen je u prosincu kada su obrađena 38 incidenta. Prosječan broj incidenata po mjesecu iznosi 61.



Broj incidenata koje je 2017. 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 moguće je očitati da je u Hrvatskoj broj registriranih zaraženih računala u padu te da ih u odnosu na prethodnu godinu ima manje. Broj otkrivenih botova prikazan ovim statistikama temelji se na vanjskim izvorima koji dostavljaju podatke Nacionalnom CERT-u te ne odgovara broju stvarno zaraženih korisničkih računala, ali prikazuje trend i okvir stvarnog stanja.

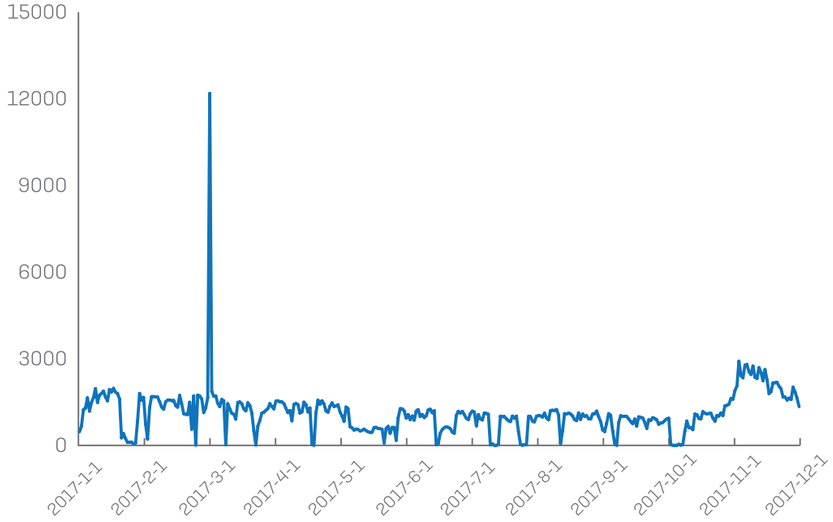
U tablici u nastavku prikazano je deset najčešće prijavljivanih botova prema tipu (vrsti zlonamjernog sadržaja) kroz 2017. godinu, koji su bili diseminirani davateljima usluge pristupa internetu.

Downadup	92 537
Unknown	58 191
Avalanche-andromeda	38 614
Mirai-botnet	32 655
Mirai	31 090
Sality-p2p	24 953
Zeroaccess	12 393
Pushdo	10 143
Renocide	9 964
Ghost-push	9 673

Top 10 botova prema tipu u 2017. godini

Suma zabilježenih botova prema tipu (vrsti zlonamjernog sadržaja) tijekom 2017. godine iznosi 404 266, što je smanjenje od visokih 28 % u odnosu na 2016. godinu.

Broj zabilježenih botova po danima u 2017. 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. Srednja vrijednost broja botova po danu za 2017. godinu iznosila je 1 125,53. U nekoliko navrata može se primijetiti vrlo nizak broj botova, što je posljedica tehničkih problema u sustavu vanjskog izvora što im je onemogućilo slanje izvještaja. Većinu podataka o broju botova Nacionalni CERT dobiva od spomenutog izvora.

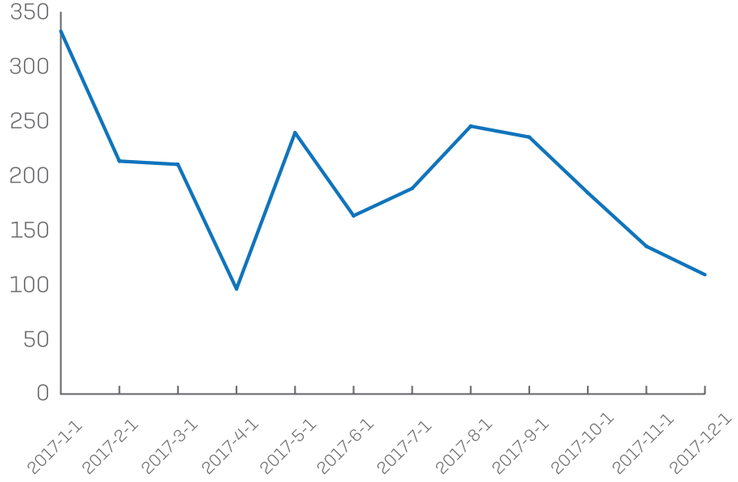


Trend kretanja broja botova po danu u 2017. godini

5.6. Statistika o obrađenim incidentima koji su prijavljeni službi CARNET Abuse

Služba CARNET Abuse bavi se incidentom ako je izvor incidenta korisnik CARNET mreže (ustanova članica ili korisnik AAI@Edu.hr elektroničkog identiteta). Tijekom 2017. godine služba CARNET Abuse obradila je ukupno 2325 incidenata. U odnosu na 2016. godinu to je smanjenje od visokih 44 %. To je, između ostalog, rezultat podizanja svijesti korisnika CARNET mreže o ugrozama na internetu. Pozitivan ishod mjera primijenjenih na populaciji korisnika CARNET mreže služi nam kao temelj povećanja svijesti o računalnoj sigurnosti u cijeloj populaciji. Osim toga, suradnjom s ostalim pružateljima internetskih usluga (*Internet Service Provider* – ISP) u Hrvatskoj, dio incidenata obrađuje se kod davatelja usluge koju pojedini korisnik koristi.

Najveći postotak incidenata odnosi se na povredu autorskih prava (distribuciju datoteke putem BitTorrent protokola koja je zaštićena autorskim pravom). Drugi najčešći incident je pokušaj neovlaštenog pristupa računalu i/ili mreži. U drugom slučaju, korisnike se redovito upućuje na portal antibot.hr kako bi skenirali računalo i očistili ga od zlonamjernog sadržaja.



Broj incidenata koje je 2017. godine obradila služba CARNET Abuse, s prikazom po mjesecima

6 Značajniji incidenti, otkrivene ranjivosti i događaji

1. kvartal

- U siječnju 2017. godine otkrivena su četiri kompromitirana web sjedišta u čijim se html stranicama nalazio umetnuti maliciozni kod koji je pogađao korisnike web preglednika Chrome na Windows OS-u, a ciljao je korisnike u Hrvatskoj prema geolokaciji IP adrese.
- U istom mjesecu zabilježena je phishing kampanja na hrvatske korisnike gdje je cilj napadača bio stjecanje novčane dobiti. Ciljani su bili uglavnom djelatnici računovodstva unutar tvrtki ili ustanova, a napadač se lažno predstavljao u ime nadležne osobe koja doista i radi u toj tvrtki/ustanovi.
- Sredinom veljače Google je pokrenuo implementaciju novih restriktivnih pravila kojima će blokirati JavaScript privitke elektroničke pošte. Nakon što postupak implementacije bude u potpunosti završen, Gmail korisnici neće biti u mogućnosti slati i primati poštu uz koju su vezane .js datoteke, bez obzira na to jesu li u sažetom, tj. arhivskom obliku.
- Krajem veljače Google je objavio kako je SHA-1 sigurnosni algoritam postao službeno zastarjelim nakon što je uspješno izveden prvi napad kolizijom. Iako je SHA-1 algoritam prvi put probijen, dobra je vijest što su istraživači napad opisali kao jedan od najvećih računalnih izazova u povijesti te navode kako napad ovog tipa neće biti financijski moguće izvesti u doglednoj budućnosti.
- U ožujku se dogodila kompromitacija korisničkog računa u jednoj državnoj ustanovi u Hrvatskoj. Na računalo je instaliran spyware „Agent Tesla" koji, između ostalog, ima mogućnost bilježenja/praćenja pritisnutih tipki tipkovnice računala (keylogger) te uzimanje preslike ekrana (screenshot).
- Skupina njemačkih stručnjaka za sigurnost u ožujku je otkrila 26 sigurnosnih propusta kod devet najpopularnijih aplikacija za pohranu lozinki koje čine MyPasswords, Informaticore, LastPass, Keeper, F-Secure Key, Dashlane, Hide Pictures Keep Safe Vault, Avast Passwords i 1Password. Svaka je od navedenih aplikacija u trenutku testiranja bila instalirana na najmanje 500 000 uređaja diljem svijeta. Svi propusti ubrzo su otklonjeni.

2. kvartal

- U travnju 2017. godine zajedničkom akcijom sigurnosnih stručnjaka iz tvrtki Google i Lookout otkriven je novi spyware namijenjen uređajima na Android operacijskom sustavu. Google je novu prijetnju prigodno nazvao "Chrysaor", prema bratu mitskog Pegaza, upravo zato što se otkriveni spyware ponaša vrlo slično kao Pegasus, mobilni spyware razvijen godinu prije.
- Početkom svibnja dogodio se pokušaj provale u e-Dnevnik korištenjem alata 'slowhttptest' i 'acunetix'.
- Sredinom mjeseca svibnja 2017. zabilježen je novi vrlo ozbiljan oblik prijetnje na internetu u obliku zlonamjernog ransomware programa – „Wannacry", koji iskorištava ranjivost u SMBv1 protokolu. Ovom prijetnjom bila su zahvaćena sva računala s Windows operacijskim sustavom na kojima nije bila instalirana zakrpa objavljena u ožujku u Microsoft Security Bulletinu s oznakom MS17-010. Zaraza velikog broja računala u kratkom vremenu i brzo širenje ransomwarea omogućeni su korištenjem alata DoublePulsar backdoor koji je nedavno objavljen na internetu kao skup alata koje koristi NSA.
- Sredinom svibnja ponovo je zabilježena phishing kampanja koja je ciljala korisnike u Hrvatskoj. Zaprimljeno je nekoliko prijava za phishing poruke gdje se napadač lažno predstavljao stvarnim imenima visoko pozicioniranih osoba u tvrtki/instituciji, u ovom slučaju, ovisno o tipu funkcije, imenom predsjednika Uprave, predsjednika Upravnog vijeća, ravnatelja i sl., gdje djelatnicima računovodstva i drugih odgovornih osoba šalju lažni zahtjev za uplatom određene svote novca. Cilj napada bio je stjecanje novčane dobiti.
- Stručnjaci za informacijsku sigurnost sredinom lipnja otkrili su ranjivost staru više od desetljeća u nekoliko operacijskih sustava baziranih na Unixu, uključujući Linux, OpenBSD, NetBSD, FreeBSD i Solaris. Otkrivenu ranjivost potencijalni napadači mogli su iskoristiti za stjecanje root ovlasti, a time i preuzimanje kontrole nad zahvaćenim sustavom.
- Krajem lipnja 2017. zabilježen je novi ozbiljni oblik prijetnje na internetu u obliku zlonamjernog ransomware programa – „Petya", koji iskorištava ranjivost u SMBv1 protokolu u kombinaciji s ranjivošću Microsoft Office paketa koja je zakrpana u travnju, a odnosi se na oznaku CVE-2017-0199.

3. kvartal

- Početkom srpnja stručnjaci za informacijsku sigurnost otkrili su kritičnu ranjivost u kriptografskoj biblioteci GnuPG koja omogućava probijanje kriptografskog algoritma RSA-1024 i otkrivanje tajnog RSA ključa za dešifriranje podataka. Napad potencijalnom napadaču omogućuje otkrivanje tajnog kriptografskog ključa sa zahvaćenog sustava analiziranjem uzoraka korištene memorije ili elektromagnetskih izlaznih podataka na uređaju, koji su rezultat procesa dešifriranja.
- Kasnije tog mjeseca potvrđen je "pad" dva najveća tržišta na "Dark Webu", AlphaBay i Hansa, u koordiniranoj međunarodnoj operaciji u kojoj su sudjelovali FBI (*Federal Bureau of Investigation*), DEA (*US Drug Enforcement Agency*) te nizozemska policija u suradnji s *Europolom*. Radi se o jednoj od najsofisticiranijih operacija u borbi protiv kibernetičkog kriminala. Ugašena je infrastruktura velikog kriminalnog tržišta odgovornog za razmjenu više od 350 000 ilegalnih proizvoda uključujući drogu, vatreno oružje i zlonamjerne kodove korištene za hakiranje raznih servisa i usluga.

- Početkom kolovoza prijavljen je pokušaj *SQL injection* napada na poslužitelju portala znanstvenih časopisa Republike Hrvatske – Hrčak.
- U kolovozu je Adobe izdao zakrpu za ranjivost u Adobe Flash Player programskom paketu koja je napadačima omogućavala pribavljanje povjerljivih korisničkih podataka s Windowsa za prijavu na računalo. Napadima ove vrste bili su podložni programski paketi Microsoft Office 2010, 2013 i 2016 te preglednici Firefox i Internet Explorer.
- Početkom rujna ponovna phishing kampanja na korisnike u Hrvatskoj. Kao i kod prethodne kampanje, napadač se lažno predstavljao, a ovog puta incidentom su bile zahvaćene banke, CARNET, fakulteti i tvrtke.
- Sredinom rujna pojavile su se phishing/scam web stranice koje su služile za dijeljenje lažnih poklon kupona u trgovačkim lancima Bipa i Lidl. Phishing stranice nisu služile za prikupljanje povjerljivih korisničkih podataka. Trgovački lanci Bipa i Lidl dali su svoje službeno priopćenje preko medija da se radi o lažnoj marketinškoj kampanji te upozorili svoje kupce da ne koriste lažne stranice. Nadležni strani pružatelj usluge udomljavanja web sjedišta ubrzo je uklonio lažne stranice.

4. kvartal

- Početkom listopada prijavljena je takozvana „CEO fraud" poruka koja je ciljala djelatnike CARNET-a, gdje se napadač lažno predstavljao imenom ravnatelja CARNET-a, a poruka je poslana djelatnicima računovodstva s lažnim zahtjevom za uplatom određene svote novca. Pravovremeno je detektiran pokušaj prijevare te uplata novca nije izvršena. Isti pokušaj prijevare pokušan je na jednu privatnu tvrtku, također bez financijskih posljedica zbog pravovremene reakcije.
- Sredinom mjeseca otkriven je niz ranjivosti u jezgri WPA2 (Wi-Fi Protected Access II) protokola koje potencijalnom napadaču mogu omogućiti ostvarivanje pristupa bežičnoj mreži te praćenje internetske komunikacije. Tim istražitelja proveo je KRACK (engl. Key Reinstallation Attack) napad kojim su dokazali na koji je način moguće kompromitirati bežičnu mrežu i otkriti osjetljive informacije poput brojeva kreditnih kartica, lozinki, IM poruka, e-pošte i fotografija.
- Tijekom cijelog studenog trajala je phishing kampanja prema korisnicima u Hrvatskoj. Zaprimljen je veći broj upita, a financijski gubitci nisu zabilježeni zbog pravovremene reakcije.
- U prvoj polovici studenog zabilježena je phishing poruka elektroničke pošte s umetnutim phishing URL-om koji je vodio na lažnu domenu 'porezna-uprava.net', s koje se nudi preuzimanje maliciozne datoteke. Nekoliko dana kasnije domena i URL su blokirani. CERT ZSIS napravio je analizu maliciozne datoteke te su zabilježeni URL-ovi s kojima komunicira pokrenuti malware. Šira javnost obaviještena je o prijetnji te nisu zabilježene teže posljedice.
- U drugoj polovici prosinca zaprimljeno više prijava za phishing prijetnju putem elektroničke pošte u kojoj se pošiljatelj lažno predstavlja u ime FINA-e i gdje napadač vještim navođenjem pokušava namamiti potencijalnu žrtvu na preuzimanje maliciozne datoteke preko umetnute zlonamjerne poveznice u tekstu poruke. Tekst poruke jezično je ispravan te lako navodi korisnika na pokretanje poveznice. Iza zlonamjerne datoteke nalazio se zlonamjerni program ransomware koji šifrira datoteke na računalu, a zauzvrat traži otkupninu za dešifriranje šifriranih podataka. Prema nekim saznanjima, u slučaju pokretanja, malware se širi po lokalnoj mreži pogođene ustanove/tvrtke.
- Lažna domena i phishing URL kasnije su uklonjeni. Uz to, na *www.cert.hr* objavljeno je upozorenje o zabilježenoj phishing kampanji.
- Sredinom prosinca stranice WordPressa diljem svijeta postale su meta masivne *brute-force* kampanje. Napadači ovom kampanjom pokušavaju ostvariti pristup velikom broju stranica kako bi na njih postavili Monero miner. Iz tvrtke WordFence, tvrtke koja brine o sigurnosti Wordpressa, kažu kako je riječ o najvećem napadu od osnutka tvrtke 2012. godine. Također navode kako je broj napada u jednom trenutku dosegao gotovo 14 milijuna napada po satu s više od 10 000 različitih IP adresa i to prema oko 190 000 stranica WordPressa.

7 Zaključak

Tijekom 2017. godine Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave sigurnosnih incidenta i umanjenja štete u slučaju njihovog nastanka. Nastavio je razvijati suradnju s institucijama izvan 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 informacijske sigurnosti.

Nacionalni CERT predstavio je široj javnosti svoj prvi samostalni projekt sufinanciran sredstvima Instrumenta za povezivanje Europe pod nazivom GrowCERT. Projektom se doprinosi ispunjenju ciljeva Nacionalne strategije kibernetičke sigurnosti. Dvogodišnji projekt usmjeren je na jačanje nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o kibernetičkim incidentima i prijetnjama te na podizanje svijesti o kibernetičkoj sigurnosti opće populacije, akademske zajednice i poslovnog sektora.

Nacionalni CERT je i tijekom 2017. godine uspješno sudjelovao u NATO-ovoj CyberCoalition vježbi, gdje je Republika Hrvatska sudjelovala u svojstvu igrača. Vještine djelatnika koji se bave digitalnom forenzikom i obradom incidenata morale su ponovo biti podignute na višu razinu. U simulacijskoj vježbi upravljanja u krizama Organizacije Sjevernoatlantskog ugovora (Crisis Management Exercise - CMX17), Nacionalni CERT, zajedno s članovima Nacionalne upravljačke skupine za pripremu provedbu Vježbe, testira sposobnosti komunikacije unutar zemlje, ali i između partnera, te sposobnost donošenja odluka vezanih uz strateška vojno-politička pitanja.

Sumarno, prema statistikama, može se zaključiti kako razina incidenata koji se odnose na broj registriranih *botova* konstantno pada, međutim, u porastu je broj obrađenih prijava koje se mogu klasificirati kao računalni incidenti u nadležnosti Nacionalnog CERT-a. To možemo pripisati činjenici o povećanju svijesti korisnika o ugrozama na internetu te većoj vidljivosti Nacionalnog CERT-a u javnosti u odnosu na prethodnu godinu. Posjećenost portala antibot.hr tijekom 2017. godine dosegla je brojku od 62 455 posjetitelja, što je gotovo trostruko povećanje, te je u korelaciji s manjim brojem zabilježenih zaraženih računala krajnjih korisnika (*botova*). Broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu povećao se za 8 %, što je rezultat vanjskih (automatiziranih) izvora koji su to prijavljivali češće nego prethodne godine. Najznačajnija promjena u odnosu na prethodnu godinu rast je broja phishing incidenata, što je rezultat nekoliko učestalih phishing kampanja koje su ciljale korisnike u Hrvatskoj. Velika promjena odnosi se i na rast broja web defacement incidenata kojih je bilo stotinu više nego prethodne godine, što je rezultat alata za povlačenje informacija o web defacement incidentima razvijenog unutar Nacionalnog CERT-a.

Zaključno, Nacionalni CERT u 2017. godini ostvario je značajne pomake na području nacionalne i međunarodne suradnje, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

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 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	Skup malicioznih programa koji korisniku onemogućuju 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**.

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.

2/2018.

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