# Kibernetički kriminal i njegov porast za vrijeme pandemije koronavirusa

**Fuljatić, Petra**

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2021./2022.

Petra Fuljatić

# Kibernetički kriminal i njegov porast za vrijeme pandemije koronavirusa

Završni rad

Mentor: dr. sc. Vedran Juričić, doc.

Zagreb, siječanj 2022.

# Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

# Sadržaj

# 1. Uvod

U vrlo kratkom vremenu napredni razvoj digitalne tehnologije transformirao je naše društvo. Razvojem digitalne tehnologije svijet postaje povezaniji, obrazovanje, zdravstvo, zabava i sl. postaju pristupačniji, a načini komunikacije, poslovanja i brojnih drugih aktivnosti postaju jednostavniji i automatizirani. Iako digitalni razvoj donosi napredak i nove mogućnosti u gotovo svim aspektima života, otvaraju se vrata i novim mogućnostima kriminala. U doba kada gotovo svi sektori gospodarstva ovise ili se velikim dijelom koriste informacijskim i komunikacijskim tehnologijama, važno je obratiti pažnju kibernetički kriminal koji prati tehnološki napredak u korak te koji može u vrlo kratkom vremenu prouzročiti veliku štetu ne samo jednom korisniku, poslovanju ili organizaciji već više njih i to samo jednim napadom. Osim raznolikosti vrsta kibernetičkih napada, opasnost predstavlja i brojnost načina na koji kibernetički napad može biti izvršen, posebno u doba kada je kibernetski prostor postao važno područje odvijanja svjetskog gospodarstva.

Pojava pandemije koronavirusa u 2020. godini uzdrmala je tok naših svakodnevnih aktivnosti te unijela brojne promjene i neizvjesnost. U tom slučaju, kibernetička sigurnost nije iznimka, a o tome posebno govori znatni porast kibernetičkih napada koji prati pojavu pandemije. Rizik od kibernetičkih napada ionako je u porastu zbog konstantnog digitalnog razvoja i sve većeg oslanjanja svjetskih infrastruktura na kibernetski prostor, no taj se rizik još više povećao prelaskom na rad od kuće, online nastavu, online kupovinu i sl., nakon što su diljem svijeta uvedene restriktivne mjere kako bi se spriječilo širenje virusa. Porast kibernetičkih napada za vrijeme krize uzrokovane pandemijom koronavirusa na jasan način ukazuje na važnost zaštite od kibernetičkih napada. Edukacija o samom kibernetičkom kriminalu, njegovim vrstama te metodama zaštite od kibernetičkih prijetnji ima veliku ulogu u smanjenju rizika od kibernetičkih napada i razornih posljedica koje kibernetički kriminal može ostaviti na svakoga.

# 2. Kibernetički kriminal

Kako bi se na pravilan način mogli zaštititi od kibernetičkih prijetnji najvažnije je poznavanje same definicije kibernetičkog kriminala i koje sve vrste kriminalnih aktivnosti obuhvaća taj termin. Znanje o različitim kategorijama napada jedan je od koraka i kod prevencije napada kao i u svladavanju štetnih posljedica koje napad iza sebe ostavlja. Postoji mnogo rasprava i zabune oko definicije, opsega i ozbiljnosti kibernetičkog kriminala što predstavlja problem kod prevencije i posljedica napada dok je u isto vrijeme broj žrtava kibernetičkog kriminala konstantno u porastu (Hosseinian-Far, Jahankhani, i Al-Nemrat, 2014, str. 152).

Termin kibernetički prostor (engl. *cyberspace*), kojeg je 1984. popularizirao William Gibson u njegovoj noveli *Neuromancer* predstavljao je „mentalno konstruirano virtualno okruženje u kojemu se odvijaju aktivnosti umreženih računala," te prema tome termin „kibernetički kriminal" u širem smislu opisuje zločine koji se događaju unutar tog prostora te simbolizira nesigurnost i rizik na internetu (Wall, 2007, str. 10). Porast naše ovisnosti o računalima i digitalnim mrežama čini tehnologiju metom kriminalnih aktivnosti poput dobivanja informacija ili kao sredstvo za izazivanje nereda ili štete, stoga je ideja o zasebnoj kategoriji računalnog kriminaliteta nastala otprilike u vrijeme kada su računala postala *mainstream*. (Chawki, Darwish, Khan i Tyagi, 2015, str. 4)

Prilikom definiranja kibernetičkog kriminala, International Telecommunication Union (2012) smatra da je najprije važno razlikovati i odrediti odnos između pojmova „kibernetički kriminal" i „računalni kriminal" te navodi kako je pojam „kibernetički kriminal" uži od pojma „računalni kriminal" zato što mora uključivati računalnu mrežu, odnosno pojam „računalni kriminal" obuhvaća i kriminalne aktivnosti koje ne uključuju korištenje računalne mreže. Zatim, postoji nekoliko perspektiva i polazišta kod definiranja kibernetičkog kriminala, primjerice jedna od češćih definicija opisuje kibernetički kriminal kao „svaku aktivnost u kojoj su računala ili mreže alat, cilj ili mjesto kriminalne aktivnosti," no problem kod ove definicije je širina njezina opsega. Ta bi definicija obuhvaćala i tradicionalni zločin poput ubojstva ukoliko bi se, primjerice, računalo koristilo kao fizičko oružje kojim je počinjeno ubojstvo. (ITU, 2012, str. 12) Još jedan problem kod definiranja kibernetičkog kriminala vezan je uz okruženje u kojemu se odvija (Hosseinian-Far i sur., 2014, str. 152). Naime, pojedine kriminološke perspektive opisuju zločine na temelju socijalnih, kulturnih i

materijalnih karakteristika te ih promatraju kao zločine koji se odvijaju na nekoj specifičnoj geografskoj lokaciji. Taj način opisa i definiranja zločina ne može se u potpunosti prenijeti na kibernetički kriminal zbog toga što se kibernetički napadi odvijaju na mreži i najčešće nisu točno povezani s jednom zemljopisnom lokacijom te se stoga okolina u kojoj su kibernetički napadi počinjeni ne može točno odrediti određenim geografskim položajem ili prepoznatljivom društvenom ili kulturnom skupinom (Hosseinian-Far i sur., 2014, str. 152). Razlika u definicijama pojmova u pravosuđu je treća stavka koja se može navesti kao problem u definiranju kibernetičkog kriminala. Poznavanje zakona primjenjivih na počinjene kibernetičke napade važno je ne samo pravosudnim službenicima već i mrežnim administratorima napadnutih mreža, no zakoni u različitim pravosudnim sustavima na drugačije načine objašnjavaju određene termine što onda predstavlja problem. (Chawki i sur., 2015, str. 5) Osim toga, prijavljivanje kibernetičkog zločina je dobrovoljno te je stoga broj počinjenih zločina zasigurno znatno viši nego što to govore statistički podaci, a taj nedostatak realnih podataka također čini prepreku u adekvatnom definiranju kibernetičkog kriminala. (Chawki i sur., 2015, str. 5)

Zatim, prema Chawkiu i sur. (2015) jedna od detaljnijih definicija donesena je na desetom kongresu Ujedinjenih naroda (UN) o „Sprječavanju kriminala i postupanju s prijestupnicima," koja je podijeljena u dvije kategorije:

- U užem smislu: svako nezakonito ponašanje posredstvom elektroničkih operacija koje cilja ka ugrozi sigurnosti računalnih sustava i podataka koje obrađuju.
- U širem smislu: svako nezakonito ponašanje počinjeno putem ili u vezi s računalnim sustavom ili mrežom, uključujući i zločine poput nezakonitog posjedovanja, ponude ili distribucije informacija pomoću računalnog sustava ili mreže.

Dakle, prema navedenim definicijama, kibernetički kriminal uključuje računala i mreže, a riječ „kibernetički" odnosi se na nove vrste kaznenih djela koje su omogućene informacijskom tehnologijom ili na integriranje kibernetičkog prostora u tradicionalna kaznena djela (Chawki i sur., 2015, str. 6).

## 2.1. Povijesni pregled

Prema Liu (2017), povijest kibernetičkog kriminala može se grubo podijeliti u četiri stadija: stadij nicanja, stadij brzog razvoja, stadij široke ekspanzije i stadij uspostavljanja rutine.

Prvi stadij počeo je u kasnim 40-ima i trajao do kasnih 60-ih godina prošlog stoljeća. U ovom razdoblju korištenje računala nije bilo rašireno kao što je to danas, odnosno jedva je postojalo tržište računala, no svejedno je došlo do pojave računalnog kriminala iako tada još nisu postojali ni specifični zakoni ili protumjere protiv te pojave (Li, 2017). Iako u porastu, napadi na računalne sustave nisu bili toliko česti kao što su bili napadi na telefonske sustave. Tzv. *phreakeri* (engl. *phreakers*) su tada bili rani oblik hakera te su njihovi upadi i stvaranje smetnji u telekomunikacijskim sustavima postali kažnjiva djela (Li, 2017). Termin *phreaking* označava „prijevarnu manipulaciju telefonskom signalizacijom radi besplatnih telefonskih poziva," a izraz *phreak* kombinacija je riječi čudak (engl. *freak*), telefon (engl. *phone*) i slobodan (engl. *free*). (Brush, 2014).

Zatim, drugi stadij počeo je 1970-ih i trajao do kraja 1980-ih godina, tijekom kojeg zbog veće ovisnosti pojedinaca i organizacija o računalima dolazi do porasta računalnog kriminala. Opća tendencija bila je da se računalni kriminal povećavao s promjenom metoda napada te se počeo javljati i pravni odgovor (Li, 2017). Također, dok je u tehnologija u tom razdoblju napredovala izvan mogućnosti razumijevanja prosječnih građana, način rada računala ostao je i dalje jednostavan i podložan kriminalnoj manipulaciji te su neki od najčešćih računalnih zločina tog razdoblja bili vandalizam, krađa informacija, usluga i imovine te prijevara. Osim toga, zlonamjerni programi poput virusa, crva, Trojanskih konja i logičkih bombi nastali su tijekom 1980-ih godina te uzrokovali i pojavu antivirusnih poslovanja. Ukratko, drugo razdoblje obilježio porast opsega kibernetičkog kriminala i počinitelja, a novi zakoni protiv rastućih zločina povećali su zastrašivanje kriminalaca što je dovelo do povećane vjerojatnosti njihova otkrivanja od strane novih policijskih snaga (Li, 2017).

Treći stadij je otprilike obuhvatio čitave 1990-te godine i obilježen je daljnjim širenjem kibernetičkog kriminala i implementiranjem relevantnog zakonodavstva (Li, 2017). Okarakteriziran je i ulaskom osobnih računala u domove i urede u razvijene te čak i neke od manje razvijenih zemalja svijeta. Izumom WWW-a pristup internetu postaje dostupan i prosječnim korisnicima koji onda postaju suočeni s prijetnjama globaliziranog kibernetskog prostora u kojemu dolazi do razvoja sve složenijih vrsta kibernetičkih napada. Autor navodi kako su ovome razdoblju osobna računala mogla biti napadnuta tijekom dobrovoljnog surfanja Internetom, web stranice više nisu bile samo alat za izvođenje napada već i mete za napade te je pojava niza napada zlonamjernim programima uzrokovala još veći porast proizvodnje antivirusnih alata. U trećem stadiju gotovo sve vrste kibernetičkog kriminala su

se pojavile i kriminalizirale, većina potencijalnih korisnika računala i mreža bili su povezani, težina kažnjavanja dosegnula je viši stupanj te je stoga i vjerojatnost otkrivanja zločina dosegnula višu razinu (Li, 2017).

Četvrti stadij počeo je otprilike od 2000. godine, kada kibernetički kriminal više nije novost već postaje rutina, a dotadašnja pravna praznina postaje popunjena (Li, 2017). Ozbiljnu prijetnju predstavljale su razne nove vrste virusa, napisanih uz pomoć specifičnih softvera, koji su uključivali višestruke metode napada i onesposobili antivirusne alate te uzrokovali milijarde dolara gubitka (Li, 2017). Kao i u svakom prethodnom stadiju razvoja, četvrti stadij je također obilježen otkrićima novih trendova u računalnom i kibernetičkom kriminalu. Prvim desetljećem 21. stoljeća dominirale su nove, visoko sofisticirane metode kibernetičkih napada kao što su *phishing* i *botnet* napadi, kao i sve veća upotreba tehnologije kao što je *voice-over-IP* (VoIP) komunikacija i *cloud computing.* Kako su kriminalci postali sposobniji u automatiziranju napada, njihov broj se povećao stoga su regionalne i međunarodne organizacije dale konkretnije odgovore na rastuće izazove kibernetičkog kriminala. (ITU, 2012, str. 13 i 14)

## 2.2. Klasifikacija

Razvoj sheme klasifikacije kibernetičkog kriminala koja povezuje slična kaznena djela u zasebne skupine, drugi je pristup njegovom definiranju (Hosseinian-Far i sur., 2014, str. 154). Tijekom godina razvijeno je nekoliko različitih shema. Primjerice, smatrajući dostupne definicije kibernetičkog kriminala preširokima, Gordon i Ford (2006) predlažu kako je korisno podijeliti kibernetički kriminal na dvije različite kategorije s ciljem stvaranja konceptualnog okvira kojeg zakonodavci mogu koristiti u stvaranju pravnih definicija koje bi bile smislene iz tehničke i iz društvene perspektive. Prema autorima, prva kategorija kibernetičkog kriminala ili tip I ima sljedeće karakteristike:

- Općenito je pojedinačni ili diskretni događaj iz perspektive žrtve.
- Često je omogućen uvođenjem zlonamjernih programa poput *keystroke loggersa*, virusa, *rootkit* programa ili Trojanskih konja u korisnikov računalni sustav.
- Uvođenje zlonamjernih programa može, iako ne nužno, biti olakšano određenim ranjivostima.

Zatim, Gordon i Ford (2006) navode kako kibernetički kriminal tipa II, uključuje aktivnosti poput *cyber* uhođenja i uznemiravanja, dječje pornografije, iznuđivanja, ucjene, manipulacije

tržištem dionica, složene korporativne špijunaže i planiranja ili izvođenja terorističkih aktivnosti na mreži te ima sljedeće karakteristike:

- Suprotno tipu I, najčešće nije omogućen uvođenjem zlonamjernih programa, već se razgovori između žrtve i počinitelja mogu odvijati putem alata za slanje istovremenih poruka ili se datoteke mogu prenijeti putem FTP mrežnog protokola.
- Iz korisnikove perspektive, najčešće su to ponavljajući kontakti ili događaji.

Iz karakteristika dvaju tipova može se zaključiti kako kibernetički kriminal objedinjuje raspon kriminalnih aktivnosti od onih koje su gotovo potpuno tehnološke prirode do onih koje su u svojoj prirodi više povezane uz ljude (Gordon i Ford, 2006, str. 15).

Kibernetički kriminal često se klasificira na temelju odnosa računala i računalnih sustava prema zločinu, pa tako Chawki i sur. (2015) dijele kibernetički kriminal na tri kategorije:

- Računalni sustav kao cilj
- Računalni sustav kao alat
- Kaznena djela povezana sa sadržajem

Prva kategorija obuhvaća hakiranje i ostala kaznena djela povezana s hakiranjem te vrste zlonamjernih programa – virusi, crvi i Trojanski konji. Druga kategorija obuhvaća načine na koje kibernetički kriminalci koriste Internet kao alat što uključuje *phishing* i seksualno uznemiravanje u kibernetičkom prostoru, a treća kategorija uključuje proizvodnju, distribuciju, dijeljenje i konzumiranje dječje pornografije (Chawki i sur., 2015).

Na sličan način Wall (2007) također dijeli kibernetički kriminal na tri kategorije:

- Zločini protiv integriteta računala – hakiranje, krekiranje i napadi uskraćivanjem usluga
- Računalno potpomognut zločini – virtualne pljačke, prijevare i krađe
- Zločini nad računalnim sadržajem – pornografija, nasilje i uvredljiva komunikacija

Nadalje, Konvencija o kibernetičkom kriminalu usvojena na konferenciji Vijeća Europe u Budimpešti, koju je Republika Hrvatska potpisala 23. studenoga 2001. godine, utvrđuje četiri kategorije kibernetičkog kriminala: kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava, računalna kaznena djela, kaznena djela u svezi sa sadržajem i kaznena djela povrede autorskih i srodnih prava (Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu NN 9/2002).

Klasifikacija kibernetičkog kriminala koju pruža Konvencija o kibernetičkom kriminalu nije u potpunosti dosljedna jer se sve četiri kategorije ne temelje na jedinstvenom kriteriju za razlikovanje među kategorijama, točnije kategorija „računalna kaznena djela“ usmjerena je na načine izvršenja kaznenih djela, dok su ostale kategorije usmjerene na objekt pravne zaštite. Iako ova nedosljednost dovodi do nekoliko preklapanja vrsta napada među kategorijama, taj način klasifikacije kibernetičkog kriminala može poslužiti kao korisna osnova u daljnjoj diskusiji o kibernetičkom kriminalu (ITU, 2012, str. 12). Kategorija kaznenih djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava obuhvaća kaznena djela kao što su nezakoniti pristup, nezakonito presretanje, ometanje podataka, ometanje sustava i zloporabu naprava te sva kaznena djela u ovoj kategoriji su usmjerena protiv (najmanje) jednog pravnog načela – tajnosti, cjelovitosti ili dostupnosti (ITU, 2012). Zatim, kategorija računalnih kaznenih djela obuhvaća računalno krivotvorenje i računalnu prijevaru, a kaznena djela u svezi sa sadržajem fokusiraju se na kaznena djela vezana uz dječju pornografiju, rasizam, govor mržnje, veličanje nasilja i sl. Posljednja kategorija, odnosno kaznena djela povrede autorskih i srodnih prava odnose se na nezakonito preuzimanje, kopiranje i distribuiranje proizvoda zaštićenih autorskim i srodnim pravima (ITU, 2012).

## 2.3. Motivi kibernetičkih kriminalaca

Za bolje razumijevanje kibernetičkog kriminala važno je poznavanje i motiva kibernetičkih kriminalaca odnosno njihovih razloga za upuštanje u takve kriminalne aktivnosti. Ako imamo u vidu način na koji razmišljaju ili smo upoznati s nekim od mogućih motiva kibernetičkih kriminalaca, barem smo nekoliko koraka bliže prevenciji kibernetičkih napada.

„Glavni agenti u aktivnostima kibernetičkog kriminala su hakeri,“ no nisu svi kibernetički kriminalci hakeri (Cano, Cavaller, Sabillon, i Serra, 2016). Kompjuterski haker može se definirati kao “stručnjak za programiranje i rješavanje problema s računalom“ i „osoba koja ilegalno stječe pristup informacijama u računalnom sustavu i ponekad njima petlja“ („Hacker“, 2011). Gledajući na povijest termina haker (engl. *hacker*), termin je u svojim početcima korištenja u 1960.-im godinama imao pozitivniju konotaciju nego danas, odnosno tada se češće koristila prva navedena definicija kako bi se opisali tadašnji „pioniri interneta, oni koji su približili računala i internet široj publici“ (Steinmetz, i Yar, 2019, str. 53). Tadašnji hakeri među sobom su formirali neku vrstu zajednice koja je imala vlastitu etiku koja je zagovarala vrijednosti poput slobodnog pristupa znanju i informacijama te

njihovoj slobodnoj razmjeni, iskazivala nepovjerenje u političke, vojne i korporativne vlasti kao i otpor uobičajenom načinu života, stavovima i socijalnoj hijerarhiji – vrijednosti poput onih koje zagovara hakerska etika (engl. *hacker ethics*) koju prvi put spominje Steven Levy 1984. u knjizi *Hackers: Heroes of the Computer Revolution* (Steinmetz, i Yar, 2019, str. 54). S vremenom, pojam haker gubi svoj pozitivan prizvuk te se razumijevanje tog pojma usredotočuje na njegovu negativnu stranu, odnosno onu povezanu s ilegalnim aktivnostima. Neki su zbog toga počeli koristiti i termin kreker (engl. *cracker*) kako bi razlikovali zlonamjerne od dobronamjernih hakera (Steinmetz, i Yar, 2019, str. 53).

Motivi kibernetičkih kriminalaca mogu biti raznovrsni, a neki od najčešćih općenitih motiva su stjecanje protupravne imovinske koristi, osveta, želja za samodokazivanjem i postizanjem određenog uspjeha, intelektualni izazov, znatiželja, zavist, mržnja, oduševljenje vlastitim znanjima i vještinama, kompleks niže vrijednosti, radoznalost, zabava, potreba za pobjedom, želja za stjecanjem ugleda među ostalim hakerima itd. (Bingulac, Dragojlović i Matijašević-Obradović, 2014).

Prema Chawkiu i sur. (2015) kriminalno profiliranje je pojam koji „predstavlja znanost razvijanja opisa fizičkih, intelektualnih i emocionalnih karakteristika kriminalaca na temelju informacija prikupljenih na mjestu zločina.“ Kada je riječ o kriminalnom profiliranju kibernetičkih kriminalaca, nemoguće je svrstati sve kibernetičke kriminalce u jednu skupinu odnosno stvoriti jedan univerzalni profil kibernetičkog kriminalca, no postoje određene karakteristike koje bi mogle pomoći kod efektivnije prevencije od napada (Chawki i sur., 2015, str. 15). Bingulac, Dragojlović i Matijašević-Obradović (2014) dijele kibernetičke kriminalce na zlonamjerne izvršitelje kibernetičkih napada i hakere, na temelju njihovih kriminalnih odnosno psiholoških profila. Zlonamjerni izvršitelji kibernetičkih napada najčešće su motivirani koristoljubljem, u prosjeku imaju između 19 i 30 godina, pretežno su muškog spola, iznimno su inteligentni i nerijetko prekvalificirani za svoje radno mjesto na kojem uglavnom imaju više godina radnog iskustva, također najčešće sebe uopće ne smatraju kriminalcima. Potom, psihološki profil hakera obuhvaća karakteristike poput visoke inteligencije, radoznalosti, brzog upijanja novog znanja, obraćanja pozornosti na sitnice, nepristranosti zbog želje za intelektualnim naporom, arogancije itd. (Bingulac, Dragojlović i Matijašević-Obradović, 2014). Također, hakeri su dobri u tzv. socijalnom inženjeringu – postupku u kojem se ljude putem telefona ili interneta navodi da otkriju povjerljive informacije o sebi. Osim toga, slično kao i zlonamjerni kibernetički kriminalci, koji negiraju sebe kao kriminalce, hakeri smatraju svoje činove opravdanima i etički korektnima

(Bingulac, Dragojlović i Matijašević-Obradović, 2014). Općenito, mnogi kibernetički kriminalci imaju tzv. „Robin Hood sindrom“ – opravdavaju svoje postupke zbog toga što uzimaju onima koji si to (prema njihovom mišljenju) mogu priuštiti (Chawki i sur., 2015, str. 15). Kao primjer takvog načina opravdavanja kibernetičkog kriminala može poslužiti nedavni hakerski napad izvršen u 11. mjesecu 2020. godine od strane hakerske grupe pod imenom Darkside. Darkside grupa ukrala je oko $20,000 u bitcoinu od nekoliko velikih tvrtki koje je zatim odlučila donirati dobrotvornim ustanovama. Na svom blogu, grupa je izjavila da cilja samo velike komercijalne tvrtke i da smatraju pravednim to što će dio novca koji te tvrtke posjeduju ići u dobrotvorne svrhe. (Tidy, J., 2020).

Iako korisno kod procjene krivnje ili sužavanja polja osumnjičenika, važno je naglasiti da kriminalno profiliranje kibernetičkih kriminalaca daje samo ideju o generalnom tipu osobe koja je počinila kazneno djelo, odnosno ne može sa sigurnošću nekoga optužiti za zločin (Chawki i sur., 2015, str. 16).

Zatim, kada je riječ o podjeli hakera u specifične kategorije, ne postoji globalno prihvaćena kategorizacija hakera, ali najčešće glavne kategorije u koje se hakeri dijele su hakeri crnih, bijelih ili sivih šešira, dok se sve ostale potkategorije baziraju na specifičnim motivima, propagandi, hakerskom aktivizmu i političkim ili vjerskim razlozima (Cano et al., 2016). U svome članku, autori opisuju svaku od 3 temeljnih kategorija hakera:

- Bijeli hakeri/hakeri bijelih šešira: Pojedinci koji rade u skladu s hakerskom etikom, odnosno oni koji ne čine štetu ili rade kao stručnjaci za sigurnost.
- Crni hakeri/hakeri crnih šešira: Hakeri koji su motivirani ljutnjom, mržnjom ili moći i ne oklijevaju u krađi i uništavanju podataka u koje prodiru.
- Sivi hakeri/hakeri sivih šešira: Ova vrsta hakera djeluje i ofenzivno i obrambeno u različitim situacijama, odnosno oni su „reformirani crni hakeri“ koji sada rade kao sigurnosni savjetnici.

Osim podjele hakera u samo dvije (hakeri i krekeri) ili tri kategorije (crni, bijeli i sivi), odnosno jednostavnih podjela na „dobre i loše“ hakere ili kibernetičke kriminalce, potrebno je napraviti detaljniju distinkciju u njihovoj kategorizaciji prema njihovim aktivnostima odnosno vrstama napada (Furnell, 2001). Iako napominje da ni ova kategorizacija hakera nije najpotpunija, Furnell (2001) dijeli hakere u sljedećih nekoliko skupina:

- *Cyber* teroristi: Teroristi koji koriste hakerske tehnike kako bi izvršili napad na podatke, mreže ili sustave zbog određene društvene ili političke agende.

- *Cyber* ratnici: Osobe koje primjenjuju hakerske tehnike u vojnom ili ratnom aspektu, kako bi napale sustave kritičnih infrastruktura.
- Haktivisti: Vrsta hakera koji provalama u računalne sustave pokušavaju promovirati određenu aktivističku agendu.
- Pisači *malwarea*: Pojedinci koji stvaraju zlonamjerne programe poput crva, virusa i Trojanskih konja, ne smatraju se strogo podvrstom hakera.
- *Frikeri*: Hakeri koji svoje napade usmjeravaju isključivo na telefonske mreže i pripadajuće tehnologije.
- *Sneakeri* (engl. *sneakers*): Pojedinci unajmljeni za obavljanje legalnih upada u računalne sustave iz opravdanih razloga.
- *Script kiddies*: Hakeri koji se uslijed ograničenih hakerskih vještina oslanjaju na već napisane programe zbog čega često rade greške i zlonamjerne štete te stoga često budu ismijavani od strane drugih, iskusnijih hakera.
- Softverski pirati**:** Hakeri koji dobavljaju i potom distribuiraju ilegalne kopije softvera koji su zaštićeni autorskim pravima.

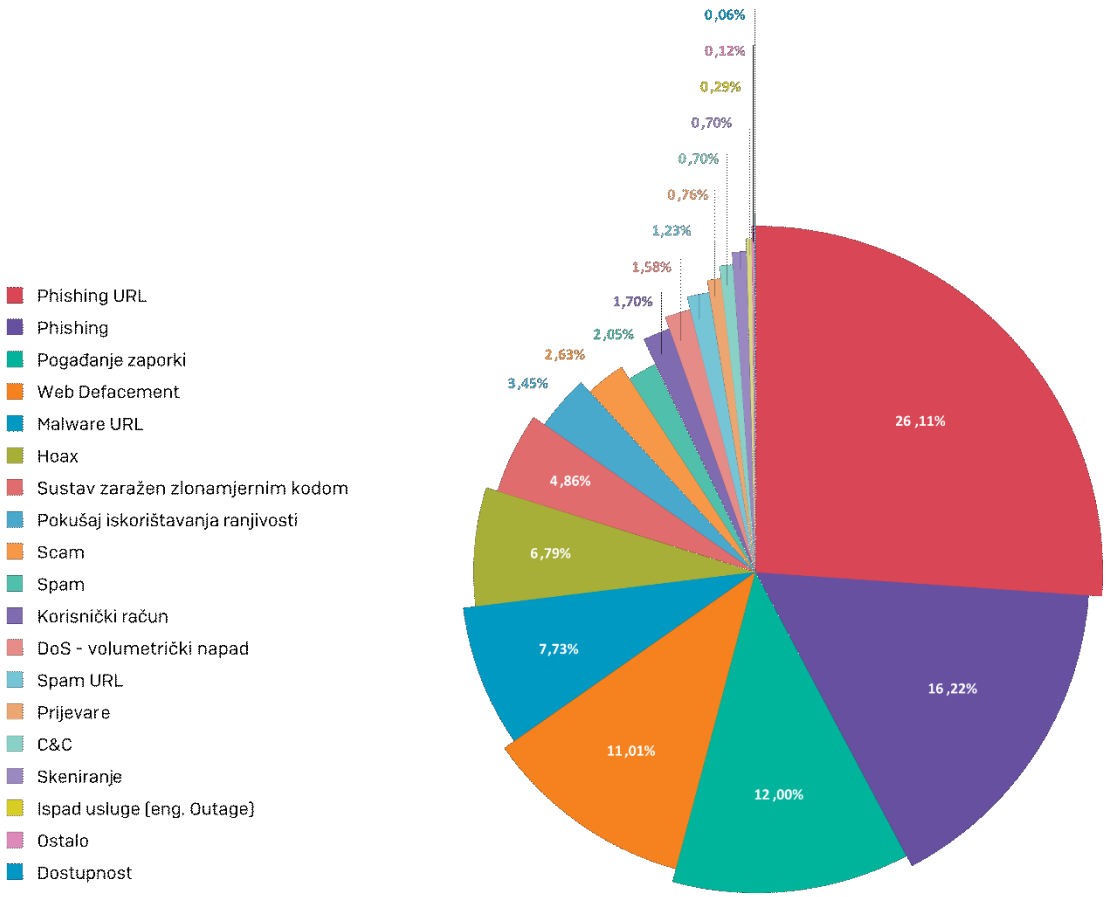
Na temelju cilja kojeg imaju na umu, Chawki i sur. (2015) dijele kibernetičke kriminalce u četiri šire kategorije:

- Djeca i adolescenti između 6 i 16 godina: Ova se dobna skupina najčešće upušta u kriminalne aktivnosti zbog radoznalosti ili želje za dokazivanjem među svojim vršnjacima.
- Organizirani hakeri: Zajednica hakera koja je organizirana kako bi ispunila neke svoje zajedničke ciljeve vezane uz isti politički ili društveni fundamentalizam.
- Profesionalni hakeri/krekeri: Hakeri koji su motivirani novcem, zaposleni su da bi hakirali stranice svojih suparnika te tako došli do vrijednih informacija ili su čak zaposleni kako bi hakirali sustav vlastitog poslodavca ne bi li ga tako učinili sigurnijim.
- Nezadovoljni zaposlenici: Odnosi se na pojedince koji hakiraju sustave svojih poslodavaca iz osvete zbog dobivenog otkaza ili općenitog nezadovoljstva poslovanjem.

# 3. Vrste kibernetičkih napada

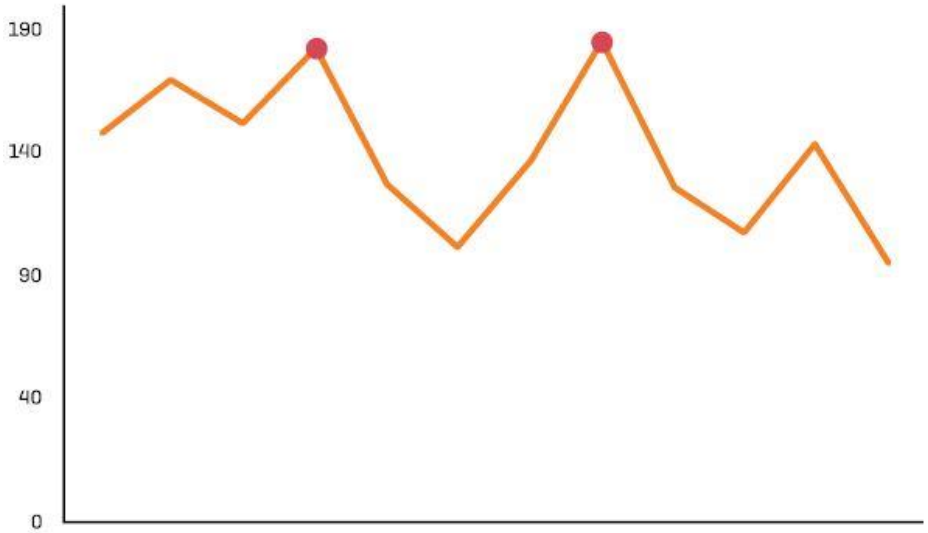
Opasnosti koje prijete na Internetu mogu se podijeliti u dvije osnovne klase napada: računalnu prijevaru i otmicu. Računalna prijevara odnosi se na pokušaj izmamljivanja novaca nuđenjem sumnjivih proizvoda putem elektroničke pošte i iskočnih oglasa ili navođenjem na otkrivanje osobnih informacija ili podataka o bankovnim računima. Najčešće metode računalne prijevare su krađa identiteta, *phishing* i *spam* (Conry-Murray, 2005, str. 2). Otmica se odnosi na pokušaje kriminalaca da preuzmu kontrolu nad računalom korisnika kako bi proveli svoje zle namjere kao što su praćenje korisnikove online aktivnosti, prikazivanje neželjenih oglasa, slabljenje performansi računala ili Internetske veze i sl. te se u tim pokušajima kriminalci vrlo često oslanjaju na zlonamjerne softverske programe (engl. *malware*) (Conry-Murray, 2005, str. 2). Ako uzmemo u obzir klasifikaciju iz Konvencije o kibernetičkom kriminalu, računalna prijevara i otmica predstavljaju najčešće vrste napada iz prve dvije kategorije kriminala, a prijetnje koje još uz njih vrebaju jesu izloženost nepoželjnim sadržajima poput dječje pornografije te aktivnostima poput *online* kockanja ili ilegalnog širenja autorskim pravima zaštićenih filmova, glazbe, video igara i sl., što pak obuhvaća najčešća kaznena djela definirana u druge dvije kategorije u Konvenciji (Conry-Murray, 2005, str. 2).

U posljednjem Godišnjem izvještaju rada Nacionalnog CERT-a za 2020. godinu zabilježeno je 66% incidenata više nego u 2019. godini te su gotovo sve kategorije incidenata u porastu. Nacionalni CERT je tijekom 2020. godine zaprimio i obradio ukupno 1710 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a, od kojih su vodeći tipovi incidenata *phishing* URL, *phishing* i pogađanje zaporki (Nacionalni CERT, 2021, str. 10). Prijave incidenata Nacionalni CERT zaprima putem adrese elektroničke pošte incident@cert.hr, korištenjem OSINT metoda (engl. *Open Source Inteligence*) za otkrivanje računalno-sigurnosnih incidenata te od vanjskih izvora kroz automatizirane softvere za obradu incidenata (Nacionalni CERT, 2021, str. 12). Na slici 1. prikazan je omjer incidenata po tipu u 2020. godini.




Slika 1. Raspodjela incidenata po tipu u 2020. godini (Nacionalni CERT, 2021, str. 12)

Zatim, slika 2. prikazuje broj obrađenih incidenata na poslužiteljima po mjesecima, a na prikazu se primjećuju 2 skoka u broju incidenata od kojih je jedan u travnju, a drugi u kolovozu (Nacionalni CERT, 2021, str. 13). Autori navode kako je prvi skok rezultat velikog broja *phishing* kampanja vezanih uz COVID-19 jer je u tom razdoblju „velik broj država bio u *lockdownu* i poslovanje se kod velikog broja korisnika prebacilo u model rada od kuće, što je napadačima dalo dodatnu motivaciju za kreiranjem phishing kampanja“ (Nacionalni CERT, 2021, str. 13). Drugi skok u broju incidenata autori objašnjavaju korištenjem OSINT metoda koje dovode do većeg broja otkrivenih zlonamjernih stranica te kompromitiranih web sjedišta s izmijenjenim izgledom i sadržajem web stranica.




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

Slika 2. Broj incidenata na poslužiteljima u 2020. godini po mjesecima (Nacionalni CERT, 2021, str. 13)

## 3.1. Spam

Neželjena pošta (engl. *spam*) su „poruke elektroničke pošte, najčešće komercijalnoga sadržaja, nerijetko vezane uz neku obmanu, koje se masovno šalju na adrese slučajno odabranih primatelja“ (Hrvatska enciklopedija, 2021). U usporedbi s krađom identiteta ili napadima zlonamjernim programima, *spam* i ne predstavlja toliku opasnost (osim ako ne sadrži zlonamjerni softver), no veoma je raširena i česta vrsta napada koja zatrpava elektronski poštanski sandučić te može sadržavati uvredljiv sadržaj ili slike (Conry-Murray, 2005, str. 3) Ipak, zahvaljujući naprednoj tehnologiji, većina *spama* uspije se filtrirati na ulazu te tako ni ne uspije ući u poštanski sandučić (Conry-Murray, 2005, str. 99). U pozadini *spama* nalazi se neko poduzeće koje želi reklamirati svoj proizvod i spremno je napadaču platiti za reklamu koja će doseći veliki broj korisnika, prema obećanju kojim se napadač reklamira (Šolić i Velki, 2018, str. 74). Gledajući na veličinu Interneta, može se zaključiti da napadači pomoću spama mogu izvući značajnu financijsku dobit (Šolić i Velki, 2018, str. 74). *Spammeri* se u ostvarivanju svog napada koriste određenim metodama, a prema Conry-Murrayu (2005) neke od najuobičajenijih metoda su kupovanje popisa e-pošte, strvinari e-

pošte (programi koji pužu Web stranicama u potrazi za adresama e-pošte), krivotvorenje (sakrivanje izvora poruke), *spam proxyji* (poslužitelji e-pošte ili računala koja su oteta za slanje *spama*) te napad po rječniku/žetva imenika. U posljednjoj metodi program kružno prolazi kroz varijante uobičajenih imena, bira određenu domenu kao ciljnu i pokreće program koji zatim šalje ogromne količine poruka e-pošte u nadi da će naciljati dovoljno ispravnih kombinacija imena kojima će se poruke isporučiti (Conry-Murray, 2005, str. 106).

## 3.2. Krađa identiteta

Krađa identiteta također je vrsta računalne prijevare, a označava kopiranje informacija poput brojeva kreditnih računa, lozinki ili drugih osobnih podataka, koji se onda koriste za *online* ili *offline* prijevare (Conry-Murray, 2005, str. 3). Krađa identiteta često je povezana s financijskom dobiti, no koristi se i za stjecanje neovlaštenog ulaska u sustav te određenih privilegija i benefita (Radin, 2016). Prema Conry-Murrayu (2005) identiteti se mogu ukrasti na dva načina. Prvi način označava krađu informacija iz baza podataka banaka, davatelja internetskih usluga, maloprodajnih mjesta, obračunskih ustanova i drugih entiteta koji pohranjuju osobne informacije, a drugi način je da napadač ukrade informacije direktno od korisnika. Drugi način krađe identiteta je manje zahtjevniji i češći, a provodi se putem različitih načina i kombinacija provala kao što su društveni inženjering, *spoofing*, *phishing* napadi i *keystroke loggeri* (Conry-Murray, 2005, str. 10).

### 3.2.1. Društveni inženjering

Društveni inženjering je tehnika manipulacije koja iskorištava ljudsku pogrešku za dobivanje privatnih informacija, pristupa ili dragocjenosti, a u kontekstu kibernetičkog kriminala te vrste prijevare obično namame korisnike da nenamjerno razotkriju podatke, daju pristup ograničenim sustavima ili šire zaraze zlonamjernim softverom (Kaspersky, bez dat.). Napadi pomoću društvenog inženjeringa korisni su u manipulaciji korisnikovim odlukama jer jednom kada napadač shvati što motivira korisnikove radnje, vrlo lako ga može prevariti i izmanipulirati u svoju korist (Kaspersky, bez dat.). Društveni inženjering je danas jedan od najopasnijih vektora napada jer omogućuje značajnu personalizaciju i napadačima otvara puno mogućnosti za daljnje napade (Šolić i Velki, 2018, str. 74).

### 3.2.2. Spoofing

Internetski *spoofing* (podvaljivanje, krivotvorenje) predstavlja „kreiranje lažne ili krivotvorene verzije nečega, poput Web lokacije ili adrese e-pošte“ (Conry-Murray, 2005, str. 12). Primjerice, spoofing napad može izgledati tako da počinitelj korisniku pošalje poruku e-

pošte koja izgleda kao da dolazi od osobe od povjerenja, poput suradnika ili menadžera koji vas je zamolio da mu posudite nešto novaca putem digitalnog bankarstva, dajući uz to uvjerljivo obrazloženje. Ovdje se počinitelj najčešće koristi društvenim inženjeringom kako bi od korisnika dobio povjerenje (Kaspersky, bez dat.).

### 3.2.3. Phishing

*Phishing* je oblik kriminalnog ponašanja, pri kojemu se uz upotrebu informacijskih i komunikacijskih tehnologija te prikrivanjem pravog identiteta pokušavaju ukrasti osjetljivi osobni podaci poput korisničkog imena, lozinke, brojeva kreditne kartice, osobni identifikacijski broj te slični osobni podaci (Bača i Čosić, 2013, str. 155). Termin *phishing* izvedenica je od engl. *fishing* što znači ribarenje ili pecanje što upućuje na „pecanje ili ribolov podataka“ (Bača i Čosić, 2013, str. 155). Prema Conry-Murrayu (2005) *phishing* je jedna od najštetnijih vrsta kibernetičkog napada jer nerijetko kombinira i *spam*, *spoofing* te društveni inženjering. Velik broj *phishing* napada samo započinje tzv. pecačkom porukom, primjerice organizacija kriminalaca pošalje tisuće spam poruka koje izgledaju kao da ih je poslala npr. banka, kompanija za izdavanje kreditnih kartica, davatelj internetskih usluga ili kompanija za e-trgovinu. Te pecačke poruke uglavnom navode kako postoji problem s korisnikovim računom koji se hitno mora riješiti te uključuju poveznicu do Web lokacije koja izgleda kao stvarna Web lokacija kompanije čijim se identitetom kriminalci služe. Ako korisnik klikne na tu poveznicu, preusmjeren je na lažnu stranicu za prijavu s poljima za unos korisničkog imena, lozinke i drugih osjetljivih podataka, koja je ista kao i legitimna stranica. Želeći riješiti navodni „problem“ s računom, korisnik unosi svoje osjetljive podatke koji se prenose na poslužitelj kontroliran od strane kriminalaca te tako bivaju ukradeni (Conry-Murray, 2005, str. 12). No, *phishing* napadi se ne zaustavljaju samo na tome već idu i dalje te u poruke često implementiraju i zlonamjerne softverske programe koji mogu imati različite funkcije. Neki od njih upućuju računala korisnika na *spoofirane* lokacije iako se prilikom pretraživanja u tražilicu upiše točna adresa legitimne lokacije, dok drugi programi mogu bilježiti sve korisnikove pritiske na tipku (*keystroke loggers*). (Conry-Murray, 2005, str. 13).

Posljedice uzrokovane *phishingom* velikih su razmjera i uključuju znatne financijske gubitke, oštećenje ugleda kompanija i krađu identiteta. Primjerice, u Ujedinjenom Kraljevstvu gubitci od prijevara u digitalnom bankarstvu – uglavnom putem *phishing* napada, udvostručili su se s 12,2 milijuna funti u 2004. na 23,2 milijuna funti u 2005. godini (Chawki i sur., 2015, str. 57).

## 3.3. Napadi zlonamjernim programima

Pojam *malware* (kratica od *malicous software*; zlonamjerni softver) opisuje programski kod kreiran s namjerom da našteti vašem računalnom sustavu, a obuhvaća brojne zlonamjerne softvere poput virusa, crva, Trojanskih konja, *spyware* i *adware* tehnologije (Conry-Murray & Weafer, 2005., str. 47). Prema Chawkiu i sur. (2015, str. 40) neki od trendova povezanih s kibernetičkim napadima zlonamjernim softverima su sljedeći:

- Samo mali broj napadača zlonamjernim softverom bude uhvaćeno.
- Državne agencije ne uspijevaju sustići napadače zlonamjernim softverima, a kamo li izgraditi nacionalni obrambeni sustav za zaustavljanje napada.
- Velike organizacije, koje kupuju tehnologiju, zarobljenici su dominantnih tehnoloških tvrtki i imaju malo resursa ili tržišnih alternativa.
- Izabrani javni dužnosnici, od kojih su mnogi primatelji doprinosa od kampanja dominantnih tehnoloških tvrtki iz tog se razloga snažno opiru suočavanju s odgovornosti za proizvod.

Ovlasti za provedbu zakona ne mogu puno pomoći kada je riječ o području računalne sigurnosti i zločina, dok je Vlada, putem provođenja zakona i odgovora na incidente, često spora u reagiranju na navedene trendove. Možda najgore od toga je što dominantne tehnološke kompanije od kojih svi kupuju proizvode, čine vrlo malo za zaštitu korisnika tih proizvoda te stoga teret prouzročen navedenim trendovima na kraju pada na krajnje korisnike računala (Chawki i sur., 2015, str. 40).

### 3.3.1. Virusi

Virus predstavlja „program koji sam sebe replicira u drugim datotekama s kojima dolazi u kontakt“ (Conry-Murray, 2005, str. 50). Ždrnja (2003) navodi kako se virus sastoji od tri glavne komponente: infekcije, nosive komponente i funkcije za okidanje. Infekcija je komponenta u kojoj je napravljen osnovni programski dio koji omogućava širenje virusa, nosiva komponenta predstavlja glavnu komponentu virusa i kada se ona aktivira destruktivni virusi obično čine štetu nad korisnikovim podacima, a treću komponentu predstavlja funkcija za okidanje. Ona definira vrijeme ili događaj pri kojem će biti izvršena nosiva komponenta (Ždrnja, 2003, str. 3).

Kao osnovne vrste virusa mogu se navesti *boot* sektor virusi, programski virusi i makro virusi. *Boot* sektor virusi kopiraju svoj zlonamjerni kod u *Master boot* sektor i tako osiguravaju izvršenje zlonamjernog koda pri svakom pokretanju računalnog sustava.

Programski virusi se aktiviraju pri izvršenju zaražene izvršne datoteke, s najčešćom ekstenzijom .exe ili .com., a makro virusi su virusi napisani višim programskim makro jezikom koji imaju mogućnost kopiranja i brisanja samih sebe te mijenjanja dokumenata (Nacionalni CERT, bez dat.). Makronaredbe mogu se napisati kako bi se pojednostavili neki uobičajeni zadatci unutar većih aplikacija kao što je Microsoft Word. Poznat primjer makro virusa je Melissa virus (Conry-Murray, 2005, str. 51). Melissa virus je otkriven 1999. godine i zbog brzine svog širenja postao je jedan od najpoznatijih virusa te podigao svijest o riziku i potencijalnoj šteti pri otvaranju neželjenih privitaka e-pošte. Virus se širio putem privitaka e-pošte i mogao je onemogućiti brojne zaštitne mjere u Wordu 97 i Wordu 2000 (Gillis, 2021).

### 3.3.2. Crvi

Ždrnja (2003) definira crv kao „samostalni program (ili skup programa) koji je u stanju širiti svoje funkcionalne kopije na druga računala, obično putem računalne mreže“ te napominje kako, za razliku od virusa, crvi ne moraju inficirati nikakvu datoteku na ciljnom računalu, odnosno crvi ne zahtijevaju postojanje domaćinske datoteke za svoj rad već su samostalni programi koji se u većini slučajeva šire bez interakcije korisnika (Nacionalni CERT, bez dat.). Ždrnja (2003) razlikuje dvije vrste crva: crvi bazirani na računalu domaćinu i mrežni crvi. Crvi bazirani na računalu domaćinu nalaze se u potpunosti na računalu na kojem su pokrenuti, a mrežnu komunikaciju koriste samo za širenje na druga računala. S druge strane, mrežni crvi sastoje se od višestrukih dijelova od kojih je svaki pokrenut na posebnom računalu, a računalnu mrežu koriste za komunikaciju između tih dijelova (Ždrnja, 2003, str. 67). Uz širenje putem e-pošte ili sustava za dopisivanje u stvarnom vremenu, neki crvi imaju ugrađene mehanizme pomoću kojih se mogu širiti putem Interneta i lokalnih mreža (Conry-Murray, 2005, str. 51).

### 3.3.3. Trojanski konji

Trojanski konji su vrste zlonamjernih programa koji se „korisnicima predstavljaju kao legitimni i korisni programi,“ iako to nisu, a po tome su i dobili ime Trojanski konj, odnosno prema drvenom konju iz grčke mitologije (Šolić i Velki, 2018, str. 84). Trojanski konj ima mogućnost mijenjanja operacijskog sustava na zaraženom računalu kako bi mogao prikazivati oglase u svrhu ostvarivanja novčane dobiti od strane napadača, no njegova opasnija karakteristika je omogućavanje napadaču potpunu kontrolu nad zaraženim računalom odnosno instaliranje stražnjih vrata (engl. *backdoor*) na računalu korisnika. Time se napadaču otvaraju brojne nove i opasne mogućnosti za druge vrste napada koje mogu uzrokovati veliku

štetu (Nacionalni CERT, bez dat.). Trojanski konji mogu se širiti preuzimanjem zaraženog softvera, kao dio softvera, kao privitci e-pošte, putem zlonamjernih web stranica s dinamičkim sadržajem i preko ranjivosti softvera (Nacionalni CERT, bez dat.).

### 3.3.4. Spyware

*Spyware* se može definirati kao „općenita klasa softverskih programa koji nadziru aktivnosti računala i prenose te informacije na druga računala ili lokacije na Internetu“ (Conry-Murray & Weafer, 2005., str. 71.) *Spyware* ima mogućnost nadziranja korisnikove *online* aktivnosti, provođenja određenih funkcija bez znanja ili pristanka korisnika, zatim može pratiti i izvještavati o svakoj posjećenoj Web lokaciji, generirati iskočne oglase, promijeniti polaznu stranicu i postavke pretraživača ili bilježiti pritisnutu tipku pomoću *keystroke logger* programa (Conry-Murray & Weafer, 2005., str. 67). *Keystroke logger* je jedna od podvrsti *spywarea* i označuje program koji bilježi sve pritiske na tipke tipkovnice kako bi zatim prikupljene informacije slao udaljenom napadaču koji ih potom skenira u svrhu pronalaženja i krađe osjetljivih podataka poput lozinki i brojeva računa (Conry-Murray & Weafer, 2005., str. 13). *Spyware* se razlikuje od virusa ili crva u tome što ne replicira sam sebe te mu često nije u cilju zaraziti što više računala, već odabire određene mete, a uobičajeno se instalira pomoću trojanskoga konja koji uglavnom uključuje i neku vrstu društvenog inženjeringa (Šolić i Velki, 2018, str. 86). Jedna od podvrsti *spywarea* je i *adware*, program koji je dizajniran da isporučuje ciljano oglašavanje na korisnikov Web pretraživač, posebice pomoću iskočnih oglasa (Šolić i Velki, 2018, str. 67).

### 3.3.5. Ransomware

*Ransomware* se može definirati kao „vrsta zloćudnog koda koji šifrira podatke na žrtvinom računalu i traži novčanu otkupninu kako bi ih se dešifriralo“ (Šolić i Velki, 2018, str. 86). Među poznatijim primjerima *ransomware* napada je „WannaCry“ napad iz 2017. godine. CERT (2012) navodi kako se napad dogodio 12. svibnja 2017. godine i zarazio preko 75 000 računala diljem svijeta. Jedna od pogođenih organizacija bio je sustav javnog zdravstva u Ujedinjenom Kraljevstvu (National Health Service), zatim tvrtka koja upravlja željezničkom infrastrukturom u Njemačkoj (Deutche Bahn), multinacionalni pružatelj telekomunikacijskih usluga (Telefonica), tvrtka koja pruža usluge dostave (FedEx) te brojne druge organizacije. Napad se nastavio i nakon 12. svibnja te je na kraju bilo oko 200 000 žrtava u preko 150 zemalja. Iza tog napada stoje dvije hakerske grupe; Equation i Shadow Brokers grupa. National Security Agency (NSA) obavještajna je agencija SAD-a, a njezin

navodni tajni dio naziva se Office of Tailored Acces Operations (TAO) koji napadima na računalne sustave i mreže prikuplja informacije. Equation grupa kodno je ime za hakersku grupu koju sigurnosni stručnjaci povezuju s TAO-om, od koje je hakerska grupa nepoznatog sastava Shadow Brokers ukrala kibernetička oružja, odnosno alate za kompromitaciju računala te ih javno objavila. Mjesec dana nakon objave alata, točnije 12. svibnja 2017., pojavile su se prve zaraze WannaCry inačicom 2.0 s mogućnošću automatskog širenja mrežom pomoću alata EternalBlue i DoublePulsar. Ta dva alata iznimno su opasna i destruktivna jer omogućuju potpunu kontrolu nad računalom i čine napad izrazito teško primjetljivim (Nacionalni CERT, 2012).

### 3.3.6. DoS napad

DoS (*denial of service attack*) napad je vrsta napada „koji poslužitelj optereti velikim brojem zahtjeva za pružanjem usluge pa legitimni zahtjevi ne dospiju biti zadovoljeni“ (Conry-Murray, 2005, str. 223). Podtip ovog napada je i DDos (distributed denial of service attack) napad ili distribuirani napad uskraćivanja usluga. On „nastaje kada više prethodno kompromitiranih sustava poplavljuje resurse ciljanih sustava, obično jednog ili više web poslužitelja“ (Nacionalni CERT, 2008).

# 4. Utjecaj pandemije koronavirusa

Novi koronavirus, nazvan SARS-CoV-2 (*Severe Acute Respiratory Syndrome Coronavirus-2*) otkriven je u Kini krajem 2019. godine. Radi se o novom soju koronavirusa koji prije nije bio otkriven kod ljudi. COVID-19 je naziv bolesti uzrokovane SARS-CoV-2 (Hrvatski zavod za javno zdravstvo [HZJZ], 2021). Zbog porasta broja slučajeva do globalnih razmjera, diljem svijeta uvedene su mjere za ograničavanje širenja koronavirusa. Uvođenje potpunih ili djelomičnih zatvaranja (engl. *lockdown*) dovelo je do većeg provođenja vremena kod kuće pa tako i na internetu bilo radeći od kuće, zbog online nastave ili općenitog pretraživanja interneta (Europski parlament, 2020). Kao posljedica toga, sve više i više privatnih računala, koja su najčešće manje zaštićena nego ona koja se koriste na radnim mjestima, koristi se za rad od kuće. Također, raste i korištenje društvenih mreža, *streaming* i *cloud* usluga, elektroničke pošte, alata za video konferencije i sl. te se tako stvara veći rizik od kibernetičkih napada (Wiggen, 2020).

Procjena prijetnje od organiziranog kriminaliteta (Internet organised crime threat assessment, IOCTA) Europolov je vodeći strateški proizvod koji ističe dinamične i razvojne prijetnje koje predstavlja kibernetički kriminal. U procjeni iz 2020. godine, Europol (2020) ukazuje na to da su osnove kibernetičkog kriminala čvrsto ukorijenjene što ne znači da kibernetički kriminal miruje, već je njegov razvoj uočljiviji u detaljnijem istraživanju kibernetičkih trendova, odnosno u načinima na koje kibernetički kriminalci konstantno usavršavaju svoje metode te ih čine svima dostupnima. Europol (2020) navodi kako se to posebno da primijetiti tijekom krize izazvane pandemijom koronavirusa u načinu na koji kibernetički kriminalci aktivno iskorištavaju društvo kada je ono najranjivije. Kroz različite vrste napada, poput društvenog inženjeringa, distribuiranog napada uskraćivanjem usluga, *ransomware* napada te distribucije materijala seksualnog iskorištavanja djece, kibernetički kriminalci iskoristili opću nesigurnost te društvenu potrebu za pouzdanim i relevantnim informacijama uzrokovanu koronakrizom te oblikovali postojeće strategije napada kako bi što bolje iskoristili tu krizu (Europol, 2020, str. 6). Uz navedene zaključke, Europol (2020) napominje kako je pandemija uzrokovala potenciranje postojećih problema zbog znatnog povećanja ljudi koji rade od kuće te da to ne bi trebalo zasjeniti cjelokupnost prijetnji na području kibernetičkog kriminala (Europol, 2020, str. 6).

Utjecaj pandemije na kibernetički kriminal najviše se može vidjeti u području seksualnog zlostavljanja i iskorištavanja djece u kojemu je primjetan konstantni porast materijala, pogoršan koronakrizom. Neke od država članica Europske unije prijavile su porast blokiranih pokušaja pristupa web stranicama koje sadrže seksualno iskorištavanje djece te porast u detektiranom sadržaju seksualnog iskorištavanja djece na *peer-to-peer* (p2p) mrežama za vrijeme uvođenja mjere potpunog ili djelomičnog zatvaranja (Europol, 2020, str. 6).

Još jedan trend uzrokovan pandemijom je porast širenja dezinformacija što pripada vrsti hibridnih prijetnji, iznosi Europol (2020). Zbog prezasićenosti dostupnim informacijama i nedostatka pouzdanih izvora vijesti i informacija, ljudi postaju ranjivi na vjerovanje dezinformacijama koje se mogu povezati s nastojanjima kibernetičkih kriminalaca da učine društveni inženjering te *phishing* napade učinkovitijima. U kontekstu pandemije, zabilježen je porast širenja lažnih vijesti o potencijalnim lijekovima za COVID-19 koje su također omogućile profit kriminalcima koji prodaju predmete za koje tvrde da će spriječiti ili izliječiti COVID-19 (Europol, 2020, str. 13).

Nadalje, Europol (2020) naglašuje da *ransomware* napadi ostaju najdominantnija prijetnja i u 2020. godini te da *ransomware* napadači nastavljaju ciljati javne i privatne organizacije različitih veličina te industrije, radije nego osobna računala. S obzirom na to da su *ransomware* napadi na zdravstvenu industriju zabilježeni i prije koronakrize, ona nije okidač takvih vrsta napada, već je samo donijela više prilika za napade. Razlog tomu je porast broja računala zaposlenika koji su daljinski povezani s i imaju pristup infrastrukturama informacijske tehnologije svojih kompanija, a s obzirom na nedostatak sigurnosnih metoda na osobnim računalima zaposlenika, stvara se rupa u sigurnosti kompanija (Europol, 2020, str. 25). Europol (2021) u svojoj procjeni iz 2021. godine ukazuje kako COVID-19 i dalje ima značajan utjecaj na područje online prijevare i bilježi slične trendove i u drugoj godini pandemije.

Osim Europola, Interpol također proučava povezanost kibernetičkog kriminala s pojavom pandemije koronavirusa. Na temelju pristupa podatcima iz zemalja članica i privatnih partnera, Interpol (2020) je sastavio Izvješće o procjeni kibernetičkog kriminala povezanog s pandemijom kako bi pružio sveobuhvatan pregled trendova u kibernetičkom kriminalu usred pandemije. Na temelju analize dobivenih podataka, glavne prijetnje povezane s pandemijom koronavirusa su *online* prijevara i *phishing*, zatim ometajući zlonamjerni

programi (*ransomware* i distribuirani napad uskraćivanjem usluga), zlonamjerni programi za prikupljanje podataka, zlonamjerne domene i dezinformacije (Interpol, 2020).

*Online* prijevara i *phishing* po rezultatima zauzimaju prvo mjesto po učestalosti napada iz te kategorije. Pomoću uvođenja tematike povezane s COVID-19 u *phishing* poruke elektroničke pošte, kibernetički kriminalci navode žrtve na otkrivanje osobnih podataka i skidanje malicioznog sadržaja. Prilikom toga, kriminalci se često lažno predstavljaju kao državni službenici ili legitimni članovi zdravstvenih organizacija (Interpol, 2020, str. 8). Prema podacima dobivenim od država članica Interpola te njihovih privatnih partnera, najčešće teme u *phishing* napadima su:

- E-poruke nacionalnih ili globalnih zdravstvenih institucija
- Vladine naredbe i inicijative za financijsku potporu
- Lažni zahtjevi za plaćanje i povrat novca
- Ponude cjepiva i medicinskih potrepština
- Aplikacije za mobilne telefone za praćenje COVID-19
- Ponude za ulaganja i dionice
- Zahtjevi za dobrotvorne svrhe i donacije povezani s COVID-19

Sljedeća kategorija kibernetičkog kriminala koja prema Interpolu (2020) bilježi porast uključuje ometajuće zlonamjerne programe, točnije *ransomware* i distribuirani napad uskraćivanjem usluga. Kibernetički kriminalci, pokušavajući ostvariti financijsku dobit, koriste zlonamjerne programe za napade na kritične infrastrukture i zdravstveni sustav koji je već preplavljen zbog zdravstvene krize (Interpol, 2020, str. 10). Uz *ransomware* i *DDOS***,** napadi ostalim vrstama zlonamjernih programa poput Trojanskog konja, *spywarea*, bankovnih Trojanaca i dr., također bilježe porast. Isporuka tih zlonamjernih programa uvelike je omogućena kroz COVID-19 *phishing* kampanje. Jedan od najizrazitijih zlonamjernih softvera za prikupljanje podataka je tzv. Emotet, čije se širenje znatno povećalo s početkom pandemije i koji se širio putem privitaka e-pošte koji su tvrdili da sadrže mjere prevencije COVID-19, a umjesto toga sadržavali su Emotet (Interpol, 2020, str. 10-12).

Nadalje, bilježi se porast u registriranim zlonamjernim domenama s ključnim riječima „koronavirus“ ili „COVID“ koje kibernetički kriminalci stvaraju iskorištavajući povećanu potražnju informacija i vijesti o koronavirusu (Interpol, 2020, str. 10). Krajem ožujka 2020. godine zabilježeno je 116 357 COVID-19 novoregistriranih domena, od kojih je 2022 identificirano kao zlonamjerne domene, a 40 261 kao visokorizične domene. U lipnju 2020.,

Interpol je identificirao i analizirao 200 000 zlonamjernih domena koje utječu na više od 80 zemalja članica (Interpol, 2020, str. 11).

Kao posljednju prijetnju vezanu uz pojavu pandemije, Interpol (2020) navodi rastuću količinu širenja dezinformacija i lažnih vijesti. Neke od najčešćih tema vezanih uz širenje lažnih informacija o koronavirusu su akcije koje vlasti poduzimaju oko pandemije, opće medicinske vijesti, teorije zavjera, način prijenosa virusa, razvoj cjepiva i sl. Dezinformacije o tim temama uglavnom se dijele putem društvenih mreža (Interpol, 2020, str. 13). Interpol zaključuje kako je zabilježeni porast kibernetičkih napada u doba koronakrize stvorio priliku za razmišljanje o trenutnim mogućnostima i resursima dostupnima za poboljšanje kako bi se postigla bolja spremnost i otpornost na napade u budućnosti, kao i važnost konkretnog globalnog odgovora na suradnički i koordiniran način (Interpol, 2020, str. 19).

Nadalje, WHO (2020) također bilježi dramatičan porast broja *cyber* napada usmjerenih na svoje osoblje i prijevara putem e-pošte usmjerenih na širu javnost od početka pandemije COVID-19. WHO (2020) navodi kako je u travnju 2020. godine, u samo jednom tjednu procurilo oko 450 njihovih aktivnih adresa e-pošte i lozinki. Informacije koje su procurile nisu dovele sustav WHO-a u opasnost jer su podaci bili stariji, ali napad je utjecao na jedan stariji sustav, koji koristi sadašnje i umirovljeno osoblje, kao i partneri. Osim toga, WHO (2020) porast bilježi i u lažnim porukama e-pošte poslanima javnosti od strane kriminalaca, u kojima se lažno predstavljaju kao WHO. Kao odgovor na problem, WHO radi s privatnim sektorom na uspostavi snažnijih internih sustava i jačanju sigurnosnih mjera te educira osoblje o rizicima kibernetičke sigurnosti (World Health Organisation [WHO], 2020).

Buil-Gil, Díaz-Castaño, Kemp, Miró-Llinares i Moneva (2021) u svome članku istražuju potencijalni utjecaj COVID-19 pandemije na kibernetičke zločine prijavljene vlastima u razdoblju najstrožih mjera izolacije (engl. *lockdown*) u Ujedinjenom Kraljevstvu, uspoređujući podatke o prijavljenim online prijevarama i kibernetičkim zločinima koji su zabilježeni u svibnju 2020. godine te godinu dana prije, odnosno prije pandemije. Njihovo se istraživanje temelji na podacima prikupljenima od strane nacionalnog centra za prijavu kibernetičkog kriminala (Action Fraud) u Ujedinjenom Kraljevstvu, koji je od lipnja 2020. godine počeo objavljivati mjesečne statističke podatke o prijevarama i kibernetičkom kriminalu poznatima policiji. Vrste kibernetičkih napada koje su autori analizirali su virusi, napadi zlonamjernim softverima, *spyware*, napadi uskraćivanjem usluga, hakiranje servera/osobnih računala/društvenih mreža/e-pošte/privatnih telefonskih centrala (engl.

Private Branch Exchange – PBX), hakiranje u kombinaciji s ucjenom te online prijevare uključujući online kupovinu i aukcije (Buil-Gil i sur., 2021).

U Ujedinjenom Kraljevstvu prve mjere izolacije najavljene su 23. ožujka, nova ograničenja dodana su u travnju, dok su najstrože mjere izolacije u donesene u travnju i svibnju 2020. godine, stoga su autori uspoređivali statističke podatke o kibernetičkim zločinima iz svibnja 2019. godine, odnosno prije pandemije te iz svibnja 2020. godine, odnosno za vrijeme mjera izolacije te izračunali postotak relativne promjene između broja zločina zabilježenih u ta dva mjeseca (Buil-Gil i sur., 2021). Uz to, autori napominju kako podaci korišteni u njihovom članku uključuju kibernetičke zločine koji su poznati vlastima u Ujedinjenom Kraljevstvu odnosno podatke iz policijski evidentiranih kaznenih djela, dakle pogreške u mjerenjima mogu proizlaziti iz nedostatka podataka o neprijavljenim kibernetičkim napadima.

Tablica 1. uspoređuje *cyber*-ovisni kriminal i online prijevare zabilježene u svibnju 2019. i svibnju 2020. te izračunava relativnu promjenu između te dvije vrijednosti za svaku vrstu kriminala (Buil-Gil i sur., 2021). Iz tablice 1. se primjećuje kako većina promatranih vrsta kriminala bilježi porast između dvije godine, od kojih najveću učestalost bilježi hakiranje osobnih računala, hakiranje društvenih mreža i e-pošte te online prijevara. Također je vidljivo kako računalni virusi/*malware*/*spyware*, hakiranje privatnih telefonskih centrala i hakiranje u kombinaciji s ucjenom bilježe pad između dviju opserviranih godina (Buil-Gil i sur., 2021). Autori objašnjavaju kako na smanjen broj hakiranja privatnih telefonskih centrala može utjecati mali broj registriranih slučajeva, stoga ti podaci nisu toliko statistički značajni. Kod računalnih virusa, autori napominju kako je broj prijava iz svibnja 2019. (742) najveći broj prijava virusa te godine i izrazito veći u usporedbi s prosječnim brojem prijava po mjesecu iz 2019. godine. Isto tako, najveći broj prijavljenih računalnih virusa od travnja 2019., zabilježen je u travnju 2020. (818), te najveći broj prijavljenog hakiranja u kombinaciji s ucjenom evidentiran je također u travnju 2020. (1058 prijava), u doba kada su već bile na snazi stroge mjere izolacije (Buil-Gil i sur., 2021).

Tablica 1. *Cyber*-ovisni kriminal i *online* prijevare zabilježene u svibnju 2019. i svibnju 2020. (Buil-Gil i sur., 2021)

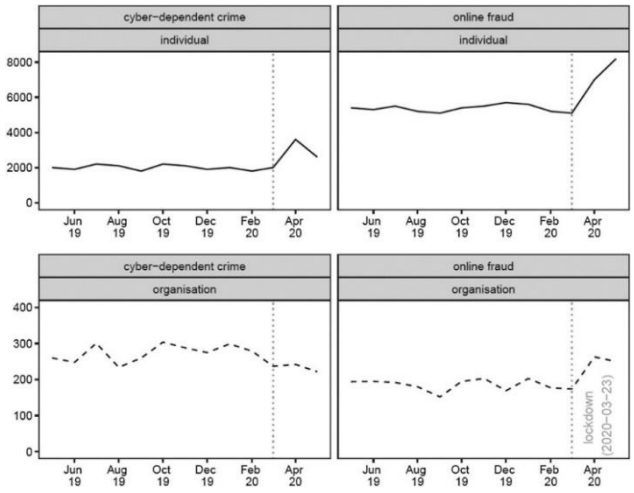
| | **Broj u svibnju 2019.** | **Broj u svibnju 2020.** | **Relativna promjena (%)** |
|---|---|---|---|
| Računalni virusi/*malware*/*spyware* | 742 | 648 | −12.67 |
| Napadi uskraćivanjem usluga | 14 | 18 | 28.57 |
| Hakiranje – serveri | 24 | 25 | 4.17 |
| Hakiranje – osobna računala | 270 | 479 | 77.41 |
| Hakiranje – društvene mreže i e-pošta | 939 | 1,449 | 54.31 |
| Hakiranje – privatne telefonske centrale | 9 | 7 | −22.22 |
| Hakiranje u kombinaciji s ucjenom | 313 | 251 | −19.81 |
| *Online* prijevara – *online* kupovina i aukcije | 5,619 | 8,482 | 50.95 |
| Sve vrste | 7,930 | 11,359 | 43.24 |

Uz navedene rezultate, Buil-Gil i sur. (2021) napominju kako neke od vrsta kibernetičkog kriminala koje u tablici 1. bilježe pad, češće pogađaju organizacije u odnosu na pojedince, stoga u tablici 2. autori promatraju trendove porasta/pada prijava određenih vrsta kibernetičkih kriminala kod pojedinaca kao i kod organizacija. U tablici 2. vidljivo je kako je broj prijavljenih *cyber*-ovisnih zločina nad pojedincima veći u svibnju 2020. nego u svibnju 2019. godine, dok je kod organizacija broj prijava iste vrste kibernetičkih zločina manji u svibnju 2020. godine (Buil-Gil i sur., 2021). Zatim, kod *online* prijevara, broj slučajeva raste i kod organizacija i kod pojedinaca, točnije kod pojedinaca se bilježi znatni porast u odnosu na svibanj prethodne godine.

Tablica 2. *Cyber*-ovisni zločini i *online* prijevare nad pojedincima i organizacijama u svibnju 2019. i svibnju 2020. (Buil-Gil i sur., 2021)

| | | **Broj u svibnju 2019.** | **Broj u svibnju 2020.** | **Relativna promjena (%)** |
|---|---|---|---|---|
| Cyber-*ovisni zločini* | Pojedinci | 2,300 | 2,643 | 14.91 |
| | Organizacije | 260 | 222 | −14.62 |
| *Online* prijevara – *online* kupnja i aukcije | Pojedinci | 5,408 | 8,220 | 51.99 |
| | Organizacije | 194 | 250 | 28.87 |
| Sve vrste | Pojedinci | 7,708 | 10,863 | 40.93 |
| | Organizacije | 454 | 472 | 3.96 |

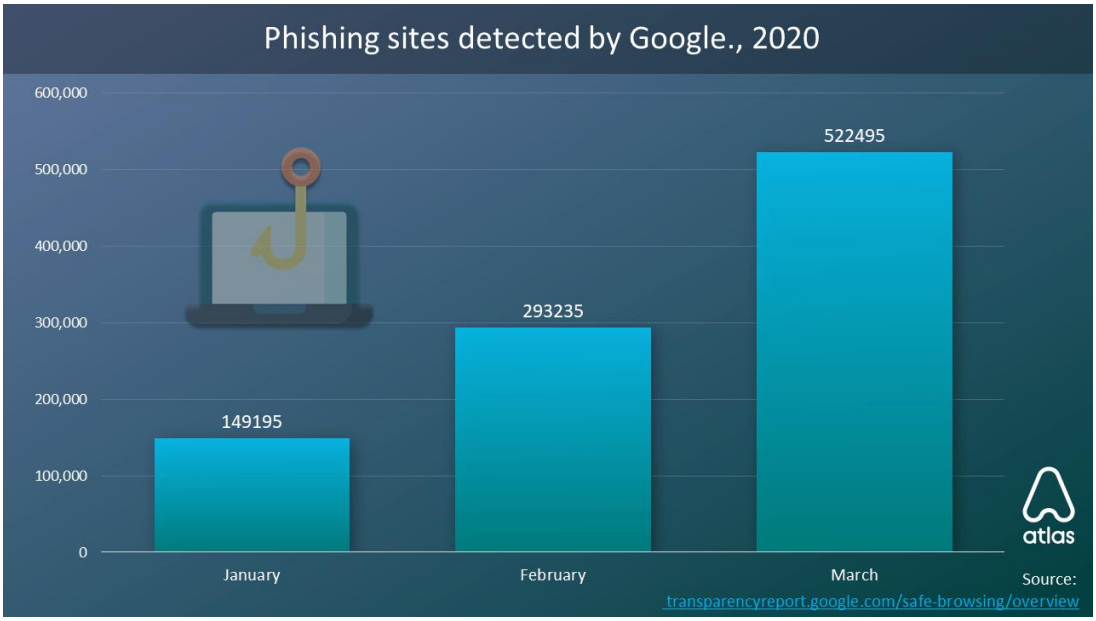
Međutim, Buil-Gil i sur. (2021) napominju kako je uz usporedbu trendova zločina između dva mjeseca potreban i dodatan kontekst u smislu usporedbe tih trendova s ukupnim vremenskim obrascem između dvaju promatranih mjeseca. Kao što je naznačeno na slici 1., broj *cyber*-ovisnih zločina nad pojedincima dosegnuo je vrhunac u travnju 2020. te bio izrazito visok u svibnju 2020. godine u usporedbi s ostalim mjesecima, dok broj istih zločina nad organizacijama bilježi pad u istom tom razdoblju (Buil-Gil i sur., 2021). Broj internetskih prijevara povezanih s online kupnjom i aukcijama također doseže vrhunac u travnju i svibnju 2020. godine – u razdoblju najstrožih mjera izolacija, no ovaj put porast u tim mjesecima se bilježi i kod pojedinaca i kod organizacija (Buil-Gil i sur., 2021).




Slika 3. Broj *cyber*-ovisnih zločina i *online* prijevara po tipu žrtve od svibnja 2019. do svibnja 2020. (Buil-Gil i sur., 2021)

Buil-Gil i sur. (2021) zaključuju kako dolazi do porasta prijava kibernetičkog kriminala tijekom izbijanja COVID-19 pandemije s posebno visokim stopama zločina za vrijeme najstrožih mjera izolacije odnosno potpunog zatvaranja. Porast u prijavama *online* prijevara autori zapažaju i kod pojedinaca i organizacija, dok se porast *cyber*-ovisnih zločina primjećuje najviše kod pojedinaca. Autori nagađaju da je razlog tomu veliki broj poduzeća koja su u potpunosti ili na neko vrijeme prestala s radom za vrijeme pandemije, stoga se u napadima više cilja na pojedince (Buil-Gil i sur., 2021).

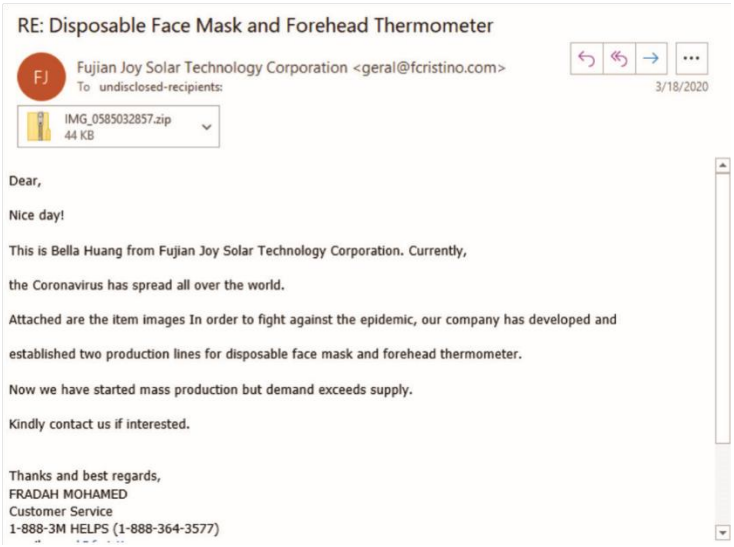
Prema podacima o *phishing* web-mjestima koje je Google detektirao tijekom siječnja, veljače i ožujka 2020. godine, bilježi se porast broja *phishing* web stranica za 350% u vrijeme najstrožih mjera izolacija i potpunih zatvaranja. Kao što je vidljivo na slici 2., u siječnju 2020. godine, Google je registrirao ukupno 149 195 aktivnih web stranica za krađu identiteta. U veljači iste godine taj broj je narastao na 293 235, dok je u ožujku dosegnuo brojku od ukupno 522 495 registriranih *phishing* web stranica, što je u usporedbi s podacima iz siječnja porast od 350% (Atlas VPN, 2020).



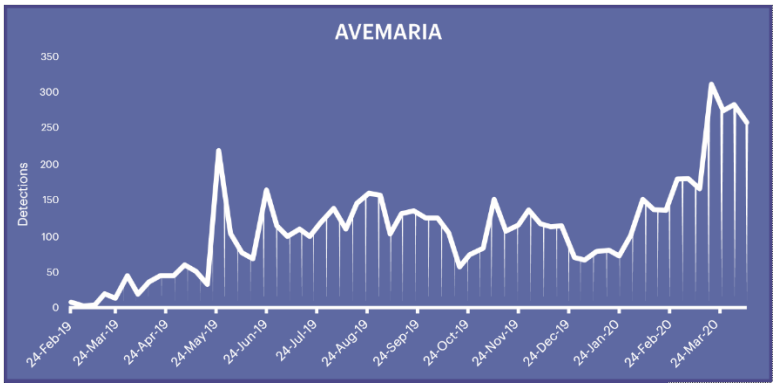

Slika 4. *Phishing* web stranice detektirane u 2020. godini (Atlas VPN, 2020)

Zatim, tvrtka za kibernetičku sigurnost, Malwarebytes (2020), u svojem izvješću za razdoblje od siječnja 2020. do ožujka 2020. godine, istražuje najrasprostranjenije primjere zlonamjernih softvera koje koriste COVID-19 tematske kampanje za svoje širenje. Jedan

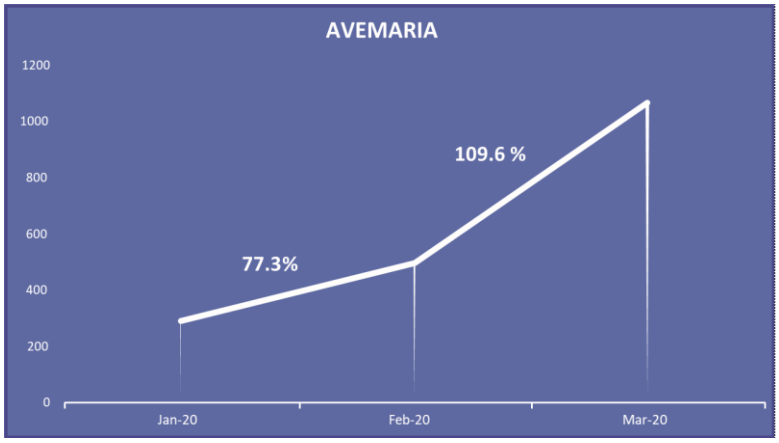
takav primjer je Trojanski konj s udaljenim pristupom (engl. *Remote Access Trojan*, RAT) pod nazivom AveMaria, koji preuzima sustave i pruža napadačima mogućnost udaljenog pristupa, daljinsko upravljanje web kamerom, krađu lozinke, skidanje nepoželjnih datoteka, bilježenje svih pritisaka tipki tipkovnice (*keylogger*), itd. Prvi put je uočen 2018. godine, a njegova nedavna aktivnost uključuje širenje putem zlonamjernih *phishing* poruka e-pošte koje sadržavaju informacije o učinkovitim maskama za lice i sličnim temama vezanima uz COVID-19, kao što je prikazano slici 3. Slike 4. i 5. pokazuju porast širenja AveMaria trojanca u vrijeme pojave pandemije koronavirusa, s porastom od 109,6 % između veljače i ožujka 2020. godine (Malwarebytes, 2020).




Slika 5. *Phishing* poruka e-pošte koja sadrži AveMaria RAT (Malwarebytes, 2020)

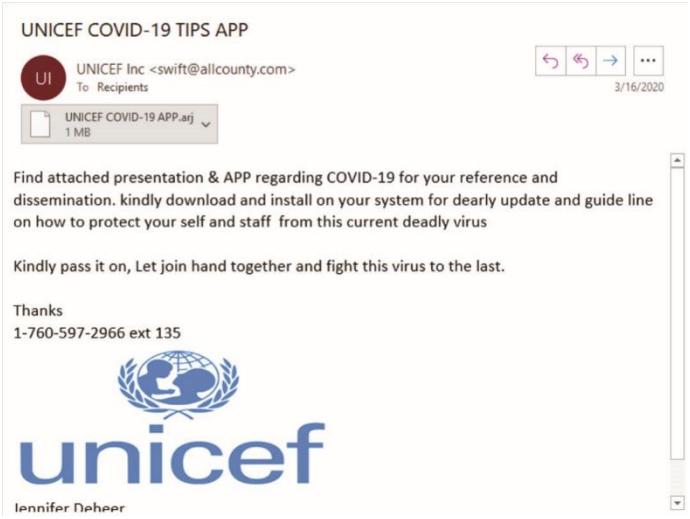



Slika 6. Detekcija aktivnosti AveMaria *malwarea* u razdoblju od veljače 2019. do ožujka 2020. (Malwarebytes, 2020)

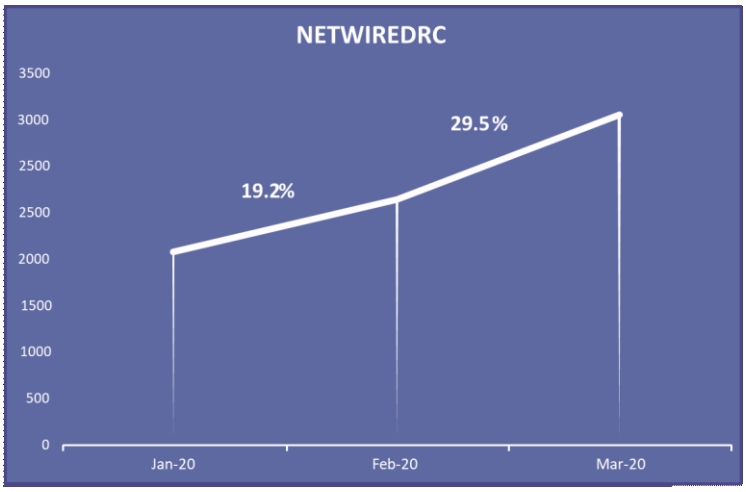



Slika 7. Promjena postotka pojave AveMaria *malwarea* od siječnja 2020. do ožujka 2020. (Malwarebytes, 2020)

Još jedan primjer zlonamjernog programa koji koristi koronakrizu je NetWiredRC, koji je otkriven 2014. godine i iznimno je opasan jer ima sposobnost manipulacije sustavom, špijuniranja te krađe podataka i aplikacija od korisnika (Malwarebytes, 2020). Kao kod prethodnog primjera, autori navode kako se ova vrsta zlonamjernog programa također širi putem e-pošte, koristeći se COVID-19 tematikom. Na slici 6. nalazi se primjer poruke e-pošte u kojoj se napadači predstavljaju kao UNICEF organizacija koja pruža informacije o COVID-19, a zapravo sadrži NetWiredRC. Slika 7. prikazuje postotak pojave NetWiredRCa od siječnja 2020. do ožujka 2020. te ukazuje na porast od otprilike 40% od početka godine (Malwarebytes, 2020).



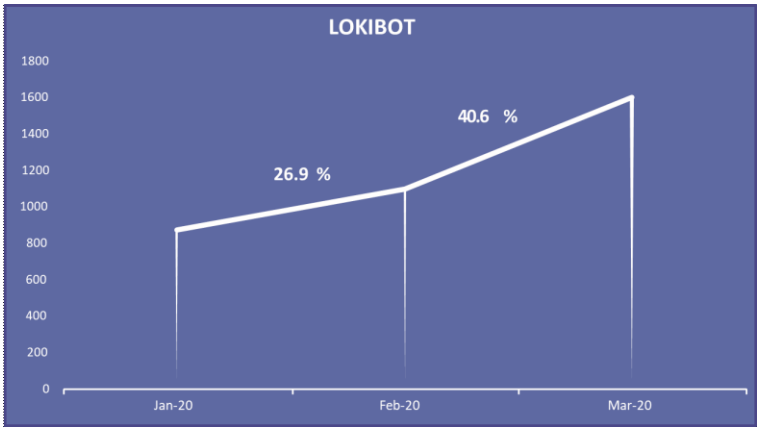

Slika 8. Poruka e-pošte koja se lažno predstavlja kao UNICEF šireći NetWiredRC (Malwarebytes, 2020)




Slika 9. Promjena postotka pojave NetWiredRC *malwarea* od siječnja 2020. do ožujka 2020. (Malwarebytes, 2020)

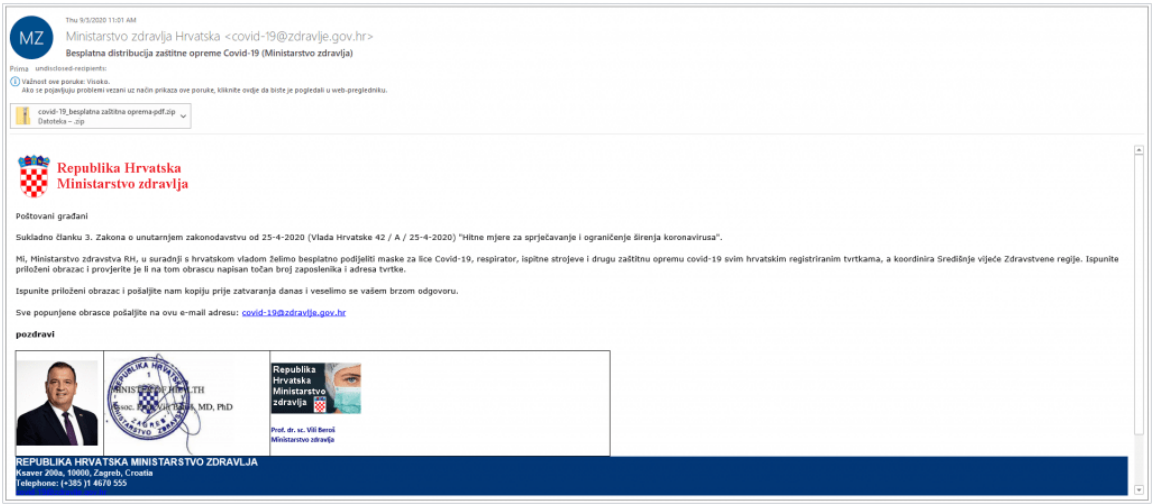
Zatim, LokiBot je poznati primjer *botneta* koji je aktivan od 2015. godine te se sada ponovo bilježi njegov porast u širenju kroz COVID-19 kampanje kao što je vidljivo na slici 8. (Malwarebytes, 2020). *Botnet* je naziv za „skup uređaja povezanih s internetom, koji mogu uključivati osobna računala, poslužitelje, mobilne uređaje i Internet stvari, koji su zaraženi i kontrolirani uobičajenom vrstom zlonamjernog softvera, često bez znanja njihovog vlasnika“ (Lutkevich, Terrell Hanna i Wright, 2021). LokiBot ima mogućnost krađe lozinka te je ujedno i *keylogger*. Na slici 9. vidljiv je porast detekcije LokiBot *botneta* za otprilike 60% od siječnja do ožujka 2020. godine.


Slika 10. LokiBot u privitku poruke e-pošte s COVID-19 tematikom (Malwarebytes, 2020)



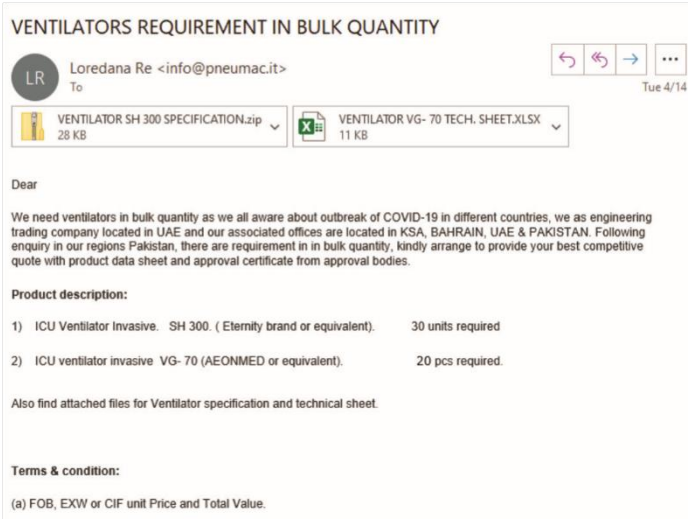

Slika 11. Promjena postotka pojave LokiBot *malwarea* od siječnja 2020. do ožujka 2020. (Malwarebytes, 2020)

O napadu LokiBot zlonamjernom softveru, koji se koristi COVID-19 tematikom, izvijestio je Nacionalni CERT (2020). Upozorenje o phishing kampanji vezanoj uz COVID-19, Nacionalni CERT objavio je 3. rujna 2020. godine. Napadač se predstavljao kao Ministarstvo zdravlja te u privitku e-pošte nalazila se .zip datoteka koja je sadržavala zlonamjerni LokiBot sadržaj. Na slici 10. nalazi se prikaz takve *phishing* poruke e-pošte (Nacionalni CERT, 2020).




Slika 12. LokiBot u privitku poruke e-pošte s lažnim predstavljanjem kao Ministarstvo zdravlja (Nacionalni CERT, 2020)

Sljedeći primjer zlonamjernog softvera koji iskorištava pojavu pandemije koronavirusa za svoje širenje je AZORult. AZORult je opasni zlonamjerni softver koji postoji od 2016. godine i koji se primarno širi putem *phishing* poruka. Slika 10. sadrži *phishing* poruku e-pošte na temu COVID-19, u čijem se privitku nalazi AZORult. Njegove mogućnosti uključuju krađu lozinke i kriptovaluta te se može ponašati kao sredstvo za skidanje drugih zlonamjernih programa (Malwarebytes, 2020).


VENTILATORS REQUIREMENT IN BULK QUANTITY

LR Loredana Re <info@pneumac.it>
To
Tue 4/14

VENTILATOR SH 300 SPECIFICATION.zip 28 KB
VENTILATOR VG- 70 TECH. SHEET.XLSX 11 KB

Dear

We need ventilators in bulk quantity as we all aware about outbreak of COVID-19 in different countries, we as engineering trading company located in UAE and our associated offices are located in KSA, BAHRAIN, UAE & PAKISTAN. Following enquiry in our regions Pakistan, there are requirement in in bulk quantity, kindly arrange to provide your best competitive quote with product data sheet and approval certificate from approval bodies.

**Product description:**

1) ICU Ventilator Invasive. SH 300. ( Eternity brand or equivalent). 30 units required

2) ICU ventilator invasive VG- 70 (AEONMED or equivalent). 20 pcs required.

Also find attached files for Ventilator specification and technical sheet.

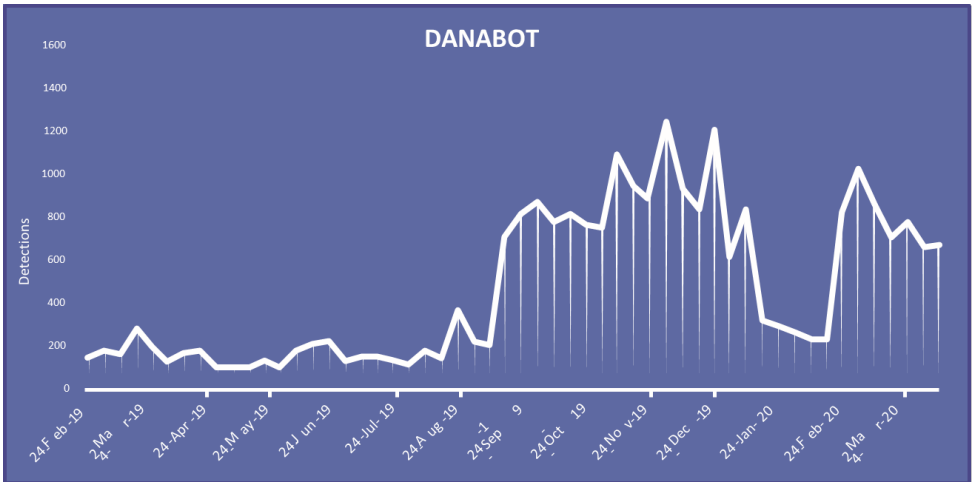
**Terms & condition:**

(a) FOB, EXW or CIF unit Price and Total Value.

Slika 13. AZORult u privitku poruke e-pošte s COVID-19 tematikom (Malwarebytes, 2020)

Malwarebytes (2020) navodi kako širenje AZORult *malwarea* teče kontinuirano kroz 2019. godinu sve do studenog kada se bilježi veći pad koji je trajao do otprilike veljače u 2020. godini, što je vidljivo na slici 11., te zaključuju kako je AZORult prijetnja koja najvjerojatnije neće uskoro nestati. (Malwarebytes, 2020).

Posljednji primjer zlonamjernog softvera kojeg autori navode je DanaBot. DanaBot je vrsta bankovnog trojanca koji je primarno bio raširen u Australiji, no kasnije se proširio i u ostale dijelove svijeta. To je zlonamjerni program koji krade bankovne vjerodajnice, lozinke, identitet te ima mogućnost manipulacije preglednikom, a može služiti i kao sredstvo za skidanje drugih zlonamjernih programa. Iz slike 11. vidljivo je kako DanaBot bilježi porast aktivnosti u rujnu 2019. godine, nakon čega slijedi najprije pad aktivnosti u siječnju 2020. godine te nakon toga ponovni nagli porast između veljače i ožujka 2020. godine (Malwarebytes, 2020).

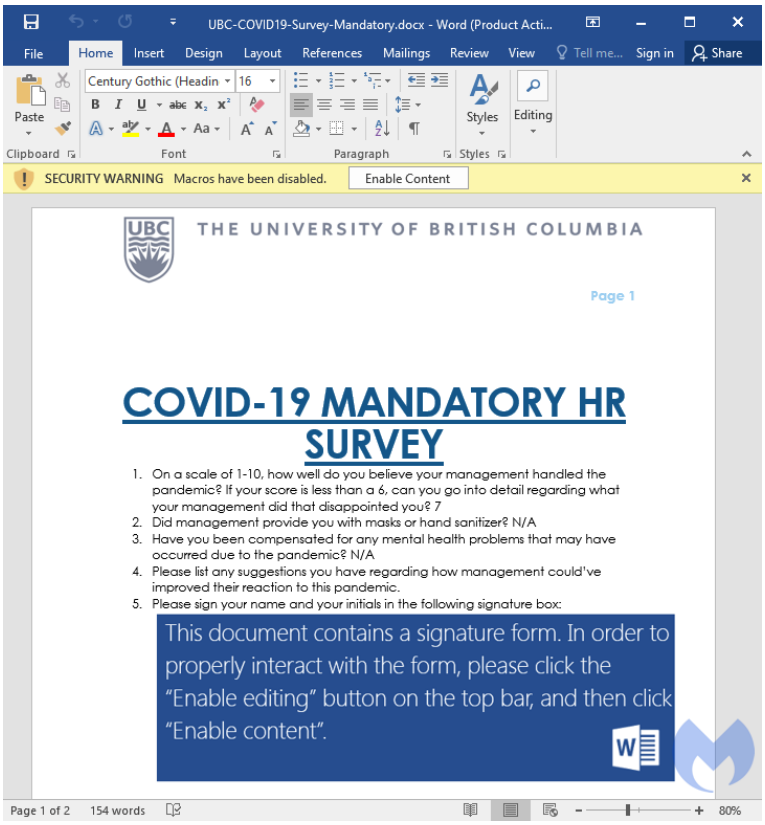



Slika 14. Detekcija aktivnosti DanaBot *malwarea* u razdoblju od veljače 2019. do ožujka 2020. (Malwarebytes, 2020)

Poljska CERT organizacija nedavno je poslala upozorenje svojim građanima o kampanji kojom se kroz PowerPoint prezentacije širi DanaBot *malware*. Također, DanaBot je jedna od komponenata koje se instaliraju na korisnikovo računalo pomoću lažne koronavirus karte Sveučilišta Johns Hopkins, prikazane na slici 12., koja se prvi put pojavila u ožujku 2020. godine (Malwarebytes, 2020).

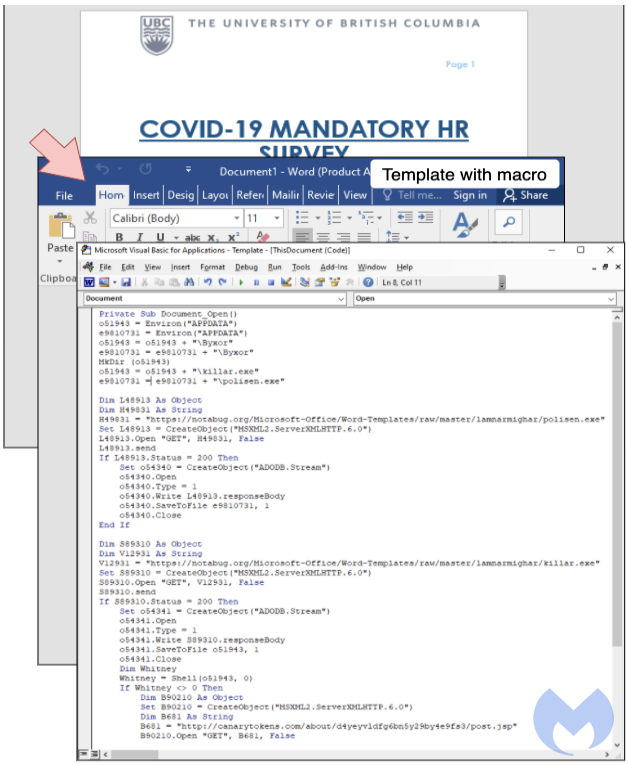

Slika 15. Lažna karta koronavirusa Sveučilišta Johns Hopkins koja se koristi za širenje zlonamjernog softvera poput DanaBota (Malwarebytes, 2020)

Napad na osoblje Sveučilišta British Columbia (UBC) pomoću *phishing* dokumenta s lažnom COVID-19 anketom još je jedan od konkretnih primjera napada koji iskorištavaju kriznu situaciju pandemije koronavirusa. Napad se dogodio u listopadu 2020. godine, a izvršen je pomoću zlonamjernog Word dokumenta u kojem se nalazila lažna COVID-19 anketa čija je svrha preuzimanje *ransomware* koda pomoću kojeg se žrtva ucjenjivala kako bi oporavila svoje šifrirane datoteke (Malwarebytes, 2020). Izgled lažne ankete prikazan je na slici 16. Napadač je kreirao e-mail adresu s uslugom „mailpoof.com“ kako bi registrirao račune na servise za upravljanje sadržajem u oblaku „Box.net“ i „DropBox,“ na koje je najprije prenio i pomoću njih distribuirao dokument lažne ankete. Napadač je to učinio kako bi izbjegao filtere za neželjenu poštu i krađu identiteta koji bi blokirali poruke novoregistrirane adrese e-pošte niske reputacije jer je puno teže otkriti neželjenu poštu od usluga dijeljenja datoteka bez stvaranja niza lažnih pozitivnih rezultata (Malwarebytes, 2020). *Phishing* dokument koristi injekciju predloška za preuzimanje i izvršavanje udaljenog predloška koji je naoružan zlonamjernom makronaredbom prikazanom na slici 17.




Slika 16. *Phishing* document s lažnom COVID-19 anketom (Malwarebytes, 2020)

Zatim, nakon što se *ransomware* implementira, počinje šifrirati korisničke datoteke i dodavati im ekstenziju .VAGGEN, a kada je proces enkripcije gotov, pojavljuje se poruka na radnoj površini u kojoj se zahtjeva plaćanje otkupnine u iznosu od 80 USD u Bitcoinu. Ovaj napad u konačnici nije bio uspješan zbog brzog odgovora tima za kibernetičku sigurnost UBC-a (Malwarebytes, 2020).




Slika 17. Predložak sa zlonamjernom makronaredbom (Malwarebytes, 2020)

# 5. Metode zaštite

Kako bi se na koristan način zaštitili od kibernetičkih napada, odnosno poduzeli pravilne korake u prevenciji ili posljedicama napada, važno je poznavati i konkretno primjenjivati metode zaštite od kibernetičkih napada. Postoji više načina obrane od kibernetičkih napada, čijim se poduzimanjem korisnici do neke mjere mogu osigurati od štetnih posljedica koje pojedine vrste napada mogu ostaviti.

Prije definiranja metoda zaštita, važno je napomenuti da postoji tri vrste ranjivosti koje pružaju mogućnost napadačima da dobiju pristup korisnikovim sustavima, a to su: nedostatci, posebne značajke programa i korisnička pogreška (National Cyber Security Centre [NCSC], 2016, str. 6). Nedostaci predstavljaju neke nenamjerne funkcionalnosti koje mogu biti rezultat lošeg dizajna ili pogreške napravljene tijekom implementacije te mogu ostati neotkrivene značajan vremenski period. S druge strane, posebne značajke predstavljaju namjerne funkcionalnosti koje napadači mogu iskoristiti da probiju u sustav korisnika te koje su inače podstavljene kako bi poboljšale iskustvo korisnika u određenim aplikacijama ili programima. Korisnička pogreška je treća vrsta ranjivosti i uključuje česte pogreške korisnika poput odabira prejednostavne lozinke, ostavljanja računala ili mobilnih uređaja bez nadzora, otkrivanja osjetljivih informacija ili slučajnog instaliranja zlonamjernih softvera (NCSC, 2016, str. 6).

Zatim, NCSC (2016) navodi nekoliko korisnih preventivnih mjera u reduciranju izloženosti korisnika ili organizacija od kibernetičkih napada:

- Uspostavljanje obrane perimetra mreže - poput *proxy* poslužitelja ili vatrozida
- Uspostavljanje i održavanje obrane od zlonamjernog softvera za otkrivanje i reagiranje na poznate kodove napada
- Upravljanje zakrpama, odnosno instalacija najnovijih verzija softvera kako bi se spriječili napadi koji iskorištavaju softverske greške
- Sprječavanje nepoznatog softvera da se može sam pokrenuti ili instalirati
- Ograničavanje funkcionalnosti svakog uređaja, operacijskog sustava i aplikacije na minimum potreban za funkcioniranje poslovanja
- Osiguravanje postojanja i poštivanja odgovarajuće politike lozinki

- Kontroliranje pristupa korisnika ograničavanjem dopuštenja izvršavanja na privilegije koje su bitne za rad tog korisnika

*Proxy* je računalo koje djeluje kao posrednik između klijenta i poslužitelja (Nacionalni CERT, 2010). Klijent se povezuje na *proxy* poslužitelj tražeći neku uslugu (datoteku, web stranicu ili nešto drugo) od drugog poslužitelja, klijentski zahtjev se, nakon obrade unutar *proxy* poslužitelja, prosljeđuje do željenog poslužitelja (u izvornom ili izmijenjenom obliku) ili odbacuje ako nije zadovoljio neki od zadanih uvjeta postavljenih na *proxy* poslužitelju (Nacionalni CERT, 2010). Proxy poslužitelji se koriste u razne svrhe kao što su anonimnost klijentskih računala tj. krajnjih korisnika, ubrzanje pristupa resursima upotrebom metode privremene pohrane (engl. *caching*), zabrana pristupa određenim web stranicama ili web stranicama s određenim ključnim riječima, zabrana određenih protokola, zabrana pristupa određenim priključcima (engl. *ports*) ili određenim korisnicima, praćenje korisnikovih zahtjeva itd. (Nacionalni CERT, 2010).

Antivirusni program može se definirati kao „softver koji skenira i čisti viruse iz računalnog sustava“ (Conry-Murray & Weafer, 2005., str. 221). Antivirusni programi mogu se podijeliti u tri kategorije: programi za pregledavanje, programi za nadgledanje aktivnosti i programi za detekciju promjena (Ždrnja, 2003, str. 138). Uloga programa za pregledavanje (engl. *scanners*) je pregled informacija na diskovima i u memoriji računala kako bi detektirali uzorke pojedinih virusa, zatim uloga programa za nadgledanje aktivnosti (engl. *activity monitors*) je pregled svih operacija koje se provode tijekom rada računala i upozoravanje korisnika na potencijalno opasne aktivnosti, dok se uloga programa za detekciju promjena (engl. *change-detection software*) odnosi na nadgledanje svih promjena unaprijed određenih direktorija i datoteka te upozoravanje korisnika o detektiranim promjenama (Ždrnja, 2003, str. 138).

Dakle, antivirusni softver obično radi kao pozadinski proces, skenirajući računala, poslužitelje ili mobilne uređaje kako bi otkrio i ograničio širenje zlonamjernog softvera. Mnogi antivirusni softverski programi uključuju otkrivanje prijetnji i zaštitu u stvarnom vremenu kako bi se zaštitili od potencijalnih ranjivosti dok se one događaju (Rosencrance, 2017). Prema Rosencrance (2017) osnovne značajke koje većina antivirusnih softvera obavlja uključuju:

- Skeniranje direktorija ili određenih datoteka u potrazi za poznatim zlonamjernim uzorcima koji ukazuju na prisutnost zlonamjernog softvera

- Omogućavanje korisnicima da zakažu automatsko pokretanje skeniranja
- Omogućavanje korisnicima da započnu nova skeniranja u bilo kojem trenutku
- Uklanjanje detektiranih zlonamjernih softvera – automatski u pozadini ili obavještavanjem korisnika o infekcijama te pitanjem žele li očistiti datoteke

Zatim, najčešće tehnike detekcije zloćudnih programa koje antivirusni softveri mogu imati su detekcija bazirana na potpisima, detekcija zlonamjernog sadržaja i heuristička detekcija. Detekcija bazirana na potpisima je najstarija i najčešća metoda detekcije zloćudnih programa koja se „svodi na uspoređivanje sadržaja datoteka na računalu s potpisima već pronađenih virusa pohranjenih u bazi antivirusnog alata“ (Nacionalni CERT, 2009, str. 6). Iako se ovom vrstom detekcije ne mogu detektirati novi i nepoznati virusi te drugi zloćudni programi, u većini slučajeva je učinkovita te se na nju oslanja velik broj antivirusnih alata. Ako se detektira već poznati potpis, antivirusni softver nudi mogućnost brisanja zaražene datoteke, uklanjanja zlonamjernog koda kako bi se datoteka mogla i dalje koristiti ili spremanje datoteke u neku vrstu izolacije. Treća mogućnost je najčešće birana, no kod nekih zlonamjernih programa nije moguće obnoviti datoteku tako da se, zbog sprječavanja daljnjeg širenja zlonamjernog koda, datoteka mora obrisati (Nacionalni CERT, 2009, str. 6).

Nadalje, detekcija zlonamjernog ponašanja, uz identificiranje poznatih zloćudnih programa, uključuje i nadgledanje ponašanja svih programa pokrenutih na računalu. Ova tehnika detekcije pruža zaštitu od zlonamjernih programa koji još nisu u bazi proizvođača antivirusnog proizvoda, ali ta značajka često dovodi do velikog broja lažno pozitivnih programa, što može dovesti do toga da korisnik prestane obraćati pozornost na prečesta upozorenja (Nacionalni CERT, 2009, str. 7).

Posljednja vrsta detekcije, odnosno heuristička detekcija, sastoji se od tri metode: analiza programa, emulacija rada programa te općeniti potpisi (Nacionalni CERT, 2009, str. 7). Analiza programa je proces kod kojeg antivirusni program ispituje svaku naredbu programa te prema tome odlučuje je li program zloćudan ili nije. Primjerice, ako program sadrži naredbu koja briše neke važne sistemske datoteke, vjerojatno će biti okarakteriziran kao zloćudan što pak može dovesti do dosta lažno pozitivnih detekcija. Emulacija rada programa uključuje pokretanje programa u posebnom virtualnom okruženju, odvojenom od stvarnog računalnog sustava, u kojem se sve promjene bilježe i analiziraju te ako su rezultat neke zlonamjerne aktivnosti antivirusni program to prijavljuje korisniku. Na posljetku, korištenjem treće heurističke metode, odnosno općenitih potpisa, može se detektirati npr.

cijela familija zloćudnih programa, što je vrlo korisno zbog mogućnosti virusa da naknadno mutiraju u različite inačice (Nacionalni CERT, 2009, str. 7).

Danas postoji mnogo antivirusnih programa od raznih proizvođača, od kojih su neki besplatni, a neki zahtijevaju jednokratno ili mjesečno plaćanje te svaki od ima različite mogućnosti i značajke koje bi korisnik trebao proučiti prije nego se odluči za određenu verziju. Neki od popularnijih proizvođača antivirusnih programa su Bitdefender, Norton AntiVirus, McAfee Antivirus, Trend Micro, Malwarebytes, Avira, ESET, Avast Antivirus itd. (Investopedia, 2021).

Vatrozid (engl. *firewall*) je „softver ili hardver koji računalo ili mrežu odvaja od Interneta“ (Conry-Murray & Weafer, 2005., str. 223). Funkcija vatrozida je smanjenje potencijalne internetske prijetnje, a njegovo rješenje u obliku programske potpore koristi se uglavnom na osobnim računalima koja nisu dio računalne mreže ili su dio manje mreže, dok se vatrozid u obliku hardvera prvenstveno koristi u kompleksnim mrežama poput onih u tvrtkama (Nacionalni CERT, 2007, str. 5). Vatrozid radi tako da „filtrira podatke koji prolaze kroz njega – omogućuje ili onemogućuje njihov prolaz unutar ili van objekta ili sustava na čijem se ulazu nalazi“ (Nacionalni CERT, 2007, str. 5). Filtriranje podataka može biti skup pravila koji uspostavljaju vlasnici privatne mreže što omogućuje stvaranje prilagođene slučajeve upotrebe vatrozida (Kaspersky, bez dat.), a neki od njih uključuju:

- Blokiranje neželjene veze iz izvora koji se čudno ponašaju
- Roditeljski nadzor nad eksplicitnim web sadržajima
- Ograničavanje pregledavanja weba na radom mjestu
- Nacionalno kontroliran intranet, odnosno blokiranje pristupa web-sadržaju koji je potencijalno neskladan s vodstvom ili vrijednostima određene nacije

# 6. Zaključak

Razmjeri štetnih posljedica, koje kibernetički kriminal može ostaviti na pojedince, organizacije ili kompanije, ukazuju na važnost pravovaljane prevencije i zaštite od kibernetičkih napada. Osim ozbiljnosti posljedica napada, zabrinjavajuće karakteristike kibernetičkih napada su i brzina njihova širenja, raznolikost postojećih i novih vrsta te brojnost načina na koje se mogu počiniti. Metode kojima su kibernetički kriminalci naučili izmanipulirati korisnike kako bi od njih ukrali osjetljive informacije te brojne vrste zlonamjernih kodova koji se neprestano razvijaju, upućuju na to koliko je bitna edukacija o kibernetičkom kriminalu, motivima napadača i načinima obrane od raznoraznih računalnih prijetnji. Uz to, trenutna kriza zbog pandemije koronavirusa, savršen je pokazatelj nespremnosti brojnih organizacija i tvrtki kada je u pitanju zaštita od kibernetičkih napada. Nagli prijelaz na rad od kuće, *online* nastavu i općenito povećanje vremena provedenog na računalu uzrokovali su nedostatke u kibernetičkoj sigurnosti koje su kibernetički kriminalci pomno iskoristili. Trenutno nema puno literature o vezi između porasta kibernetičkog kriminala i pandemije koronavirusa, no na temelju postojećih izvora može se zaključiti kako veza ipak postoji i kako koronakriza, kao i na ostale aspekte života, ima utjecaj i na kibernetički kriminal.

# 7. Literatura


1. Atlas VPN. (2020). *Google Registers a 350% Increase in Phishing Websites Amid Quarantine.* Preuzeto 20. siječnja 2022. s https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine
2. Bača, M., i Čosić, J. (2013). *Prevencija računalnog kriminaliteta*. Časopis „Policija i sigurnost.“ (Zagreb), godina 22., broj 1, str. 146-158 Preuzeto 08. siječnja 2022. s https://hrcak.srce.hr/105623
3. Bingulac, N., Dragojlović, J., i Matijašević-Obradović, J. (2013). *Psihologija hakera i značaj njihovih aktivnosti u internet komunikacijama savremenog društva*. Proceedings of the 3rd International Scientific Conference on „Power of Communication.“ Beograd: Panevropski univerzitet Apeiron. Preuzeto 08. siječnja 2022. s https://www.researchgate.net/publication/341685498_Psihologija_hakera_i_znacaj_njihovih_aktivnosti_u_Internet_komunikacijama_savremenog_drustva
4. Brush, H. Marie (2014). *Phreaking*. *Encyclopedia Britannica*. Preuzeto 08. siječnja 2022. s https://www.britannica.com/topic/phreaking
5. Buil-Gil, D., Díaz-Castaño, N., Kemp, S., Miró-Llinares, F., Moneva, A. (2021). *Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK*, European Societies, 23:sup1, S47-S59, DOI: 10.1080/14616696.2020.1804973
6. Cano J., Cavaller V., Sabillon R., i Serra J. (2016). *Cybercrime and Cybercriminals: A Comprehensive Study*. International Journal of Computer Networks and Communications Security, Vol. 4, No. 6: 165–176. Preuzeto 08. siječnja 2022. s https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study
7. Chawki, M., Darwish, A., Khan, M. A., i Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing.
8. Conry-Murray, A. (2005). *Sigurni na Internetu*. Zagreb: Miš
9. Europol. (2020). *Internet Organised Crime Threat Assessment* (IOCTA). Luxembourg: Publications Office of the European Union. Preuzeto 08. siječnja 2022. s https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

10. Europol. (2021). *Internet Organised Crime Threat Assessment* (IOCTA). Luxembourg: Publications Office of the European Union. Preuzeto 08. siječnja 2022. s https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
11. Europski parlament. (2020). *Kako se zaštititi od kibernetičkog kriminala*. Preuzeto 08. siječnja 2022. s https://www.europarl.europa.eu/news/hr/headlines/priorities/odgovor-eu-a-na-koronavirus/20200327STO76003/kako-se-zastititi-od-kibernetickog-kriminala
12. Furnell, S. M. (2001). *Categorising cybercrime and cybercriminals: The problem and potential approaches*. *Journal of Information Warfare*, *1*(2), 35–44. Preuzeto 08. siječnja 2022. s https://www.researchgate.net/publication/292770598_Categorising_cybercrime_and_cybercriminals_The_problem_and_potential_approaches
13. Gillis, A.S. (2021). *Melissa virus*. Preuzeto 08. siječnja 2022. s https://www.techtarget.com/searchsecurity/definition/Melissa-virus
14. Gordon, S., i Ford, R. (2006). *On the definition and classification of cybercrime*. Journal in Computer Virology, 2(1), 13–20. doi: 10.1007/s11416-006-0015-z
15. Hacker. (2011). U Merriam-Webster online. Preuzeto 08. siječnja 2022. s https://www.merriam-webster.com/dictionary/hacker
16. Hosseinian-Far, A., Jahankhani, H., i Al-Nemrat, A. (2014). *Cyber crime Classification and Characteristics*. U B. Akhgar (ur.), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (str. 149-164). Waltham, MA 02451, USA: Elsevier. Preuzeto 08. siječnja 2022. s https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics
17. Hrvatska Enciklopedija. (2021). *Neželjena pošta*. Preuzeto 08. siječnja 2022. s http://www.enciklopedija.hr/Natuknica.aspx?ID=68390
18. Hrvatski zavod za javno zdravstvo [HZJZ]. (2021). *Pitanja i odgovori o bolesti uzrokovanoj novim koronavirusom*. Preuzeto 08. siječnja 2022. s https://www.hzjz.hr/priopcenja-mediji/pitanja-i-odgovori-o-bolesti-uzrokovanoj-novim-koronavirusom/
19. International Telecommunication Union [ITU]. (2012). *Understanding cybercrime – phenomena, challenges and legal response*. Preuzeto 08. siječnja 2022. s

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

20. Interpol. (2020). *Cybercrime: COVID-19 Impact*. Lyon: INTERPOL General Secretariat. Preuzeto 08. siječnja 2022. s https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
21. Investopedia. (2021). *Best Antivirus Software*. Preuzeto 22. siječnja 2022. s https://www.investopedia.com/best-antivirus-software-5084503
22. Kaspersky. (bez dat.). *What is a Firewall? - Definition & Explanation*. Preuzeto 22. siječnja 2022. s https://www.kaspersky.com/resource-center/definitions/firewall
23. Kaspersky. (bez dat.). *What is Social Engineering?* Preuzeto 08. siječnja 2022. s https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
24. Kaspersky. (bez dat.). *What is Spoofing – Definition and Explanation.* Preuzeto 08. siječnja 2022. s https://www.kaspersky.com/resource-center/definitions/spoofing
25. Li, J. X. (2017). *Cyber crime and legal countermeasures: A historical analysis*. International Journal of Criminal Justice Sciences (IJCJS) – Official Journal of the South Asian Society of Criminology and Victimology (SASCV), Vol. 12 (2): 196–207. doi:10.5281/zenodo.1034658
26. Lutkevich, B., Terrell Hanna, K., i Wright, R. (2021). *Botnet*. Preuzeto 20. siječnja 2022. s https://www.techtarget.com/searchsecurity/definition/botnet
27. Malwarebytes. (2020). *Cybercrime tactics and techniques*. Preuzeto 20. siječnja 2022. s https://www.malwarebytes.com/resources/files/2020/06/ctnt_q1_2020_covid-report_final.pdf
28. Malwarebytes. (2020). *Fake COVID-19 survey hides ransomware in Canadian university attack*. Preuzeto 21. siječnja 2022. s https://blog.malwarebytes.com/cybercrime/2020/10/fake-covid-19-survey-hides-ransomware-in-canadian-university-attack/
29. Nacionalni CERT. (2012). *Analiza WannaCry ransomwarea.* Preuzeto 08. siječnja 2022. s https://www.cert.hr/33204/
30. Nacionalni CERT. (2007). *Comodo vatrozid*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2007-02-184.pdf
31. Nacionalni CERT. (bez dat). *O crvima*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/crvi/

32. Nacionalni CERT. (2008). *DDoS napad*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/ddos-napad/
33. Nacionalni CERT. (2021). *Godišnji izvještaj Nacionalnog CERT-a za 2020. godinu*. Preuzeto 21. siječnja 2022. s https://www.cert.hr/GINC2020
34. Nacionalni CERT. (2009). *Ispitivanje antivirusnih alata*. Preuzeto 22. siječnja 2022. s https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-07-269.pdf
35. Nacionalni CERT. (2010). *Proxy poslužitelji*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-08-309.pdf
36. Nacionalni CERT. (bez dat). *Ransomware*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/19795-2/ransomware/
37. Nacionalni CERT. (bez dat). *O trojanskim konjima*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/trojanski_konji/
38. Nacionalni CERT. (2020). *Važno upozorenje: u tijeku je phishing kampanja vezana uz COVID-19.* Preuzeto 21. siječnja 2022. s https://www.cert.hr/vazno-upozorenje-u-tijeku-je-phishing-kampanja-vezana-uz-covid-19/
39. Nacionalni CERT. (bez dat). *O virusima*. Preuzeto 08. siječnja 2022. s https://www.cert.hr/virusi/
40. National Cyber Security Centre [NCSC]. (2016). *Common cyber attacks: reducing the impact.* Preuzeto 08. siječnja 2022. s https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact
41. Radin, T. J. (2016). *Identity theft. Encyclopedia Britannica*. Preuzeto 08. siječnja 2022. s https://www.britannica.com/topic/identity-theft
42. Rosencrance, L. (2017*). Antivirus software (antivirus program).* Preuzeto 22. siječnja 2022. s https://www.techtarget.com/searchsecurity/definition/antivirus-software
43. Steinmetz, K. F., i Yar, M. (2019). *Cybercrime and Society*. London, UK: Sage Publications.
44. Šolić, K., i Velki, T. (2018). *Priručnik za informacijsku sigurnost i zaštitu privatnosti*. Osijek: Fakultet za odgojne i obrazovne znanosti. Preuzeto 08. siječnja 2022. s https://csi.hr/2020/05/03/prirucnik-za-informacijsku-sigurnost-i-zastitu-privatnosti/
45. Tidy, J. (2020). "*Mysterious 'Robin Hood' hackers donating stolen money*." BBC News Technology. Preuzeto 08. siječnja 2022. s https://www.bbc.com/news/technology-54591761

46. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge, UK: Polity Press.
47. Wiggen, J. (2020). *The impact of COVID-19 on cyber crime and state-sponsored cyber activities*. Berlin: Konrad-Adenauer-Stiftung e. V. Preuzeto 08. siječnja 2022. s https://www.jstor.org/stable/resrep25300
48. World Health Organisation [WHO]. (2020). *WHO reports fivefold increase in cyber attacks, urges vigilance*. Preuzeto 08. siječnja 2022. s https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
49. Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, Narodne novine, br. 9/2002. Preuzeto 08. siječnja 2022. s https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html
50. Ždrnja, B. (2003). *Što su i kako rade virusi*. Zagreb: Bug i SysPrint

# Kibernetički kriminal i njegov porast za vrijeme pandemije koronavirusa

## Sažetak

Ubrzani tehnološki razvoj donosi sa sobom i napredak kibernetičkog kriminala, posebno u doba kada društvo sve više ovisi o informacijskoj i komunikacijskoj tehnologiji koja postaje ključno sredstvo za upravljanje gotovo svim kritičnim sustavima suvremenog društva kao i ključno sredstvo u komunikaciji. Važnost informacijske i komunikacijske tehnologije naglašena je uslijed pandemije koronavirusa, kada se, zbog uvođenja restriktivnih mjera radi povećanja sigurnosti, obrazovanje, posao i svakodnevni život uvelike oslanja na korištenje digitalne infrastrukture. U radu će se analizirati porast kibernetičkog kriminala usred pandemije koronavirusa te će se istražiti uzročno-posljedična veza. Dat će se pregled vrsta kibernetičkih napada, a posebno će se obraditi i opisati one vrste koje bilježe porast uslijed pandemije. Osim navedenog, istražit će se motivi koje kibernetički kriminalci mogu imati u određenim situacijama te najvažnije metode zaštite i obrane od kibernetičkih napada.

**Ključne riječi:** kibernetički kriminal, pandemija koronavirusa, računalna sigurnost, zlonamjerni programi

# Cybercrime and its rise during the coronavirus pandemic


## Summary

Accelerated technological development brings along the progress of cybercrime, especially at a time when society is increasingly dependent on information and communication technology, which is becoming a key tool for managing almost all critical systems of modern society and a key tool in communication. The importance of information and communication technology has been highlighted by the coronavirus pandemic, when, due to the introduction of restrictive measures to increase security, education, work and daily life rely heavily on the use of digital infrastructure. The paper will analyze the rise of cybercrime in the midst of a coronavirus pandemic and investigate the cause-and-effect relationship. An overview of the types of cyber attacks will be given, and those types that are on the rise due to a pandemic will be specifically addressed and described. In addition to the above, the motives that cybercriminals may have in certain situations and the most important methods of protection and defense against cyber attacks will be explored.



**Key words:** cybercrime, coronavirus pandemic, computer security, malware