Примљено: 26. јун 2023.
Прихваћено: 02. август 2023.

004.4`242:355.404.51
COBISS.SR-ID 112252681
DOI 10.5937/ssb202301049R

ТАЈНЕ АПЛИКАЦИЈЕ ЗА НАДЗОР

Ана Радовановић, демонстратор*
Универзитет у Београду, Факултет безбедности

* aradovanovic099@gmail.com

ТАЈНЕ АПЛИКАЦИЈЕ ЗА НАДЗОР

Сажетак: *Тајне апликације за надзор спадају у категорију шпијунског софтвера. Постоје две категорије тајних апликација за надзор: bossware и stalkerware. Bossware налази своју примену у пословној сфери, за праћење продуктивности радника, док се stalkerware користи за надзор партнера/супружника и за надзор деце од стране родитеља. Stalkerware представљају опасне апликације, јер омогућавају потпуну контролу над животом жртве, захваљујући великом броју напредних опција које пружају својим корисницима. Само неки од примера су тајно снимање телефонских позива, преглед фотографија и видео записа, преглед историје контакта, слушање телефонског окружења уживо. Висок степен опасности по кориснике представљају 'прикривене' stalkerware апликације. Под појмом 'прикривених' stalkerware апликација може се сматрати велики број популарних апликација које поседују одређене функције које им омогућавају прикупљање података о корисницима и остваривање надзора над њима. Посебан проблем представља чињеница да се stalkerware не појављује у менију апликација уређаја или, пак, на почетном екрану, тако да су могућности да корисник уређаја схвати да је предмет надзора сведен на минимум. У раду ће бити представљене stalkerware апликације, 'прикривене' stalkerware апликације, знакови који указују на постојање stalkerware апликација на уређају и Google-ова политика и однос према stalkerware-у.*

Кључне речи: *тајне апликације за надзор, stalkerware, 'прикривене' stalkerware, људска права*

Увод

Двадесети век је у историји забележен као век убрзаног технолошког развоја, услед развоја рачунара, телевизије и Интернета. Ова открића допринела су промени комуникационе праксе људи. За разлику од тадашњег интерперсоналног комуницирања долази до развоја масовног комуницирања. Развоју новог облика комуникационе праксе, односно масовног комуницирања, допринели су развој друштвених

мрежа, блогова и форума, где људи остављају велику количину информација на Интернету. Међутим, историјски моменат за развој шпијунског софтвера, односно технологија за надзор, десио се 11. септембра 2001. године, када се догодио терористички напад у Америци. Након овог догађаја државе почињу да користе ову врсту технологија у циљу борбе против тероризма, криминала, али и против политичких неистомишљеника, радозналих новинара и активиста. У прикупљању података примарно учествују безбедносне службе и приватне компаније. Приватне комапније које нуде ову врсту софтвера афирмишу своје производе као значајне алате у борби против организованог криминала и тероризма. Откриће Едварда Сноудена показало је размере коришћења ове технологије и да се она већ увелико користи за остваривање контроле и надзора над грађанима. Међутим, до значајног развоја и употребе шпијунског софтвера, односно тајних апликација за надзор од стране грађана, долази са појавом Ковида-19. Појавом вируса Ковид-19 и каснији развитак глобалне пандемије имао је велики утицај на начин живота људи. Готово целокупна комуникација на глобалном нивоу престала је да постоји у свом „класичном" облику, као последица предузимања широког спектра мера од стране држава, које су за циљ имале спречавање ширења вируса, у виду ограничења кретања и интеракције између људи. У таквим околностима где су могућности за социјалном интеракцијом и кретањем сведене на минимум, а када долази до масовне употребе дигиталних средстава комуникације, било је потребно пронаћи начин опстанка економије и очувања здравља људи. Она су омогућила неометано одвијање комуникације, тако да је целокупна комуникација, од пословне, образовне, па до личне, прешла у свет на мрежи. А све заједно представљало је позитиван подстицај развоју индустрије за надзор и произвело је убрзани развој технологија. С обзиром на чињеницу да је целокупна комуникација пренесена у дигитални свет и да се ту налази велика количина података, могућности злоупотребе и надзора су велике (Радовановић, 2022: 4). Пандемија, као и бројне мере које су предузимане у циљу спречавања исте приморале су бројне компаније и њихове запослене да пређу на рад од куће, што је довело до експанзије ширења тајних апликација за надзор запослених од стране послодаваца, познате под називом bossware. Поред њих, на тржишту је присутан stalkerware, који се може дефинисати као софтвер чијом инсталацијом је омогућено праћење кретања корисника телефона, надгледање позива и порука, преглед активности на друштвеним мрежа-

ма, као и приступ фотографијама и видео снимцима. Поред ових опција, постоји још једна опција која има изразито висок степен опасности по жртву, а састоји се у могућности укључивања камере уређаја, да би се видело шта праћена особа ради и са ким је (Информација, 2021а). Овај софтвер користи се за надзор партнера или супружника, а често се користи и за надзор деце од стране родитеља. Имајући у виду претходно речено, евидентно је да stalkerware омогућава потпуно контролу над животом жртве и да представља велику опасност по њен живот. Колика је заступљеност ових апликација показује истраживање из 2018. године, које је показало да је у Сједињеним Америчким Државама, 15,8% жена и 5,3% мушкараца било изложено насиљу ухођења, а у прилог овој тврдњи иде и податак добијен у недавном истраживању, које је дошло до резултата да је чак 10% одраслих испитаника у САД признало да је користило апликацију за шпијунирање, тј. надзор интимног партнера (Han et al., 2021: 1). Подаци добијени у илустрованим истраживањима доводе нас до закључка да су жене чешће жртве ове врсте апликација него мушкарци. У раду ће бити приказане stalkerware апликације, са посебним осврtом на „прикривене" stalkerware апликације, знакови који указују на постојање ове врсте апликација на уређају и Google-ова политика и однос према stalkerware апликацијама.

Stalkerware апликације

Прво ћемо дефинисати појам шпијунски софтвер, а затим и појам тајне апликације. У страној и домаћој литератури постоје многобројне дефиниције појма шпијунски софтвер, а једна од њих је и следећа: под појмом шпијунски софтвер подразумева се злонамерни софтвер који угрожава приватност, али и веома често технологија пасивног прикупљања података, а кључна карактеристика шпијунског софтвера је његова тајна природа, која се састоји из тајности рада саме апликације, постојања тајне комуникације са трећом страном, као и прикупљање информација без сагласности власника (Howah, 2011: 12). Различити типови информација су предмет интересовања шпијунског софтвера, од лозинки, преко података о онлајн куповини, до email поште и разговора на WhatsApp и другим платформама, а саме тајне апликације за надзор спадају у категорију шпијунског софтвера. Stalkerware је термин који се користи за означавање апликација за

тајни надзор. Stalkerware представља опасан софтвер из разлога што апликације омогућавају тајно прикупљање информација о власнику телефона, кроз опције читање порука на друштвеним мрежама, као и у апликацијама попут WhatsApp, Viber, Telegram и другим, омогућавају увид у листу контакта и историју позива, праћење кретања жртве, прикупљањем информација о планираним догађајима из календара, прегледањем фотографија које су сачуване на телефону, прављење снимака екрана и фотографија злоупотребом предње камере телефона (Информација, 2022а). Као још један разлог због кога stalkerware представља опасан софтвер лежи у чињеници да га веома често користе насилници да контролишу жртве, а најчешће су у питању чланови породице или партнери. Уз то, важно је нагласити да веома често физичко насиље произлази из дигиталног насиља (Информација, 2022б). Код ове класе апликација постоји тенденција да деле низ заједничких карактеристика, у виду прегледа СМС порука, различитих апликација за комуникацију, попут WhatsApp и Viber-а, затим евиденције телефонских позива, као и сачуване медије, попут фотографија и видео снимака, затим веб саобраћај и ГПС информације (Parsons et al., 2019: 21). Међутим, важно је нагласити да немају сви stalkerware исте могућности. Поједине stalkerware апликације могу да надгледају е-пошту, активности на друштвеним мрежама, контакте у адресару, уносе у календару, притиске на тастеру, па чак и да тајно активирају микрофон или фотографишу (Parsons et al., 2019: 21). Међутим, оно што изазива забринутост јесте чињеница да постоји велики број популарних апликација које поседују одређене функције које им омогућавају надзор корисника, прикупљањем података о њима, и које се могу сматрати „прикривеним" stalkerware-ом. Почели су већ да се јављају напори у циљу побољшања приватности корисника, а као један од позитивних примера може се узети Apple-ово представљање IOS 14, у коме је креирана једна од функција која је обавештавала корисника када нека апликација приступа clipboardu и на тај начин је омогућено корисницима да знају које апликације приступају подацима на њиховим уређајима, а колики је позитиван ефекат произвела ова функција говори у прилог то да је, управо захваљујући овој функцији, једно истраживање показало да је више од 50 апликација, од које су неке веома популарне, приступале подацима у clipboardu, међу тим апликацијама нашле су се Linkedln, TikTok и Reddit (Информација, 2020в). Између stalkerware-а и апликација које се могу преузети из званичних продавница, а које су намењене за заштиту од крађе

или, пак, родитељски надзор, постоји веома јасна граница, и састоји се у томе што stalkerware ради скривено од корисника и без његовог пристанка (Информација, 2022б). Могућност да жртва сазна или посумња на постојање ове врсте апликација спречена је, тј. онемогућена у високом проценту, тиме што су ове апликације дизајниране тако да сакрију своје присуство на уређају мете, и у таквим случајевима stalkerware се не појављује у менију апликација уређаја или, пак, на почетном екрану (Parsons et al., 2019, p. 18). Према подацима Kaspersky Security Network (KSN), у 2021. години је око 33.000 корисника на свом уређају имало инсталирано ову врсту апликација, што представља историјски минимум, ако се узме у обзир чињеница да је у 2020. скоро 54.000 корисника било предмет интересовања stalkerware апликација, а 2019. године тај број је износио 67.000 (Информација, 2022б). Забележени тренд пада може се објаснити чињеницом да је у току пандемије потреба насилника за овом врстом апликација опала, из разлога што је само кретање жртава било ограничено, као последица предузимања мера сузбијања ширења вируса. Према подацима компаније Karspesky у току 2022. године 29.312 појединаца широм света је погођено stalkerware апликацијама (Securelist, 2023). Анализа података показује стабилну пролиферацију ових апликација, у просеку 3.333 особе погођено је stalkerware-ом (Securelist, 2023).

„Прикривене" stalkerware апликације

Под појмом „прикривених" stalkerware апликација може се сматрати велики број популарних апликација које поседују одређене функције које им омогућавају прикупљање података о корисницима и остваривање надзора над њима. Формално гледано, да би апликације могле да прикупљају податке о кориснику потребна је корисникова дозвола за одређене функције. Међутим, у пракси нису ретки случајеви да се подаци прикупљају без дозволе корисника, о чему ће бити речи даље у тексту.

Стварна опасност или ипак не?

Приликом инсталирања било које врсте апликације на уређај потребно је да корисник постави себи два кључна питања. Прво, колико личних података ће делити са апликацијом и, друго, да ли сматра

да су све дозволе које апликација тражи стварно неопходне (Пајић, 2021)? Са једне стране, постоје оправдани разлози апликација за прикупљањем података корисника, ради праћења интеракције, а у циљу унапређења искуства или отклањања евентуалних проблема који се јављају, док, са друге, проблем је то што компанија која стоји иза одређене апликације која прикупља ову врсту података може тако прикупљене податке продавати трећим странама, које те исте податке могу користити за циљано оглашавање (БаштаБалкана, 2021). Није редак случај да подаци корисника заврше у рукама компанија за друштвено ослушкивање, као на пример Hootsuite или BuzzSumo, које прикупљају податке корисника са циљем да те податке проследе компанијама које ће их анализирати и продати им производ (БаштаБалкана, 2021). Међу апликацијама које највише деле приватне податке корисника са трећим странама налази се велики број изразито популарних апликација, као што су Instagram, Facebook, Linkedln, You Tube, TikTok и eBay (БаштаБалкана, 2021).

Пре свега, не представљају све дозволе које се дају апликацијама „ризичне дозволе", то се пре свега односи на оне дозволе које обезбеђују приступ подацима или ресурсима који укључују личне информације корисника, или, на пример, могу да потенцијално утичу на сачуване податке корисника, као и на рад других апликација (Пајић, 2021). Као примери „ризичних дозвола" могу се навести дозволе које омогућавају приступ локацији корисника, затим СМС порукама, телефонским евиденцијама, тј. позивима, камери или календару. Најтраженија дозвола која се може категорисати као „ризична" јесте дозвола за приступ камери и њена заступљеност је преко 45%. На другом месту се налази дозвола за снимање звука са заступљеношћу преко 25%, а на трећем месту се налази дозвола за читање СМС порука са 15%. На четвртом месту се налази дозвола за приступ евиденцији телефонских позива са 10% заступљености (Пајић, 2021). Вил Страфач (Will Strafach) је током бављења анализом промета на мрежи 2017. године дошао до открића да и када је ГПС искључен на телефону постоје „празнине" које омогућавају праћење података, на пример Akuveder апликација, која представља једну од популарних апликација која се користи за временску прогнозу, она шаље податке о локацији корисника и у случају када је опција за дељење локације искључена (РТС, 2020). Овде највећи проблем представља што се овакве апликације налазе у Google и Apple продавницама, а нису ретки ни случајеви у којима овакве апликације долазе инсталиране с телефоном, а веома

често се не ради само о једној апликацији, пре свега овде треба ставити акценат на начин на који су оне повезане, о скривеној мрежи података у коду која им у значајној мери помаже да створе свеобухватну слику о некоме и шта неко ради (PTC, 2020). Иако компаније тврде да су подаци анонимни и да нема места за бригу, потребно је врло мало напора уложити како би се утврдило ко је особа, на основу података о локацији, времену и активностима (PTC, 2020). Постоји велики број апликација у Google и Apple продавници које се промовишу као апликације за релаксацију и забаву и које делују крајње безазлено за просечног корисника, али које својим радом, тј. начином функционисања могу угрозити приватност корисника прикупљањем података о њему. Као пример такве врсте апликација може се навести апликација Astro Guru: Astrology, Horoscope & Palmistry, која прикупља бројне податке својих корисника, као што су датум рођења, пол, локација, e-mail адреса и податке о плаћању (N1, 2021). У априлу 2022. године, захваљујући компанији AppCensus, откривено је чак 11 Андроид апликација које су без дозволе корисника прикупљале њихове податке, од броја телефона, e-mail адресе, до ГПС-а, а ове апликације је преузело чак 46.000.000 корисника из званичне Google Play продавнице (Објектив, 2022). На основу броја корисника који су поседовали ове апликације јасно је да је реч о великој количини информација које су прикупљене и злоупотребљене на различите начине (Радовановић, 2022: 23). Међу тим апликацијама нашле су се и апликације попут Simple weather & clock widget, Speed Camera Radar, QR & Barcode Scanner (Објектив, 2022). Временом су развијене бројне препоруке за заштиту података и спречавање нежељеног прикупљање података од стране апликација, које су у значајном проценту ефикасне.

Како бисмо заштитили податке, најпре је потребно проверити које апликације већ имају дозволу за коришћење микрофона и камере и то је могуће врло лако урадити, потребно је само ући у мени за менаџмент апликација и ту кликнути на опцију подешавања, а затим на опцију менаџер дозвола (Телеграф, 2020). Као још једна препорука наводи се инсталирање апликације која ће пратити када су микрофон или камера укључени, а још једна у низу препорука је да се онемогући само снимање кроз физичко блокирање, да ли у виду налепнице коју ће корисник прелепити преко предње и задње камере, или коришћењем футроле са „слајдер" поклопцем, који покрива и предњу и задњу камеру када се не користе; код онемогућавања микрофона ту су на располагању посебни блокатори микрофона (Телеграф, 2020). Из

претходног реченог може се видети да постоје различите врсте мера које корисници могу предузети како би заштитили своје податке од недозвољеног прикупљања, а које значајно доприносе подизању нивоа заштићености података. С обзиром на висок ниво развијености области заштите, као и самих мера, различите категорије корисника могу пронаћи одговарајућу опцију, а у складу са финансијским могућностима и афинитетима. Од изузетног значаја је да свака апликација има политику приватности, у којој се јасно наводи који се подаци прикупљају, на који начин, где се чувају и са ким се деле (Пајић, 2021). У циљу заштите своје приватности као најједноставнији, а са друге стране поуздан начин провере да ли су све тражене дозволе заиста неопходне апликацији, потребно је само у случају Андроид апликација отићи у мени подешавања, затим кликнути на опцију дозволе, уклањање дозвола у случају лоше дизајниране апликације може проузроковати престанак рада апликације, док, са друге стране, добро дизајниране апликације показаће да ли им је заиста неопходна дозвола, када покуша да изврши функцију за коју је захтевала дозволу. У случају iOS апликација дозвола се може уклонити одласком у менији подешавања, а затим је потребно кликнути на опцију приватност (Пајић, 2021). Значајан допринос у борби за заштиту података даје и употреба апликација AppCensus и CharlesProxy које је развио Серж Иглман (Serge Egelman). AppCensus пружа могућност кориснику претраживања апликација и увид у податке који су послати и који се шаљу, а CharlesProxy базира се на принципу пресретања мрежног промета са компјутера и телефона (PTC, 2020). На основу свега изложеног у овом делу рада долази се до неколико закључака. Евидентно је да „прикривене" stalkerware апликације представљају велику опасност по безбедност корисника, с обзиром на то да прикупљају податке корисника без његовог знања. Кључан проблем представља чињеница да сами корисници не поклањају довољно пажње политици приватности, односно њеном читању. Веома често корисници одмах прихвате услове коришћења без претходног пажљивог читања. Имајући то у виду, потребно је уложити додатан напор у погледу едукације грађана о начинима злоупотребе њихових података, али и о широком спектру мера њихове заштите, како би се остварио значајан помак на овом пољу.

Знакови који указују на постојање stalkerware апликација

Као што истиче компанија Kaspersky, корисници тешко могу да препознају постојање stalkerware апликација из неколико разлога. Пре свега, ова врста софтвера остаје скривена, икона stalkerware апликације на почетном екрану и у менију телефона је такође скривена, и долази до чишћења насталих трагова (Информација, 2021а). Ипак, постоји неколико знакова који могу указати на постојање ове врсте апликација. Корисници могу пре свега проверити постојање stalkerware апликација помоћу антивирусног програма, а неки од знакова који указују на постојање stalkerware апликације су брзо пражњење батерије, затим константно прегрејавање уређаја и раст потрошње мобилних података (Информација, 2021а). Као још неки знакови који указују на постојање stalkerware апликације су и успорен рад телефона, замрзавање или прекид рада апликације, затим добијање чудних порука, појављују се искачући прозори или поруке о грешкама програма који су увек добро функционисали и промена подешавања без пристанка корисника, која се манифестује у виду нових икона, новог подразумеваног претраживача, нове почетне странице претраживача итд. (Информација, 2020г). Још један начин на који корисници могу да утврде постојање stalkerware апликације је провера историје прегледача, пошто онај који их надгледа најчешће је морао да преузме апликацију са неког веб сајта. Из тог разлога, корисници обавезно треба да провере да ли су на уређају омогућени „непознати извори", што може представљати знак да је злонамерни софтвер инсталиран из независних извора. Такође, неопходно је да провере дозволе инсталираних апликација с обзиром на то да stalkerware апликације могу бити сакривене под другим именом, са сумњивим приступом порукама, евиденцијама позива, локацији и другим сродним активностима (Информација, 2021а). У овом делу рада приказани су најчешћи знакови који указују на постојање ове врсте апликација, с обзиром на убрзани развој ове врсте апликација, који подразумева широк опсег функција које стоје на располагању корисницима ове врсте апликација, постоји значајна могућност јављања нетипичних знакова који указују на постојање ове врсте апликација. Као што је и у претходним деловима рада истицано, кључна је едукација становништва, како би се остварио значајан помак на плану борбе против ове врсте апликација. Неопходно је утицати на свест становништва о постојању и великој заступљености ове

врсте апликација преко медија, како би се допрело до што већег броја људи, а затим и кроз сам систем школовања и организовања курсева и различитих радионица на ову тему, како би се постигао значајнији напредак (Радовановић, 2022: 18). Уколико би се реализовале наведене активности постигла би се свеобухватност и значајнији напредак у борби против ове врсте апликација, где би дошло прво до развијања саме свести о постојању ове врсте апликација, затим научило би се на који начин реаговати уколико се открије ова врста апликација и које мере предузети, као и како се психолошки суочити са насталом ситуацијом. Тек тада се може рећи да је друштво испунило своју улогу по овом питању (Радовановић, 2022: 18).

Google-ова политика и однос према stalkerware-у

Може се рећи да је Google 2019. године незванично кренуо у борбу против ове врсте апликација, уклањањем чак 7 stalkerware апликације из Google Play-а, које су тајно шпијунирале друге кориснике (it mixer, 2019). Avast, антивирусна компанија, је 2019. године пронашла седам stalkerware апликација доступних за Андроид тржиште, које су биле инсталиране више од 130.000 пута, а Google је уклонио ове апликације након пријаве Avast-а о кршењу приватности, након овог догађаја Google је издао саопштење у ком је истакао да његова политика забрањује комерцијалне шпијунске апликације, и да се залаже за пријаву људи апликација које крше њихову политику и стандарде (it mixer, 2019). Google је званично кренуо у борбу против stalkerware-а у јулу 2020. године. Донете су тада измене смерница за огласе, и постављен је рок од месец дана компанијама да уклоне ове огласе. Поред тога, било је ипак предвиђено и да након истека овог периода они који рекламирају stalkerware добијају седмодневно упозорење, а након истека овог периода долази до њиховог блокирања уколико не уклоне спорне огласе (Информација, 2020д). Google је ставио забрану рекламирања апликација за прислушкивање телефона, чија је изричита сврха праћење или надзор над другом особом, или њеним активностима без њеног одобрења (Информација, 2020д). Забрањена је и промоција GPS trakera, који се продају у сврхе шпијунирања или праћења, као и забрана продаје саме опреме за надзор, као што су камере, аудио рекордери, ауто камере или камере за бебу, које се продају за искључиву сврху надзора или шпијунирања (Информација, 2020д).

Међутим, и након ове забране у Google-овим резултатима претраге могле су се пронаћи овакве апликације. Google се правдао чињеницом да примену нових смерница није увек могуће одмах реализовати (Информација, 2020ђ). Наведено је да проблем представља и то што постоје апликације које прикривају намеру производа, и на тај начин покушавају да избегну примену њихове политике, и да се увек анализира неколико сигнала, као што су да ли текст самог огласа, креативна и одредишна страница поштују правила и да, чим установе да оглас или оглашивач крше правила, предузимају адекватне мере (Информација, 2020ђ). Оно што је спорно и што чини Google-ову политику непотпуном јесте чињеница изузећа од примене своје нове политике на производе или услуге, чија је намена да омогуће родитељима да прате или надгледају своју малолетну децу (Информација, 2020ђ). Као што истиче и сам Malwarebytes, један од произвођача антивируса који активно учествује у борби против stalkerware-а, Google-овом политиком граница између апликација типа stalkerware-а и родитељског надзора је нејасна. Поред њега, значајан допринос у борби против stalkerware-а пружила је и Фондација за електронске границе, оснивањем Коалиције против stalkerware-а 2019. године (Информација, 2020ђ). Чланови ове групе су научници, компаније и непрофитне организације, а циљ овакве коалиције је откривање, подизање свести о stalkerware-у и борба против ове врсте апликација (Информација, 2020ђ). На основу изложеног у овом делу рада може се закључити да и даље постоји простор за унапређење Google-ове политике. Пре свега, боља детекција „прикривених" stalkerware апликација, тј. апликација које су представљене у легитимне сврхе, али које поседују функције које омогућавају надзор корисника. Поред наведеног, потребно је укинути stalkerware апликације за праћење деце, које су, према тренутној Google-овој политици, доступне у Play продавници, што би значајно допринело унапређењу Google-ове политике. Ипак, и поред наведених недостатака Google-ове политике, евидентно је да је Google остварио значајан напредак на пољу борбе против stalkerware-а.

Закључак

Постоје две категорије тајних апликација за надзор: bossware и stalkware апликације. Bossware апликације се користе за праћење продуктивности радника, односно налази своју примену у пословној

сфери, док се stalkerware апликације користе за надзор партнера/супружника и деце. Stalkerware апликације својим корисницима пружају велики број функција од ГПС праћења, тајног снимања телефонских позива, прегледа фотографија и видео записа, преко снимања листе свих инсталираних апликација на уређају, до напредних функција попут пресретања позива и лажне СМС поруке, као и многе друге. Захваљујући бројним опцијама које пружају својим корисницима, ове апликације омогућавају потпуну контролу над животом жртве. Ако се узме у обзир чињеница да ове апликације омогућавају потпуну контролу над жртвом и да остављају бројне психичке последице по жртву, јасно је да је реч о веома опасним апликацијама. С обзиром на то да корисници ове врсте апликација представљају лабилне личности које желе да остваре контролу над животом друге особе, постоји висок степен опасности од појаве физичког и психичког насиља уколико се жртва не понаша у складу са очекивањима насилника. На основу података Kaspersky Security Network (KSN) који су приказани у раду, може се доћи до закључка да је у току пандемије корона вируса заинтересованост за овом врстом апликација опала, пре свега јер су бројне мере предузете у циљу сузбијања ширења вируса у значајној мери ограничиле кретања жртава, тако да је потреба насилника за овом врстом апликација опала. Забележено је да је у току 2021. године 33.000 корисника на свом уређају имало инсталирано ову врсту апликација. У току 2022. године тај број је износио 29.312 појединаца. Анализа података показује стабилну пролиферацију ових апликација, у просеку 3.333 особе погођено је stalkerware-ом (Securelist, 2023). Тренд стабилизације наводи нас на постављање два кључна питања, да ли ћемо кроз пар година живети у ери масовног надзора, а приватност података представљати прави луксуз, или можда већ живимо у ери масовног надзора, ако се има у виду чињеница да државе већ више од деценију активно користе ову врсту апликација. Такође, тренд показује и да је потребно уложити додатни друштвени напор и ангажман у циљу сузбијања тајних апликација за надзор. Потребно је развити свеобухватан приступ борбе против ове врсте апликација кроз укљученост свих заинтересоваих и одговорних актера, а то је могуће постићи једино кроз едукацију становништва у форми различитих радионица и програма обуке. Поред појединаца, потребно је и да државе активно раде на побољшању актуелне законске регулативе и доношењу нове, које регулишу област надзора, али и укљученост мултинационалних компанија, које ће кроз унапређење својих политика и стандарда безбедности дати свој допринос.

ЛИТЕРАТУРА

Han, Y., Roundy, K., and Tamersoy, A. (2021). *Towards Stalkerware Detection with Precise Warnings*. In *ACSAC 2021 – Proceedings of Annual Computer Security Applications Conference, Dec 2021, Online, United States* (pp. 1–13). New York: Association for Computing Machinery.

Howah, K. (2011). *Factors affecting user decisions to download and install software that may contain spyware*. Master's thesis. Queensland: Faculty of arts, business, informatics and eucation, school of information communications technologies.

It mixer. (18. јул 2019). *Google је уклонио 7 stalkerware апликација из Google play-а који тајно шпијунира друге кориснике.* Преузето 27. априла 2022. године, са https://itmixer.com/google-je-uklonio-7-stalkerware-aplikacija-iz-google-play-a-koji-tajno-spijuniraju-druge-korisnike/.

N1инфо Хрватска (N1). (20. јун 2021). *Ове апликације требали бисте одмах уклонити с мобитела, угрожавају приватност.* Преузето 31. јула 2022. године, са https://hr.n1info.com/tehnologija/ove-aplikacije-trebali-biste-odmah-ukloniti-s-mobitela-ugrozavaju-privatnost/.

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., and Deibert, R. (2019). *The predator in your pocket*. Toronto: The Citizen Lab.

Securelist. (08. март 2023). *The state of stalkerware in 2022*. Преузето 17. јуна 2023. године, са https://securelist.com/the-state-of-stalkerware-in-2022/108985/.

БаштаБалкана. (4. мај 2021). *Које апликације прикупљају и продају највише података?* Преузето 31. јула 2022. године, са https://www.bastabalkana.com/2021/05/koje-aplikacije-prikupljaju-i-prodaju-najvise-podataka/.

Вермезовић, Т. (2016). Заштита права на приватност као друштвени императив дигиталног доба колико смо рањиви? *Зборник радова Правног факултета у Нишу*, *LV*(74), стр. 249–265.

Информација. (2. март 2021а). *Упркос Google-овој забрани, апликације за праћење партнера и даље се често налазе на мобилним уређајима.* Преузето 28. априла 2022. године, са https://www.informacija.rs/Vesti/Uprkos-Googleovoj-zabrani-aplikacije-za-pracenje-partnera-i-dalje-se-cesto-nalaze-na-mobilnim-uredjajima.html.

Информација. (15. април 2022б). *Апликације за праћење (stalkerware) – претња која је још увек ту.* Преузето 27. априла 2022. године, са https://www.informacija.rs/Vesti/Aplikacije-za-pracenje-stalkerware-pretnja-koja-je-jos-uvek-tu.html.

Информација. (13. јул 2020в). *Linkedln тужен због шпијунирања корисника које је открила нова функција у IOS 14.* Преузето 28. априла 2022. године, са https://www.informacija.rs/Vesti/LinkedIn-tuzen-zbog-spijuniranja-korisnika-koje-je-otkrila-nova-funkcija-u-iOS-14.html.

Информација. (9. октобар 2020г). *Сумњате да Вас партнер прати: како да откријете апликацију за праћење на свом телефону.* Преузето 28. априла 2022. године, са https://www.informacija.rs/Vesti/Sumnjate-da-vas-partner-prati-kako-da-otkrijete-aplikaciju-za-pracenje-na-svom-telefonu.html.

Информација. (10. јул 2020д). *Google забрањује огласе за програме за праћење супружника.* Преузето 28. априла 2022. године, са https://www.informacija.rs/Vesti/Google-zabranjuje-oglase-za-programe-za-pracenje-supruznika.html.

Информација. (12. август 2020ђ). *И после Google-ове забране, апликације за шпијунирање телефона и даље се рекламирају у Google претрази.* Преузето 28. априла 2022. године, са https://www.informacija.rs/Vesti/I-posle-Googleove-zabrane-aplikacije-za-spijuniranje-telefona-i-dalje-se-reklamiraju-u-Google-pretrazi.html.

Матијашевић, Ј., Бјелајац, Ж. и Димитријевић, Д. (2012). Конвенција Савета Европе о високотехнолошком криминалу. *Европско законодавство*, *11*(42), стр. 37–52.

Објектив. (11. април 2022). *11 апликација под лупом стручњака: тајно скупљале податке- можда су и на вашем телефону?* Преузето 31. јула 2022. године, са https://objektiv.rs/vest/1075129/11-aplikacija-pod-lupom-strucnjaka-tajno-skupljale-podatke-mozda-su-i-na-vasem-telefonu/.

Пајић, Т. (2021). *Мобилни под лупом: шта ваше апликације знају о вама?* Преузето 31. јула 2022. године, са https://www.securitysee.com/2021/12/mobilni-pod-lupom-sta-vase-aplikacije-znaju-o-vama/.

Политика. (28. април 2022). *Србија подржала Декларацију о будућности интернета представљену у Белој кући.* Преузето 2. августа 2022. године, са https://www.politika.rs/scc/clanak/506025/Srbija-podrzala-Deklaraciju-o-buducnosti-interneta-predstavljenu-u-Beloj-kuci.

Прља, Д., Рељановић, М., и Ивановић, З. (2012). *Интернет право.* Београд: Институт за упоредно право.

Радио и Телевизија Србије (РТС). (15. фебруар 2020). *Како нам апликације краду податке.* Преузето 31. јула 2022. године, са https://www.rts.rs/page/magazine/sr/story/1882/tehnologija/3853091/kako-nam-aplikacije-kradu-podatke.html.

Радовановић, А. (2022). *Тајне апликације за надзор*. Дипломски рад. Београд: Универзитет у Београду – Факултет безбедности.

Surčulija, J. (2010). Regulatorni izazovi slobode izražavanja na Internetu. U J. Surčulija (Ur.) (2010). *Sloboda izražavanja na internetu* (str. 19–25). Beograd: Centar za razvoj Interneta.

Телеграф. (6. августа 2020). *Како да сазнате да ли вас апликације са вашег телефона шпијунирају?* Преузето 31. јула 2022. године, са https://www.telegraf.rs/hi-tech/mobilni/3222088-aplikacije-telefon-spijuniranje.

COVERT SURVEILLANCE APPLICATIONS

Ana Radovanović, Student Assistant
University of Belgrade, Faculty of Security Studies

Summary

Hidden spy applications are categorized as spy software. There are two categories of hidden spy applications: bossware and stalkerware. Bossware finds its usage in the business domain, for the tracking of employee productivity. On the other hand, stalkerware is used for partner surveillance, as well as the monitoring of children by the parents. Stalkerware are dangerous applications because they provide full control over the life of a victim, due to the large number of advanced options which allow their users to secretly record phone calls, view photos and videos, access users' contact history, listen in on the phone environment live, etc. "Hidden" stalkerware applications are especially dangerous to their users. A large number of popular applications, which possess certain functions that allow them to gather data on their users and surveil them, are considered "hidden" stalkerware applications. A particular problem with these applications is the fact that they are not visible in the application menu or the title screen, making the odds of the device user realizing they are being surveilled minimal. The paper introduces stalkerware applications, "hidden" stalkerware applications, the signs that indicate the existence of stalkerware applications on the device and Google's politics and attitude towards stalkerware.

Keywords: *covert surveillance applications, stalkerware, 'hidden' stalkerware, human rights.*