УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

КАТЕДРА СТУДИЈА БЕЗБЕДНОСТИ

Тајне апликације за надзор

– ДИПЛОМСКИ РАД –

Ментор:
Др Ана Ковачевић

Студент:
Ана Радовановић
Број индекса : 96/18

Београд, 2022

Садржај

1. Увод

Појавом вируса Ковид 19 а затим и каснији развитак глобалне пандемије имао је велики утицај на начин живота људи. Како би се спречило ширење вируса до невиђених размера, државе су уводиле разне врсте ограничења кретање и саме интеракције између људи, што је имало за последицу ослањање светске популације на дигитална средства комуникације, што је произвело ситуацију да је целокупна комуникација, од личне, пословне па до образовне прешла у свет на мрежи. Све ово заједно је имало позитиван ефекат на развој индустрије за надзор, а самим тим и убрзаног развоја дигиталног надзора.

У прилог томе иде чињеница да су у многим државама развијене апликације које су представљене као иновативне мере борбе против вируса, у виду праћења контакта заражених, као и спровођења мера карантина и других, где је евидентно постојала сарадња Влада држава са провајдерима, који су омогућили приступање геолокацији и спровођење надзора држава над становништвом. Постојала је забринутост људи на који начин Владе и компаније користе њихове личне податке. 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. Као последица пандемије и мера које су донесене у циљу спречавања ширења вируса, многе компаније и њихови запослени су прешли на рад од куће, што је довело до експанзије ширења тајних апликација за надзор запослених од стране послодаваца, познате под називом bossware. Са једне стране продавци ових апликација представљају их као апликације које омогућавају праћење продуктивности рада запослених и начина обављања пословних активности радника, али са друге стране евидентно је да ове апликације пружају могућност злоупотребе, у виду задирања у приватан живот

запослених. Поред њих на тржишту је присутан stalkerware, који се може се дефинисати као софтвер чијом инсталацијом је омогућено праћење кретања корисника телефона, надгледање позива и порука, преглед активности на друштвеним мрежавама, као и приступ фотографијама и видео снимцима, а поред ових опција постоји још једна опција која поседује 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, 2021б). Овај софтвер се користи за надзор супружника или партнера, као и за надзор деце. Из наведеног може се закључити да stalkerware омогућава потпуну контролу насилника над животом жртве. Ова врста апликације је заступљена у великом проценту, али је присутан тренд пада, у прилог тој тврдњи иду подаци KSN-а. Према подацима Kaspersky Security Network (KSN) у 2021. години је око 33.000 корисника система било погођено stalkerware-ом, што представља историјски минум, ако се узме у обзир чињеница да је у 2020. години скоро 54. 000 било погођено том врстом апликација, а 2019. године тај број је износи 67.000 (Информација, 2022а). Међутим треба имати у виду чињеницу да је за време карантина и ограничења кретања потреба насилника за овом врстом апликација опала, али са друге стране и ограничење кретања као и закључавања тј. look down-ови, до којих је долазило у току пандемије омогућили су да лични предмети стално буду на дохват руке, што је створило више прилика насилницима да на уређајима својих партнера и деце инсталирају stalkerware. Тако да је евидентна оправданост предпоставке да постоји могућност поновне екпанзије и пораста броја ових апликација и њихових корисника. 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 чак 10% одраслих испитаника у САД-у признало је да је користило апликацију за шпијунирање тј.

надзор интимног партнера (Han, et al., 2021:1). На основу података који су добијени у илустрованим истраживањима може се доћи до дедуктивног закључка да су ова истраживања показала да су чешће жртве ових апликација жене него мушкарци. У раду ће бити приказани bossware и stalkerware апликације и сам начин њихов рада, њихове најзаступљеније апликације и начин њиховог рада, са критичким освртом на рад апликација, указивањем на недостатке или такозване „ слабе тачке“ у њиховом раду, као и предности појединачне апликације у односу на другу апликацију. Док ће у другом делу рада бити представљени начини њихове детекције тј. откривања и саме мере заштите које би корисници требало да примене у циљу заштите њиховог уређаја од ове врсте апликација. У завршном делу рада посебан акценат ћу ставити на анализу „прикривених stalkerware апликација“ и на који начин могу угрозити безбедност података корисника уређаја, и на крају бавићу се људским правима у дигиталној сфери, у којој мери је омогућено њихово остваривање, колико су заштићена и који су најчешћи начини њиховог кршења.

2. Апликације за надзор

Предмет разматрања овог поглавља су тајне апликације за надзор, односно две категорије ових апликација, stalkerware апликације и bossware апликације. Прво ћу дефинисати сам појам шпијунских софтвер. Након тога предмет разматрања овог поглавља су и врсте информација које су предмет интересовања тајних апликација за надзор. Затим ћу дефинисати појмове stalkerware и bossware апликације, начин њиховог рада, могућности које пружају својим корисницима у виду различитих опција. Ове опције пружају различите начине увида у приватну сферу корисника уређаја који је предмет интересовања ове две категорије апликација за тајни надзор. Као и све апликације и ова категорија има слабости и оне ће бити приказане у овом делу рада. С обзиром да постоје пропусти у њиховом раду који се испољавау у виду нефунционисања појединих опција које стоје на располагању корисницима ових апликација, или застарелости самих апликација, створена је могућност за детекцију тј. откривање постојања ових апликација на уређају жртве. Приказаћу саме знакове који могу указати на постојање ових апликација, као и на који начин Google пружа заштиту од апликација за надзор у виду Google Protect-a.

2.1 Bossware 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 , да се под појмом шпијунски софтвер подразумева злонамерни софтвер који угрожава приватност али и веома често као 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 (SpyTech, 2020). Већину ових апликација карактерише брза и једноставна инсталација, а након саме инсталације апликација нестаје из менија телефона и омогућавају кориснику да са телефона жртве види позиве, поруке, дрштвене мреже, галерију, укључивање камере у реалном времену и друге опције у зависности о којој конкретној апликацији је реч, а важно је нагласити да су ове опције доступне без обзира на удаљеност (SpyTech, 2020).

Када је реч о bossware и популарности ове врсте апликација, до екпанзије ове врсте апликација долази у току пандемије корона вируса, и са предузимањем бројних мера за спречавање ширења вируса, које су постојале у различитим државама. Ограничење кретања, спровођење мера изолације, look down- ови, све то заједно је компаније широм света приморало да се прилагоде тренутним околности и условима, и довело до преласка на систем онлајн рада тј. рада од куће. Како би послодавци осигурали продуктивност и ефикасност рада својих запослених од куће и како би се заштитили од крађе интелектуалне својине, многе компаније су прибегле коришћењу тајних апликације за надзор, веома често без знања својих запослених а назив за ову врсту апликације је bossware. Постоје два начина примене bossware апликација, као апликација која је видљива раднику или као тајна апликација коју радници не могу да виде, а већина компанија које нуде ову врсту апликација пружају обе могућности инсталирања послодавцима, с тим да су најчешћи начини употребе ове врсте апликација за аутоматско праћење времена или за аналитику радног места, а ове функције су и најчешће предмет реклама продаваца ових апликација (Cyphers & Gullo, 2020). Bossware се налази у рачунару или паметном телефону и може да приступи свим подацима на уређају, најчешћи тип надзора који спроводе ове апликације је праћење активности, ово веома често подразумева евиденцију апликација и веб локација које радници користе, а може и

укључивати прикупљање података о корисницима којима је радник послао мејл, укључујући наслове и друге мета податке, као и све објаве које објављују на друштвеним медијима (Cyphers & Gullo, 2020). Већина Bossware-а бележи нивое уноса са тастатуре и миша, што подразумева да многи алати омогућавају детаљан приказ из минута у минут шта корисник уноси, тј. које податке и где кликне, користећи то као прокси за продуктивност а софтвер ће покушати да све ове податке представи у виду једноставних графикона, и ови графикони на високом нивоу менаџерима омогућавају увид у активности и испуњавање задатака запослених (Cyphers&Gullo, 2020). Такође већина ових апликација има могућност да веома често прави снимке екрана уређаја радника, а поједине омогућавају директне видео снимке екрана и није редак случај да ови необрађени подаци о слици су поређани у временској линији, чиме је омогућено шефовима да се врате кроз радни дан и виде активности радника у било ком моменту(Cyphers& Gullo,2020). Неколико апликација пружа могућност бележења сваког притиска на тастеру коју радник изврши, укључујући и непослату е-пошту као и приватне лозинке, чак пар њих је дозволило администраторима да се убаце и преузму даљинску контролу над радном површином корисника (Cyphers&Gullo, 2020). Оно што је евидентно је да bossware представља опасност по приватност и безбедност радника, тиме што бележи сваки клик и притисак тастера, тајно прикупља информације и користи друге функције, које превазилазе циљ контроле радника (Cyphers & Gullo, 2020). Изузетно озбиљан проблем код коришћења ове врсте апликација је то што ове апликације не праве разлику између активности везаних за посао и на пример банковних података, медицинских информација итд (Ascott, 2022). Постоји чак неки типови bossware-а који допиру до физичког света, око уређаја радника. Оно што је постала пракса да компаније које нуде софтвер за мобилни уређај, укључују праћење локације помоћу ГПС података. Две апликације StaffCop и CleverControl пружају могућност послодавцима да тајно активирају веб камере као и микрофоне на уређајима радника (Cyphers&Gullo,

2020). Постоје случајеви када је радницима пружена могућност да виде да их софтвер надгледа, и стојим им на располагању опција да укључе или искључе надзор, која је веома често уоквирена као „укључивање“ или „искључивање“, али уколико радник искључи праћење то ће бити видљиво послодавцу(Cyphers &Gullo, 2020). На пример у случају апликације Time Doctor, радницима може стајати на располагању опција да избришу одређене снимке екрана са своје радне сесије, ова опција је веома корисна јер пружа могућност заштите приватности запослених и спречавање прикупљања личних података, али приликом брисања снимка екрана, такође ће се избрисати повезано радно време, тако да радници добијају само време током којег се надгледају, такође поједине апликације попут Work Smart-a пружају могућност радницима да виде закључке система о њиховој активности представљене у виду графикона(Cyphers&Gullo, 2020). Као што се може закључити из до сада изложеног постоје различите врсте bossware-a тј. апликација за праћење продуктивности запослених, неке уколико се користе на етичан начин и поштујући права запослених могу бити од велике помоћи и побољшати ангажовање запослених, док су друге инвазивне и стварају осећај код запослених „великог брата“ који гледа (Drager, 2022). На пример Microsoft Productivity Score пружа могућност да послодавци виде прилоге дадотека које запослени шаљу е- поштом или дадотеке које чувају у Cloud-у, као и које пословне алате користе, ова апликација не спада у класичан bossware зато што он контролише цео тим, а не на индивидуалном нивоу, тако да пружа могућност компанијама да остану у позитивном односу са запосленима (Drager, 2022). Као пример инвазивнијег Bossware-a може се навести апликација Kickidler, алат за надгледање који пружа ова апликација омогућава послодавцу да погледа и сними екран запосленог у било ком тренутку, ова апликација такође пружа могућност keylogging и даљинског приступа, које се дефинишу као тешке функције, оно што је веома битно са становишта корисника тј. Послодаваца, ове опције се могу користити а да то запослени не примете (Drager, 2022). Као што је већ речено

наравно да постоје врсте bossware-а које уколико се користе на етичан начин и поштујући права радника, могу бити користан алат за рад и послодавцима и запосленима, као такав се може навести Microsoft Viva Insights, који на пример пружа подсетнике запосленима да направе паузе, а менаџерима податке о времену рада запослених (Drager, 2022). Веома је тешко открити постојање ових апликација, а поједине компаније захтевају од послодаваца да посебно конфигуришу антивирусни софтвер пре инсталирања њихових производа, како би се спречило да антивирус радника не би открио и блокирао софтвера за надзор (Cyphers & Gullo, 2020). Постоји велики проценат заступљености тј. коришћења bossware-а, а у прилог томе иде податак да неке од највећих компанија на свету користе bossware, укључујући и Универзитете, попут Универзитета Аризоне и Универзитета Емори, али и градови попут Денвера и Малибуа (Cyphers&Gullo, 2020). Резултати истраживања које је спровео Digital.com, показали су (Ascott, 2022):

- 14% запослених који раде од куће нису били свесни да су под надзором;
- 60% компанија које су примениле принцип рада на даљину користе софтвер за надзор и праћење продуктивности запослених;
- 53% запослених чија је активност била под надзором проведу три и више сати дневно на нерадним активностима;
- 81% компанија које су имплементирале софтвер за надзор забележило је повећање продуктивности радника;
- 86% компанија које користе софтвер за надзор је обавестило своје запослене о њиховој употреби.

Што показује да су у већем проценту присутни послодавци који приступају професионално и етички према радницима, али да постоји мали али значајан проценат оних који се немају такав приступ према радницима. Jude Lee, програмерка једне од ове врсте апликација дала је препоруке како запослени могу заштити своју приватност. Према њеном мишљењу најбоља

ствар коју запослени могу да ураде како би заштитили своју приватност, јесте да имају насумичне лозинке за различите налоге, и препоручује коришћење месинџера лозинки, као што је на пример LastPass; такође препоручује коришћење безбедносних мера које пружају поједине апликације, као што је на пример биометријско пријављивање; још једна њена препорука је да се два пута провере дозволе за апликације, и да се процени да ли су оне заиста неопходне. Истраживање Digital.com показало је да су индустрије које највише користе bossware маркетинг и оглашавање (83%), рачунарска и информациона технологија (77%), грађевинарство (71%), финансије и пословање (60%), производња (60%), и услуге личне неге (52%), као једно од објашњења за чешћу употребу софтвера за надзор у овим индустријама је то да су ово области у којима се клијентима често наплаћује по сату (Ascott, 2022). Из овога се може закључити да послодавци користе софтвер за праћење како би се осигурали у случају да клијенти доведу у питање легитимност наплативих сати, али послодавци требају да буду свесни чињенице да без обзира на повећање продуктивности, да ове апликације неће подстаћи флексибилно или удобно радно окружење за њихове запослене, као и да стално праћење негативно утиче на креативност, умањује поверење и да у значајној мери доприноси сагоревању запослених (Ascott, 2022).

2.2 Stalkeware апликације

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 итд., 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, најчешће су у питању чланови породице или партнери, а важно је нагласити да веома често физичко насиље произилази из дигиталног насиља (Информација, 2022а). 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). Оно што представља забрињавајућу чињеницу је то што постоји велики број популарних апликација које поседују одређене функције које им омогућавају надзор корисника, прикупљањем података о њима, и које се могу сматрати прикривеним stalkerwareom. 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 је показало да 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 stalkerwarea 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, 2022а). На Андроид уређаје се могу инсталирати све апликације, док постоји одређени број апликација које циљају искључиво IOS уређаје попут FlexiSPY и mSpy, а под инсталирањем stalkerware-а на циљани уређај се подразумева привилеговани приступ том уређају, што у ствари значи да stalkerware има физички приступ телефону и зна лозинку телефона, као што је случај са већином Андроид и Apple stalkerware-а или iCloud лозинке жртве тј. мете ове апликације, као што је случај са већином Apple stalkerware-а (Parsons, et al., 2019: 21). Заобилажења потенцијалних безбедносних обавештења на уређају који је мета ових апликација реализује се пре свега физичким приступом мобилном уређају који користи Андроид оперативни систем у комбинацији са одговарајућим приступним кодовима, који омогућавају оператеру да избегне ова обавештења, као и да добије тражене дозволе након преузимања ове апликације (Parsons, et al., 2019: 18). Могућност да жртва сазна или посумља на постојање ове врсте апликација спречена 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., 2019:18). У случају већине IOS stalkerware-а, обично stalkerware добије iCloud пријаву и лозинку од особе која је предмет надзора ове врсте апликација, чиме је омогућена двофакторска аутетификација тј. физички приступ откључаном уређају повезаним са iCloud налогом, а систем ће накнадно ексфилтрирати информације из iCloud окружења и учинити их доступним насилнику, важно је нагласити да у веома малом броју случајева IOS stalkerware може укључивати и инсталирање одређених апликација на IOS уређај (Parsons, et al., 2019: 18). Али важно је истраћи да такве инсталације је најчешће ослањају на искоришћавање постојања безбедносних недостатака у претходним

верзијама IOS –а, али IOS уређаји који имају најновије софтверске закрпе најчешће нису рањиви на ове врсте IOS stalkerware (Parsons, et al., 2019: 18). Према Kaspersky Lab-у корисници Андроид паметних телефона су у већем ризику у односу на iPhone, пошто је IOS значајно затвореније природе, али ни корисници Apple-их уређаја нису у потпуности безбедни, као што се из претходно реченог могло видети, а праћење iPhone је могуће уз физички приступ и jailbreaking(Информација, 2022а). Постоји много компанија на интернету које пружају услуге инсталације таквих апликација на новом телефону, и које га испоручују примаоцу у фабричкој амбалажи, што смањује шансу да жртва посумља на могућност постојања овакве апликације на минимум, а насилник може поклонити телефон на којем је инсталиран stalkerware жртви и на тај начин остварити жељени надзор (Информација, 2021б). Једна од слабости stalkerware–а је несигуран процес ажурирања који не потврђује аутентичност преузетог кода, што пружа могућност противнику треће стране позицију човека у средини, који може да убаци и инсталира произвољну апликацију уместо намераваног ажурирања, таква врста противника има могућност укључивања било кога на позицију која се налази између мете stalkerware–а и контролног сервера stalkerware–а, као и могућност да селективно модификује податке комуникације (Parsons, et al., 2019:55). Све ово ствара могућност противнику да покрене произвољан софтвер на уређају особе која је мета, чиме би било омогућено и оператору stalkerware–а и додатном трећем лицу да надгледа или управља мобилним уређајем особе која је жртва ове апликације(Parsons, et al., 2019:55). Обично произвођачи антивирусне и безбедносне индустрије означавају ове апликације терминима ПУА, што означава потенцијално нежељену апликацију, и термином ПУП, који значи потенцијално нежељени програм,а перцепција се састоји из њиховог означавања као оне које су злонамерне, или као само потенцијално нежељене од стране корисника (Parsons, et al., 2019: 55). Током последње деценије као последица експанзије паметних телефона, употреба stalkerware-а је нагло скочила, из разлога што пружа

могућност љубоморним партнерима да константно прате своје изабранике праћењем њихових телефона, поред ове чињенице и лака доступност stalkerware-а допринела је њиховој популарности, тј.експанзији (Информација, 2020г). Колико је велика заступљеност ове врсте апликација показује и извештај о резултатима анкете о дигиталној злоупотреби, у којој је учествовало више од 21.000 испитаника из чак 21 земље, а коју је спровела Kaspersky Security Network (KSN), која представља глобалну мрежу за размену информација о сајбер претњама, а подаци показују да је у 2021. години око 33.000 корисника било мета напада stalkerwarea**,** што представља историјски минимум, док је у 2020. години, близу 54.000 било мета напада ових апликација, а у 2019. године чак 67.000 људи(Информација, 2022а). Овај пад може се објаснити једноставном чињеницом да у почетку пандемије када су се спроводиле мере карантина и многе земље су спровеле закључавање, потреба насилника за овом врстом апликација је опала, пошто је кретање жртва било сведено на минимум. Може се претпоставити да је до повећања потражње за овом врстом апликација дошло након укидања мера закључавања. Процена Коалиције против stalkerware-а, коју чине представници ИТ индустрије и непрофитне организације, да је укупан број корисника који су мете ових апликација могао бити 30 пута већи, односно према овој процени око милион људи широм света сваке године постане жртва stalkerwarea (Информација, 2022а) Присутну експанзију ових апликација у значајном обиму добро илуструје и податак до којег је дошла анкета коју је спровео KSN, где се наводи да су учесници анкете који су изјавили да су их њихови партнери /супружници шпијунирали уз помоћ технологије, чиниле су чак 50% мобилне апликације, а земље у којима живи највећи број жртва stalkerware-а су Русија, Бразил, Сад (Информација, 2022а). Док се на првом месту у Европи налази Немачка (Информација, 2021б).

2.2.1 Знакови који који указују на постојање stalkerware апликација

Као што истиче компанија Kaspersky корисници тешко могу да препознају постојање stalkerware апликација, пре свега што ова врста софтвера остаје скривена, затим због тога што долази до скривања иконе stalkerware апликације на почетном екрану и у менију телефона, и чак долази до чишћење насталих трагова (Информација, 2021б). Али 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, 2021б). 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, 2020ђ). Још један начин на који корисници могу да утврде постојање stalkerware апликације је провера историје прегледача, пошто онај који их надгледа начешће је морао да преузме апликацију са неког веб сајта, и 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 је неопходно да провере дозволе инсталираних апликација с обзиром да stalkerware апликације могу бити сакривене под другим именом, са сумљивим приступом порукама, евиденцијама позива, локацији и другим сродним активностима (Информација, 2021б). Овде је указано на пар знакова који сугеришу на постојање ове врсте апликација, али да би се у значајној мери допринело у откривању ове врсте апликација и препознавање самих знакова који могу указати на постојање stalkerware апликација, кључна је едукација становништва, почевши од најмлађих до најстаријих чланова друштва. Али

свакако треба ставити акценат и на начин на који жртва треба да реагује у случају открића постојања stalkerware апликације и које мере треба да предузме, с обзиром да нису ретки случајеви да је брисањем апликације од стране жртве довело до тога да је жртва претрпела различите облике насиља. Не треба никако занемарити и велики значај и потребу жртве за психолошком помоћи у циљу лакшег суочавања са својим емоцијама и превазилажења тренутног стања, тако да је потребно организовати едукације становништва у виду различитих предавања и радионица које ће спроводити психолози. Такође неопходно је утицати на свест становништва о постојању и великој заступљености ове врсте апликација преко медија, како би се допрело до 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. 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 преузети као и како се психолошки суочити са насталом ситуацијом и тек тада се може рећи да је друштво испунило своју улогу.

2.2.2 Google play заштита од stalkerware-а

Инсталирана Google Play продавница пружа заштиту Андроид уређајима од stalkerware-а , уз помоћ Google Play Protect, то је услуга која је слична антивирусу и која скенира апликације које су учитане са стране, тј. инсталиране на телефон изван Google Play продавнице, он функционише на тај начин што скенира све апликације са стране пре него што се инсталирају, и ако се индетификују као злонамерне, спречава њихову инсталацију (Parsons, et al., 2019:44). Оно што представља проблем јесте чињеница да Google Play Protect може да се онемогући

из Google Play продавнице, што у ствари пружа могућност некоме ко има приступ телефону да заобиђе ограничења Google Play Protecta, а још већи проблем је чињеница да многе од ових апликација имају упуства на који начин онемогућити Google Play Protect (Parsons, et al., 2019:44). Међутим, важно је истаћи да се Google Play Protect може поново омогућити, како би се покренуло ручно скенирање инсталиране апликације, а након тога ће затражити од корисника да деинсталира све апликације које су индетификоване као злонамерне тј. штетне (Parsons, et al., 2019:44). Из претходног наведног може се извести закључак да Google Play Protect може да блокира само новије верзије stalkerware апликација, након периода од неколико дана, као додатни аргументи који потврђују ову тезу може се узети пример FlexiSPY тима за подршку, они су на њиховом форуму својим корисницима сугерисали да што пре испробају нове верзије, из разлога што постоји велика вероватноћа да Google Play Protect поново открије софтвер, и да ће вероватно бити откривена у року од дан или два (Parsons, et al., 2019:55). Најчешће су разлике између верзија појединих апликација минималне и углавном се састоје од промена кода верзије, броја у дадотеци и промена у броју верзије, ове мале разлике које се јављају у коду нам сугеришу да су потребне само минималне промене које ће омогућити stalkerware-у да избегне Google Play Protect (Parsons, et al., 2019:55). Али као што је већ речено у року од пар дана ће бити откривене. Занимљиви су резултати до којих се дошло прилоком једног тестирања. Тестирање се састојало из провере да ли ће Google Play Protect апликације чије је инсталирање блокирао поново уклонити ако је онемогућен, а апликација инсталирана и покренута, а затим поново омогућен Google Play Protect, дошли су до закључка, да би у сваком случају Google Play Protect тражио од корисника да уклони сваку апликацију, постављањем упита са опцијом деинсталирања (Parsons, et al., 2019:55). Важно је нагласити да су чести случајеви да када је Google Play Protect поново активан кориснику буде експлицитно постављено питање да ли жели да деинсталира stalkerware, што значи да га одмах не деактивира или брише,

овакво понашање Google Play Protect-а има позитивне стране, у виду тога да на тај начин обавештава жртву о постојању stalkerware-а али не излаже повећаном ризику од насиља, злостављања или узнемиравања, које би могло проузроковати брисање ових апликација (Parsons, et al., 2019:55). Али са друге стране поставља се питање да ли такава Google-ова одлука, да не уклони stalkerware, може одражавати да је stalkerware заправо пожељан, као на пример у случајно наводног легитимног праћења деце (Parsons, et al., 2019:55).

Из свега наведеног може се извести закључак да Google Play Protect пружа заштиту високог квалитета, али да постоје недостаци, односно простор за унапређење његове ефикасности. Пре свега скраћивањем потребног времена за индетификацију нових stalkerware-а, као и проналажење начина који би отежали онемогућавање Google Play Protect-а. А посебну пажњу код Google Play Protect-а треба посветити развијању опције која би спречила његово онемогућавање у самој Google Play продавници.

3. „Прикривене“ stalkerware апликације

Под појмом прикривених stalkerware апликација може се сматрати велики број популарних апликација које поседују одређене функције које им омогућавају прикупљањем података о корисницима и остваривања надзора над њима. Важно је нагласити да би апликације могле да прикупљају одређену врсту података о кориснику формално гледано потребна је корисникова дозвола за одређене функције. Али нису ретки случајеви у пракси да се прикупљају без корисникове дозволе, о чему ће бити реч даље у тексту.

3.1. 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 унапређење искуства или отклањања евентуалних проблема који се јављају, док са друге стране 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 апликација 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, eBay итд (БаштаБалкана, 2021). Пре свега не представљају све дозволе које се дају апликација „ризичне дозволе“, то се пре свега односи на оне дозволе које обезбеђују приступ подацима или ресурсима које укључују личне информације корисника, или на пример могу да потенцијално утичу на сачуване податке корисника, или 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 итд; 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%, на трећем месту се налази дозвола за читање СМС порука са 15% и на четвртом месту се налази дозвола за приступ евиденцији телефонских позива са 10% заступљености (Пајић, 2021). Вил Страфач 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, веома често не ради се 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 (РТС, 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 (РТС, 2020). Постоји велики број апликација у Google-овој 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 адресу 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 милиона 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. А међу тим апликацијама нашле су се и апликације Simple weather & clock widget, Speed Camera Radar, QR & Barcode Scanner итд (Објектив, 2022). Постоје бројне препоруке како спречити нежељено прикупљање података од стране апликација и на тај начин заштити своје податке. Пре свега како би смо заштитили податке потребно је 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). Као што се овде јасно види постоји више опција на располагању тако да различите категорије корисника могу пронаћи одговарајућу опцију у циљу заштите својих

података, у складу са сопственим афинитетима и финансијским могућностима. Од изузетан значај и неопходно 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, а у случају iOS апликација дозвола се може уклонити одласком у менији подешавања а затим је потребно кликнути на опцију приватност (Пајић, 2021). Значајан допринус у борби за заштиту података даје и употреба апликација AppCensus и CharlesProxy које је развио Серж Иглман, 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 може се закључити да „прикривене stalkerware апликације“ представљају стварну и велику опасност по безбедност корисника. С обзиром да прикупљају податке корисника а да он тога није ни свестан. Међутим, као срж проблема може се навести чињеница да знатан број корисника чак и када апликација има политику приватности не прочита је са пуном пажњом, него се преко ње веома често „прелети“ тј. аутоматски прихвате услови коришћења. Донекле разумевање се може имати за старије чланове друшва који нису имали прилику за стицање основних информатичких знања, али то исто се не може рећи за млађе чланове друштва, који такође веома често не прочитају политику приватности. Пре свега потребно је едуковати грађане о начинима заштите својих

података и на који начин њихови подаци могу бити злоупотребљени, како би се остварио значајан помак на овом пољу.

4. 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, 2019a). 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, 2019a). Званично је кренуо у борбу против stalkerware-а у јулу 2020. године која се састојала од доношењења измена смерница за огласе, и постављањем рока од месец дана компанијама да уклоне ове огласе али поред тога је било 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, 2020г). 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, 2020г). 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, 2020г). Међутим и након ове забране у Google-овим резултатима претраге могле су се пронаћи овакве апликације, Google је се правдао чињеницом да примена нових смерница није увек могуће одмах реализовати (Информација, 2020д). Истакао 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

он 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, 2020д). Оно што је спорно и што чини Google-ову политику непотпуну, 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, 2020д). Као што истиче и сам Malwarebytes, један од произвођача антивируса који активно учествује у борби против stalkerware-a, Google-овом политиком граница између апликација типа stalkerware-a и родитељског надзора је нејасна, а поред њега значајан допринос у борбу против stalkerware-a пружила је и Фондација за електронске границе, оснивањем Коалиције против stalkerware-a 2019.године (Информација, 2020д). Чланови ове групе су научници, компаније и непрофитне организације, циљ овакве коалиције је откривање, подизање свести о stalkerware-у, и борба против ове врсте апликација (Информација, 2020д). Евидентно је на основу до сада реченог да је Google доста урадио на пољу борбе против stalkerware-a, али да и даље постоји простора за надоградњу његове политике, пре свега бољом детекцијом „прикривених stalkerware" апликација, тј. апликација које су представљене у легитимне сврхе, а садрже поједине функције које омогућавају праћење корисника тј. надзор. Још једно поље на којем постоји простор за унапређење, је свакако и укидање stalkerware апликација за праћење деце, које су према тренутној Google-овој политици доступне у Play продавници.

5. Анализа пет stalkerware апликација

У овом делу раде биће представљене и анализиране пет stalkerware апликација, у виду приказа могућности које оне пружају својим корисницима и недостатака који постоје код ових апликација, са критичким осврtом тј. поређењем појединачне апликације у односну на другу апликацију. The TruthSpy је тајна апликација за надзор, која се користи за праћење активности на мобилном телефону, ова апликација налази своју примену како од стране родитеља који желе да шпијунирају своју децу, преко послодаваца који желе да надзиру своје запослене, до љубоморних партнера који желе да контролишу своје партнере (Kissiah, 2021). The TruthSpy поседује велики број опција, од могућности ГПС праћења, шпијунирања порука, тајно снимање телефонских позива, преглед фотографија и видео записа, историју прегледања интернета, слушање телефонског окружења уживо, преглед историје контаката, па све до шпијунирања апликација друштвених медија, попут WhatsApp, Snapchat, Facebook Messenger, Viber, Skype, Kik, Google Talk и Line Messenger; и снимања листе свих инсталираних апликација на телефону или таблету (Kissiah, 2021). На основу до сада реченог евидентно је да TruthSpy поседује велики број напредних опција у складу са савременим трендовима и потребама његових корисника. Продавац пружа могућност тестирања производа,у року од 48 сати ,слањем пробне верзије, што је још један разлог који доприноси популарности ове апликације. Top10SpySoftware и TrustPilot. com, му дају оцену 2, од 5 звездица, што представља лошу оцену а и рецензије корисника су такође биле лоше (Kissiah,

2021). На основу рецензија и саме оцене корисника, може се рећи да ова апликација није једна од квалитетнијих stalkerware апликација, као и да њене функције не пружају све могућности које продавац наводи. Spyera је апликација која је се користи за надзор деце и дизајнирана је за мобилне телефоне, рачунаре и таблете (Black, 2021a). Након инсталирања пружа могућност својим клијентима да прате позиве своје деце, мејлове, медијске дадотеке, СМС поруке, историју претраживача, као и налоге на друштвеним мрежама, ради на већини Андроид и IOS уређаја, као и на личним рачунарима а на сајту spyer-е може се проверити компатибилност апликације са марком или моделом телефона клијента (Black, 2021a). Упркос тврдњама Spyera да је „најпродаванији софтвер за праћење који се не може открити“, на Trustpilot.com постоји велики број негативних повратних информација о њиховим услугама, а оцена ове апликације износи 2,7 звездица што представља лошу оцену (Black, 2021a). Оно што представља велики минус код ове апликације, јесте чињеница да њихов тим није одговорио на критике у последњих пар месеци, а да саме негативне критике чине чак 40% укупног броја повратних информација купаца (Black, 2021a). Као и за претходну апликацију и за Spyer-у се може рећи да није једна од квалитетнијих stalkerware апликација, и њене функције не пружају пласиране могућности, и самим тим незадовољају потребе својих корисника и спада у ред мање коришћених апликација. А свакако највећи минус ове апликације је чињеница да креатор/и Spyera нису уважили критике својих корисника, које се јављају у значајном проценту и посветили пажњу уклањању недостатака и унапређењу могућности које ова апликација пружа, што даље имплицира да се не поклања довољно пажње корисницима ове апликације и њиховим потребама. FlexiSpy је тајна апликација за надзор, која пружа могућност онлајн и офлајн шпијунирања циљаног уређаја, као и прегледање и снимање позива, прегледање СМС порука и порука на друштвеним мрежама, блокирање апликација, праћење локације, и снимање слика и видео записа итд (Ugwu, 2022). Једна од напредних функција пружа могућност даљинског снимања камере, која

омогућава кориснику да контролише камеру циљаног уређаја и снима слике и видео записе, а ту је и опција keylogger, која је нова функција апликације и она бележи све лозинке, корисничка имена или кодове откуцане на циљаном уређају (Ugwu,2022). У напредне функције спада свакако и функција пресретања позива и лажне СМС поруке, као и функција слушање уживо уз помоћ које корисници ове апликације могу пресрести телефонске позиве са другог телефона ; а једна од напредних фукција FlexiSpy је свакако и функција упозорења о локацији, која пружа могућност кориснику да постави упозорење за одређену локацију, а радијус се може подесити на најмање 50 метара, а највише 10 км (Byrant, 2022). FlexiSpy је компатибилан са Андроид и IOS уређајима (Ugwu,2022). Као још једна позитивна страна са становишта корисника поред компатибилности је и што не утиче негативно на перформансе телефона, тј. не проузрокује загревање телефона, ни трошење батерије брзо, тако да практично шансе да жртва посумља на постојање ове врсте апликације не постоје или су сведене на минимум (Byrant, 2022). Али и као све апликације и ова апликација има недостатке. Недостатак представља сам процес инсталације ове апликације, за који се може рећи да је прилично тежак и да захтева завидан ниво информатичког знања, још један недостатак је и одуство неких функција који имају други конкуренти, попут блокирања веб локација и телефонских бројева (Ugwu,2022). Као још један недостатак може се навест и то што су неке напредне функције доступне само ако је телефон roo-тован или jailbroken. Цена апликације такође представља лошу страну, где средњи пакет кошта чак 68 долара. На основу реченог може се закључити да ова апликација спада у ред најквалитетнијих stalkerware апликација, али свакако и у ред апликација за којима влада највећа потражња, због могућности које ова апликација пружа а међу којима се налази не мали број функција које пружа само ова апликација, попут пресретања позива и лажних СМС порука. У односу на претходне две анализиране апликације ова апликација је далеко квалитетнија на основу могућности и напредних опција које ставља на располагање својим

корисницима. Copy9 је тајна апликација за надзор која омогућава шпијунирање деце, запослених или партнера (Get app solution, 2022a). Представља подбренд апликације The TruthSpy (Black, 2021b). Ова апликација има више од тридесет функција које омогућавају надгледање СМС порука, позива, ГПС локације, праћење дрштвених апликација као што су WhatsApp, Viber, Facebook,Yahoo Messenger и Skype, као и управљање позива, преглед бележака и мултимедијске дадотеке, прегледање историје контаката и снимање околине и друге (Get app solution, 2022a). Шпијунски позив представља занимљиву функцију с обзиром на њен начин рада, који се састоји из упућивања позива са телефона корисника на телефон жртве, телефон жртве ће аутоматски одговорити на позив ако је закључан екран а притом не долази до вибрације, звука или светла, нити било каквих знакова који би показали долазни позив а ако се циљани уређај користи позив ће бити одбијен, попут заузетог позива (Get app solution, 2022a). Компатибилан је са Андроид и IOS уређајима (Get app solution, 2022a). Као недостатак ове апликације може се навести податак да Copy9 забрањен од стране система за претрагу 2018. године, и да од тада није ажурирана (Black, 2021b). Још један недостатак је свакако проблем који се јавља са функционисањем праћења порука, понекад је потребно од 1 до 3 дана да се виде нове поруке, на корисничкој контролној табли јавља се и недостатак је у вези са функцијом снимања телефонских позива, која је доступна само за Андроид уређаје, где постоји проблем са неким врстама Андроид уређаја и рада ове фукције а снимање је могуће свега неколико минута (Get app solution, 2022a). На основу свега реченог јасно је да је апликација застарела с обзиром да је последње ажурирање било 2018. године и да спада у ранг апликација ниског квалитета, с обзиром на проблеме који се јављају у раду појединих функција. На основу до сада анализираних апликација може се рећи да ова апликација има већи број недостатака, али свакако највећи минус ове апликације је чињеница да је 2018. године забрањена од стране система за претрагу и да од тада није ажурирана, што имплицира да није у стању да конкурише другим апликација, пре свега због

застарелости и недостатка праћења развоја технологије у овој индустрији у виду напредних опција попут оних које пружа апликација FlexiSpy. mSpy је популарна апликација за тајни надзор, пружа могућност прегледа СМС порука, историју позива, ГПС локацију, преглед апликација попут Vibera, Instagrama, WhatsAppa, Snapchata, Facebooka, Kika, Linea, затим преглед фотографија и видео записа, е-поште, контаката, белешки, активности календара, историју претраживања и друге (Get app solution, 2022b). Занимљиво је да ова апликација пружа и могућност ограничења долазних позива, као и инсталирања појединих апликација, а све ове могућности заједно пружају кориснику да има скоро апсолутну контролу над циљаним уређајем (Get app solution, 2022b). Компатибилан је са Андроид и IOS уређајима, а као недостатак ове апликације може се навести то да је за IOS уређаје неке функције захтевају од корисника да направи jailbreak (Get app solution, 2022b). Још један пропуст је свакако недостатак напредних опција за надзор тј. шпијунирање телефона, попут снимања позива, тајног активирања микрофона и снимање околине, као и тајног активирања камере мобилног телефона (Praćenje mobitela, 2018). На основу свега реченог о овој апликацији, може се закључити да ова апликација спада у ред најквалитетнијих stalkerware апликација, а самим тим и најтраженијих. Поређењем могућности које пружа ова апликација својим корисницима и могућности које ставља на располагање FlexiSpy, притом треба нагласити да обе спадају у ранг квалитетнијих апликација, евидентно је да је FlexiSpy квалитетнија апликација која поседује великој број напредних опција које друге апликације не поседују, па и mSpy. Попут функције пресретања позива и лажних СМС порука, као и функција упозорења о локацији која пружа могућност кориснику да постави упозорење за одређену локацију, а радијус се може подесити на чак 10 км.

6. Људска права у дигиталној сфери

Као резултат дуге, тешке и вишевековне борбе за једнаки третман свих људи независно од боје коже, националне и расне припадности, друштвеног статуса, дошло је до формулисања људских права усвајањем Универзалне декларације о људским правима 1948. године, од стране Генералне скупштине УН. Под појмом људских права подразумевају се права које поседује сваки човек својим рођењем. Временом су развијени бројни механизми њихове заштите од устава, закона до међународних уговора и декларација. Људска права су регулисана и загарантована бројним међународним документима, који остављају врло мало простора за нејасноће, попут Универзалне декларације о људским правима (1948), Међународног пакта о грађанским и политичким правима (1966), Међународног пакта о економским, социјалним и културним правима (1966), затим Европска конвенција о људским правима (1950), Повеља Европске Уније о темељним правима итд. Док сте то исто не може рећи за њихову заштиту у дигиталној сфери. Интернет као светски систем умрежених рачунарских мрежа или како се често користи израз „мрежа свих мрежа“, повезује велики број корисника широм планете, омогућава им брзу, лаку и једноставну комуникацију, едукацију, забаву, културу итд. Међутим често се заборавља да приликом деловања у овом простору остављају се подаци који остају трајно записани, који касније могу бити предмет бројних манипулација, модификација и злоупотреба. Што је произвело потребу регулисања ове области и заштите људских права у дигиталној сфери. Први кораци како би се остварила и заштитила људска права у дигиталној сфери су учињени, али и даље постоје празнине и ограничења за њихово остваривање. Веома је значајна Конвенција о заштити лица у односну на аутоматску обраду личних података, коју је донео Савет Европе 1981. године, циљ конвенције је био да се прошири област заштите основних права и слобода појединаца, са посебним

акцентом на приватност података (Прља и сар.,2012: 90). Такође је значајна Конвенција о високотехнолошком криминалу која је донесена 2001. године, којом је регулисана област поверљивости, целовитости и доступности рачунарских података и система (Матијашевић и сар., 2012:42). А новијег датума може се навести Декларација о будућности интернета, која је донесена у априлу ове године, која има циљ обезбеђивање поузданог, безбедног и слободног глобалног интернета у будућности (Политика, 2022). Остваривање људских права и њихова заштита у дигиталној сфери отежана је, а чести су и случајеви њиховог грубог кршења. Најчешће се повреде људских права у дигиталној сфери манифестују у виду повреде приватности, претњи, увреда, притисака и манипулација. У највећем броју случајева угрожавање људских права у дигиталној сфери је у форми угрожавање приватности, које се остварује у виду прикупљања приватних података корисника од стране различитих апликација, при том нису ретки случајеви да оне прикупљају податке без корисникове дозволе, затим често се дешава да подаци корисника буду угрожени од стране држава, као на пример за време пандемије корона вируса, када су развијене различите апликације а државе у сарадњи са провајдерима имале су на располагању велику количину информација. Што је опет стварало могућност злоупотребе у тоталитарним режимима, мада нису ретки случајеви у историји да су демократске земље злоупотребиле податке у циљу остварења масовног надзора над становништво. Ова тврдња може се поткрепити открићем Едварда Сноудена, да америчке и друге западне службе прислушкују своје грађане и прикупљају њихове податке. Велики проблем представља чињеница да се заштита људских права попут права на приватност ослањају на приватне тужбе, што ствара велике тешкоће у остваривању њихове заштите. Судска пракса је показала и велике тешкоће у доказивању кршења одређеног права, где са једне стране је потребан одређени ниво информатичког знања жртве, како би на адекватан начин сачувала доказ и не би дошло до његовог уништења. Главни проблем недовољне заштићености

људских права јесте проблем регулисања Интернета, и одређивање надлежности држава за одређену активност која се одвијала на Интернету , пре свега јасно је да рачунарска или комуникациона опрема кроз коју се одвијала активност на Интернету може бити индетификована на више локација или пак једној (Сурчулија, 2010: 21). „ Проблем се јавља када две или више држава прогласе своју надлежност над истом активношћу која се одвијала на Интернету“ (Сурчулија, 2010: 21). У тој ситуацији поставља се питање која ће држава бити јача и преузети случај (Сурчулија, 2010: 21). „Решавање питања приватности и безбедности у електронским комуникацијама захтева свеобухватан приступ, укључивање широког круга заинтересованих и усаглашавање многих, често различитих потреба и интереса“(Вермезовић, 2016: 250). На основу свега реченог у овом делу рада, може се закључити да један у низу проблема у заштити људских права свако је преклапање надлежности држава, што указује на недовољну уређеност на међународном плану, али и на недовољну усаглашеност националних законодавстава са међународном регулативом. Евидентно је да су учињени први кораци у регулисању заштите људских права у дигиталној сфери, али да и даље постоји велики простор за унапређење заштите, у виду доношења нових докумената и програма за њихову имплементацију на међународном плану, али поред тога свакако треба ставити акценат на активности појединачних држава у циљу побољшања остваривања људских права у дигиталној сфери, кроз доношење националних законодавних решења, затим организовања едукација становништва у циљу бољег разумевања и познавања својих права и начина њихове заштите.

7. Мере заштитите од тајних апликација за надзор

Пре свега потребно је предузети мере заштите уређаја од stalkerware апликација, како би се шанса за инсталирањем ове врсте апликација свела на минималну могућност. Иако постоји мали број мера које могу у одређеном проценту али не и потпуности да заштитите уређај, потребно је ове мере познавати и максимално их искористити. Део тих мера је и коришћење PIN кода или других начина провере индетитета, као што је на пример отисак прста, затим инсталирање антивирусног софтвера који ће третирати stalkerware као нежељени програм и који такође може уколико ипак дође до инсталације помоћи кориснику да га уклони (Информација, 2020). Примери добрих антивирусних програма су Norton, McAfee, BitdDefener и Avira, а у случају открића постојања stalkerware апликација постоји неколико мера које се могу предузети у циљу уклањања, једна од њих је мера рестартовање уређаја на фабричка подешавања, али прилоком предузимања ове мере потребно је да корисник прво направи резервну копију својих видеа, контаката и фотографија, овде једини проблем представља то што постоји могућност да резервна копија такође садржи stalkerware (it mixer, 2022b). Рестартовање уређаја на фабричка подешавања може представљати проблем због брисања целог софтвера, али ће такође избрисати и stalkerware, затим stalkerware се може уклонити надоградњом оперативног система, ово није поуздана мера, али у неким случајевима може бити ефикасна, пошто неки типови stalkerware-а раде само на старијим верзијама оперативног система, што значи да се stalkerware може уклонити надоградњом оперативног система (it mixer, 2022b). Важно је нагласити да постоји и могућност ручног уклањања stalkerware-а са уређаја , то је могуће урадити покретањем телефона у безбедном режиму, а затим треба уклонити све сумљиве апликације са посебним акцентом на оне које су непознате кориснику а уколико корисници нису сигурни, препоручује се да потраже информације о

сумљивој апликацији, да би видели да ли су и други корисници имали проблеме са њом (Информација, 2020ђ). Још један корак који се може предузети је и инсталирање TinyCheck, који је развила компанија Kaspersky Lab, он је алат који омогућава дискретну проверу да ли на уређају постоји шпијунски софтвер, TinyCheck се не инсталира на телефон већ на посебни спољни уређај, а сам алат функционише као посредник између корисниковог Wi-Fi рутера и телефона (Информација, 2022а). А након инсталације TinyCheck анализира интернет саобраћај уређаја у реалном времену и ако шаље много података шпијунским серверима TinyCheck ће обавестити корисника, једина мана овог алата је то што је потребан одређени ниво техничког знања (Информација, 2022а). Као што је речено и за препознавање знакова који указују на постојања stalkerware апликација на мобилном уређају и код предузимања мера уклањања и заштите од ове врсте апликација, потребно је да корисници буду упознати са мерама, а ту је свакако кључна едукација.

8. Закључак

У раду је на свеубохватан начин обрађена област тајне апликакције за надзор, кроз само дефинисање појма stalkerware апликације, који се односи на апликације које се користе у циљу праћења деце и партнера/супружника и појма bossware апликација, које користе послодавци у циљу надзора својих запослених, како би имали увид у рад својих запослених и ниво њихове продуктивности. Затим су приказане поједине stalkerware и bossware апликације, Google-ова политика према тајним апликацијама за надзор, заштита коју пружа Google у виду Google Protect-а, али и сами знаци који указују на постојање тајних апликација за надзор на мобилном уређају као и мере заштите и мере које се предузимају ради уклањања ових апликација. А у завршном делу рада је указано на опасности по безбедност података које изазивају „ прикривене stalkerware апликације“ и у којој мери су остварена и заштићена људска права у дигиталној сфери. На основу свега презентованог у овом раду може се закључити да је ово веома значајна и комплексна тема, којој у будућности треба поклонити више пажње. Оно што је евидентно и у раду већ речено да је током пандемије корона вируса дошло је до експанзије bossware апликација као последица мера у циљу спречавања корона вируса и преласка на онлајн рад од куће, док је са друге стране у случају stalkerware апликација дошло до пада потражње као последица ограничења кретања и затварања, тако да је потреба насилника за овом врстом апликација опала. Тајне апликације за надзор представљају изузетно опасне и штетне апликације, јер пружају могућност потпуне контроле над животом особе која је

мета ове врсте апликација. С обзиром на потребу корисника ових апликација да имају увид и контролу над животом друге особе може се закључити да су у питању нестабилне личности, које могу бити и склоне насиљу. Веома често мете ових апликација искусе неки облик насиља од стране корисника ових апликација, а у прилог томе иде податак Европског института за равноправност полова, чија статистика потврђује повезаност између оваквог праћења и физичког злостављања, чак 7 од 10 жена у Европи које су биле мете ове врсте апликација такође су доживеле барем један облик физичког или сексуалног насиља од стране партнера (Информација, 2021б). Бројне су негативне последице утицаја овакве врсте апликација, од физичких повреда до настанка психолошких и емоционалних повреда у виду стида, страха, губитка достојанства, као и психичке болести изазване траумом (Parsons, et al., 2019:17). Не треба заборавити да је ту присутна и финансијска штета, у виду трошкова везаних за правну подршку, услуге заштите на мрежи и друге (Parsons, et al., 2019:17). Како би се спречио настанак негативних утицаја ових апликација и људи били у стању да препознају знаке који указују на постојање ове врсте апликација и да адекватно реагују, тј. предузму адекватне мере у циљу уклањања ових апликација, кључни акценат је на едукацији становништва о овим апликацијама. Као што је у раду већ речено потребно је информисати људе преко медија, како би се допрло до што већег броја људи, али и кроз школски систем и организовањем различитих програма, курсева и едукативних радионица. Само на тај начин могу се остварити позитивни резултати у борби са овом врстом апликација.

9. Литература

Ascott, E. (2022). Bossware: 14% of remote employees are unaware they' re being monitored. Преузето 28. априла 2022. године, са https://allwork.space/2022/03/bossware-14-of-remote-employees-are-unaware-theyre-being-monitored/

Black, D.(2021a). What can our Spyera review tell you in 2022: Is the software relevant nowdays? Преузето 29. априла 2022. године, са https://blog.mspy.com/spyera-reviews/

Black, D. (2021б). Why is Copy9 app not relevant in 2022?. Преузето 29. априла 2022. године, са https://blog.mspy.com/copy9-review/

Byrant, F. (2022). FlexiSpy review: High quality comes at a price. Преузето 29. априла 2022. године, са https://spydrill.com/flexispy-review/

Cyphers, B. & Gullo, K. (2020). Inside the invasive, secretive „ Bossware“ traking workers. Преузето 27. априла 2022. године, са https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

Drager, N. (2022). What is Bossware? What you need to know about the new employee surveillance trend. Преузето 28. априла 2022. године, са https://quantumpc.com/bossware-employee-surveillance/

Get app solution. (2022a). Review of Copy9: Features and compatible what zou need to know. Преузето 29. априла 2022. године, са https://bs.getappsolution.com/copy9-review/

Get app solution. (2022b). mSpy review 2022: The best mobile monitor app for Android and iPhone. Преузето 29. априла 2022. године, са https://bs.getappsolution.com/mspy-review/

Han, Y., Roundy, K. & Tamersoy, A. (2021). In: Towards Stalkerware Detection with Precise Warnings.(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. Магистарски рад. Queensland: Faculty of arts, business, informatics and eucation, school of information communications technologies.

It mixer. (18. јул 2019а). 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/

It mixer.(2022б). Како препознати симптоме шпијунског софтвера и ако да уклоните „stalkerware". Преузето 27. априла 2022. године, са https://it-mixer.com/kako-prepoznati-simptome-spijunskog-softvera-i-kako-da-uklonite-stalkerware/

Kissiah, M.(2021). The TruthSpy. Преузето 29. априла 2022. године, са https://www.einvestigator.com/thetruthspy/

Praćenje mobitela. (2018). mSpy рецензија- Детаљни преглед свих могућности за праћење мобилног телефона. Преузето 30. априла 2022. године, са
https://www.pracenjemobitela.com/recenzije/mspy-recenzija/

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

Ugwu, C.(2022). FlexiSpy review. Преузето 29. априла 2022. године, са https://techjury.net/reviews/flexispy-review/#gref

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? У: Зборник радова Правног факултета у Нишу.(стр. 249-265). Ниш: Правни факултет.

Информација. (15. април 2022а). 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. (2. март 2021б). Упркос Googleовој 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. (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. (10. јул 2020г). 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 2020д). И после Googleove 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

Информација. (9. октобар 2020ђ). 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

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

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/

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/

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

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

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

Сурчулија, Ј. (2010). Регулаторни изазови слободе изражавања на Интернету. У: Слобода изражавања на интернету. (стр. 19- 25). Београд: Центар за развој Интернета.

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

ИЗЈАВА О АКАДЕМСКОЈ ЧЕСТИТОСТИ

Изјављујем да сам у приложеном раду поштовао/ла сва правила о академској честитости.

Овај писани рад резултат је искључиво мог личног рада, темељи се на мојим истраживањима и ослања се на наведену литературу.

У Београду, дана _____ године.

Потпис студента:

_____