УДК 343.533::004
DOI: https://doi.org/10.5937/bastina32-35814

Прегледни рад

*Ђорђе М. МИЛОШЕВИЋ**
Министарство унутрашњих послова Републике Србије, Београд

ФРЕКВЕНТНИ ОБЛИЦИ ИСПОЉАВАЊА ИНТЕРНЕТ ПРЕВАРА

Апстракт: Увећање обима електронских трансакција довело је до нужности за појачањем заштите података, од криминалних активности у онлајн окружењу. Аутор истиче да је циљ извршилаца ових илегалних радњи лукративне природе, који може бити испуњен и самим нарушавањем информатичког система, као и да они могу бити како физичка тако и правна лица. Профил сајбер криминалца, углавном, поздразумева одлично познавање дигиталног поступања, искуство кретања у онлајн окружењу и активну примену информатичких вештина. Интернет је постао неодвојивни део данашњег начина живота због чега се непрестано шири опсег криминалних активности у овој светској мрежи за комуникацију и размену података. Аутор у томе види разлог за растом потребе јачања информатичке безбедности, коју детерминише као практичну примену мера за заштиту података од спољних утицаја у онлајн средини. У овом раду презентована је статистичка анализа фреквентних облика превара на интернету у периоду од 2016. године до 2020. године, у циљу приказивања реалног интензитета ове врсте савремене криминалне претње.

Кључне речи: интернет, интернет преваре, онлајн окружење, сајбер криминал, информатички систем, информатичка безбедност, сајбер криминална претња

УВОД

У дигиталном добу, информације су постале важан економски ресурс, тако да се сматрају суштинским средством за мерење успеха или неуспеха на нивоу појединца, организације и заједнице, као и на националном и међународном нивоу, и суштински фактор у концепту развоја. Стога је безбедност података постала важно питање и све већа потреба, који утиче на све секторе друштевног живота без изузетка. Али, како је све почело?

Током 60-их године прошлог века напади на комуникације сводили су се на злоупотребу интерконтиненталних позива у оквиру фиксне телефоније, који су били намењени у забавне сврхе и на преусмеравање финансијских средстава са рачуна приватних и државних корисника фиксних телефонских бројева. Две деценије касније, програмери су почели састављање злонамерног програма, из кога су се развили облици његових самоумножавајућих верзија којима су нападани системи појединачних корисничких рачунара. Финансијски криминал 90-их година

* докторан т, djodjolos@gmail.com

прошлог века вршио се неовлашћених упадима и пласирањем субверзивних софтвера у тадашње рачунарске системе, који су са индивидуалног улазили у фазу мрежног развоја. Нови правци хакерских напада били су усмерени на рањивости таргетираних система и брзу злоупотребу података пре затварања сигурносних пропуста. Комуникација електронском поштом, заправо, је била безбедносно лоше осмишљена опозитно брзини њеног развоја, што је допринело стварању неконтролисаног тока нежељених комерцијалних и лажних електронских порука, као и фантомских електронских адреса. Половином прве деценије овог века, забринутост око физичке безбедности система за електронско гласање подигла је свест јавности о могућностима сајбер криминалне претње и учесталости хакерских напада. Извршени су информатички упади у рачунарски систем компаније CNN у америчком граду Атланти, али и нивоу целе савезне америчке државе Џорџије. Нанета штета износила је 5.000 долара због злоупотребе веб сајтова који су били повезани са CNN.com локацијом на интернету, а на месечном нивоу било је учињено 2.000 неовлашћених приступа наведеном сајту и његовим везама. Остале илегалне активности односиле су се на неовлашћене приступе веб локацијама неколико америчких колеџа у држави Џорџији (Kabay 2008).

Може се рећи да су последње деценије прошлог века биле богате циљевима за сајбер криминалце. На срећу, за компаније и кориснике који уносе своје осетљиве податке на веб, хакери су прво направили штету на самим веб сајтовима, уместо да се фокусирају на осетљиве информације које се налазе у системима. Било је потребно више година да криминална експлоатација туђих података на интернету превазиђе ниво доказивања, побеђивања система и демонстрирања властитих вештина, како би дефинисала свој лукративни циљ (White 2013). Два догађаја, тада, су ишла на руку информатичким криминалцима. Први је било откриће светске мреже веба World Wide Web, чије три кључне компоненте су веб сервер, веб претраживач, веб едитор и пратеће прве веб странице. У току 1991. године, уследило је омогућавање доступности овог пројекта на интернету у функционалној форми веб – светске мреже за комуникацију. Сасвим изненађујуће, веб је порастао и дизајнирао преко 17.000.000.000 нових веб локација. Други догађај је био састављање глобалних тачака за приступ вебу. Године 1994. америчка Национална научна база спонзорисала је четири пословне групе за изградњу јавних тачака приступа интернету. Ове пословне групе биле су: Pacific Bell Company, WorldCom Company, Sprint Company и Ameritech Company. У првој деценији овог века, криминалне активности на вебу развиле су се од повремених индивидуалних хакерских операција до узастопних илегалних поступања подржаних изузетно напредном и уједначено координисаном незаконитом информатичком логистиком. Бројне врсте хакерских активности биле су познате из претходних деценија, али у конкретним случајевима више није долазило до понављања истоветних криминалних поступања са штетним последицама подударајућег обима (White 2013).

Сада се скоро сви писани, звучни и видео садржаји приказују на онлајн мрежи, од електронске управе и електронске трговине до друштвених медија, јер је сваки део живота постао доступан на интернету. С друге стране, сајбер криминалци имају бројне могућности остваривања приступа овим информацијама како би их

злоупотребили и користили у своје сврхе. Ово доприноси потреби за јачање информатичке безбедности јер данас свако има личне податке доступне у онлајн окружењу. Неки догађаји утичу на сајбер безбедност, попут развоја технике и технологије, ширења епидемија и изазивања и вођења оружаних сукоба.

Сајбер безбедност можемо одредити као праксу заштите информација и података од спољних извора на вебу, јер експерти за сајбер безбедност штите мреже, сервере, интранете и рачунарске системе. У складу са остваривањем ове врсте безбедности поступања у онлајн окружењу неопходно је поштовати принцип да само овлашћена лица имају приступ заштићеним информацијама због тога што су осетљиве јер су личне или поверљиве природе (Nfuka, Sanga et al. 2014). Сигурност података се односи не само на њихову инорматичку заштиту, већ и на изградњу свести о могућностима неовлашћене употребе, приступа, модификације или уклањања података на вебу. Само такав приступ омогућује интегрисану безбедност података у онлајн окружењу, у односу на претње од хакерских напада, интернет превара и сајбер крађа и злоупотреба (Nfuka, Sanga et al. 2014).

ЗНАЧАЈ ПОДАТАКА НА ИТЕРНЕТУ

Подаци се процењују као информациони систем *per se* који има неко своје аутономно значење. Свака информација представља неку врста података, али немају сви подаци значење информације. Када се одређене чињенице чувају у посебном аутоматском систему за обраду података, оне се сматрају подацима. Тек када се ти подаци обраде према критеријумима функције и значења, добију својство информације. Податак или подаци сада у функционалној и вредносној форми информације постају својеврсна мета за сајбер криминалце, јер сада постају ресурс који је изложен утицају спољних извора. Важно је имати у виду да се ови спољни извори нужно не морају налазити у онлајн окружењу интернета.

Лични подаци који се могу злоупотребити у интернет преварама, сада су доступни јавности на нашим налозима за приступ садржајима на веб сајтовима друштвених медија. Осетљиве информације као што су бројеви социјалног осигурања, картични подаци и детаљи о текућем рачуну сада се складиште и чувају у тзв. облаку на интернету. Дакле, јавно и приватно ослањање на рачунарске системе расте из дана у дан. Безбедност услуга у вебовој облак бази података, комуникационо-дигиталне могућности паметних телефона и информатичка технологија интернет ствари, чине да су капацитети држава широм света све више окренути ка уочавању сајбер криминалне опасности и креирању мера и систем заштите у односу на њену све интензивнију глобалну заступљеност.

Индустрија сајбер безбедности може на добар начин обезбедити развој система за безбедност информација. Сајбер криминал је недозвољена активност на вебу која подразумева постојање корисничког рачунара и информатичке мреже за комуникацију. Кориснички рачунар је средство које се користи у извршењу кривичног дела, али може бити и мета сајбер напада. Људи се, у односу на раније историјске периоде, све више ослањају на технологију и нема знакова да ће се овај тренд успорити.

Пандемија коронавируса довела је до тога да највећи број запослених радне задатке обавља на даљину путем кућних рачунара и интернета. Многи појединци су из свог кућног окружења обављали пословне обавезе и били принуђени на опрез у поступању, посебно у односу на опасност фишинга (phishing) по личне и пословне податке јер ова врста криминалних активности на вебу има изузетну динамику развоја нарочито се користећи страхом од корона вируса ради злоупотребе поверења корисника интернет услуга. Због пандемије на локалном нивоу, рад од куће постаје тренд који доприноси ширењу и јачању сајбер криминалне претње. Ипак, запослени у највећем броју случајева располажу минималним средствима за примену мера сајбер безбедности у приватном и професионалном онлајн окружењу, у односу на избор могућности које су им доступне на вебу и у којима се крију замке сајбер криминалаца.

Интернет преваранти се користе околностима широко распрострањене панике и успевају да обману жртве на вебу садржајима о корона вирусу који су увек другачији, како би изазвали страх и преварно дошли до података из нечијег личног или радног окружења. На овај начин, настају трошкови сајбер криминала који обухватају ширење неистинитих садржаја, осиромашивање могућности за стицањем знања, брисање приватних и пословних информација, успоравање радног тока, крађу готовинских уплата, опструирање ефикасности, недозвољено преусмеравање и злоупотребу личних и ресорних података, као и криминално присвајање финансијских средстава (Tabrez 2020).

ПРЕВАРЕ НА ИНТЕРНЕТУ

Околности које доприносе јачању сајбер криминалне претње, такође, доводе и до пораста криминалних активности на итернету, обзиром на креирање онлалјн окружења које им изузетно погодује. Следеће чињенице говоре томе у прилог. Кориснички рачунари су постали јефтини, а паметни телефони су се претворили у мултифункционалне носаче информација, при чему су и једни и други изложени околностима веба у којима су доступне бесплатне апликације и продубљени нивои електронских трансакција без пропорционално ефективног присуства мера сајбер безбедности.

Већина људи користи свој паметни телефон за управљање финансијским операцијама или поступање са осетљивим личним и пословним информацијама. Већина телефона се тренутно користи за двофакторску верификацију, што је један од најшире коришћених модела сајбер безбедности. Безбедносни ризик је повећан, ако се мобилни телефонски уређај изгуби или буде украден.

У концепту интернета ствари, сами уређаји су без ваљане заштите јер највећи број њих нема интерфејс клијента. У окружењу интернета ствари, конкретни паметни уређаји су немоћни, јер значајан део њих нема интерфејс клијента. Ово може довести до проблема у разумевању које врсте информација сам уређај прикупља или надгледа, због чега постаје улазна тачка за интернет нападача, који га користи за покретање напада дистрибуираним ускраћивањем услуге (Distributed Denial of Service – DDoS).

С друге стране, интернет ствари (Internet of Things – IoT) није планиран да буде предмет сајбер безбедности, јер би стављање акцента произвођача на заштиту података значајно увећало трошкове производње ових кућних апарата, као и информатичке подршке потрошачима који их свакодневно користе у својим домаћинствима (Gravrock 2019). Већина одлика које чине предност вештачке интелигенције, нажалост је изложена онлајн злоупотреби и врло вероватно може да служи у криминалне сврхе. Овоме, свакако, доприноси чињеница да су системи вештачке интелигениције у технолошком обрасцу интернета ствари јефтини, разноврсни и анонимни.

Са гигантским развојем технологије, посебно у области интернета ствари и информатичких технологија, комуникација са онлајн жртвом мора бити изузетно једноставна. Сајбер криминалци користе за интернет преваре обману жртве да би добили њене приватне податке. Углавном је пласирање обмане мање захтевно, осим у случајевима када се клијент придржава безбедносних мера при коришћењу интернета. Интернет преваре се врше у онлајн окружењу злоупотребом људске радозналости, наивности, неопрезности, исхитрености, поводљивости, грамзивости, жеље за лаком зарадом, недоследности, неуредности, усамљености, емотивне рањивости, психолошке нестабилности, несигурности, брзоплетости и потребе за личним значајем, како би се жртва приволела или приморала да своје и туђе осетљиве личне и професионалне податке учини доступним сајбер обмањивачу (Okereafor, Adebola et al. 2020).

Уобичајени случај реализовања интернет преваре је масовно дистрибуирање лажних или нежељених (spam) односно спамованих порука путем електронске поште, којом приликом нападач шаље обмањујуће садржаје унапред неодређеној жртви како би добио њене осетљиве податке, који се односе на акредитације за пријаву приступа на веб, лозинке и безбедносне кодове. Интернет преваранти редовно праве спамоване поруке са изразима и кључним речима које стварају осећај драматичности и страха, како би код жртве потакли базичне људске слабости и извршили обману.

Након појаве пандемије корона вируса, корисници интернета су почели интензивно да врше онлајн претраге које се односе на изворе вируса, број заражених, податке о угроженим земљама и режимима преласка државних граница, врстама и доступности лекова, мерама и поступцима за заштиту, па су сајбер криминалци почели да врше интернет преваре кроз информатички напредне облике фишинга креирајући нпр. лажне веб сајтове о наведеним темама. Потакнути страхом и знатижељом, корисници су како би приступили жељеним сајтовима, обманути њиховим лажним садржајем, своје осетљиве податке чинили доступним извршиоцима сајбер превара.

Фишинг напад је врста интернет преваре која подразумева употребу детаља који се односе на циљаног примаоца и који су вешто приказани у тексту поруке упућене електронском поштом, како би комуникација изгледала аутентично. Корак даље представља спир-фишинг (spear-phishing), који као врста интернет преваре укључује обраћање жртви на прецизан и званичан начин на њеном језику, уз тачно навођење његовог професионалног статуса и коришћење правила официјене

кореспонденције. Масовно упућене електронске поруке о корона вирусу ће, под плаштом пријатељског забринутог стила обавештавања, пружати наводну услугу о упознавању са најновијим информацијама које се односе на пандемију. Ове нежељене поруке врло често у себи имају изразе и кључне речи којима се потиче осећај хитности и узнемирености због „најновијих" информација које се тичу корона вируса (Aldawood–Skinner 2019).

УЧЕСТАЛОСТ ПОЈАВНИХ ОБЛИКА ИНТЕРНЕТ ПРЕВАРА

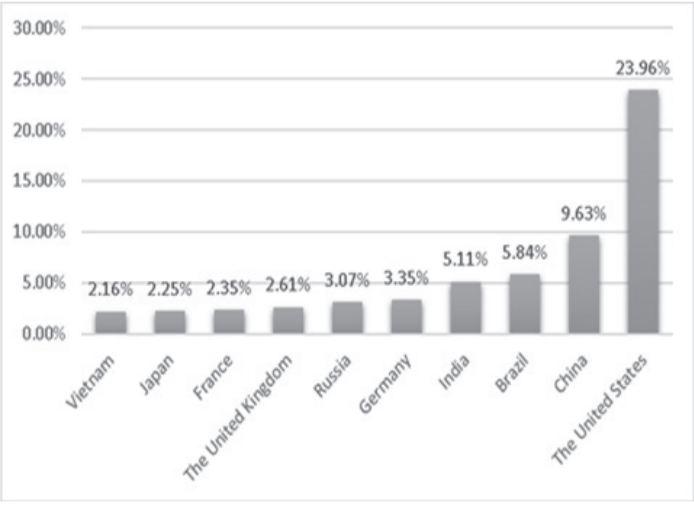
Сајбер криминал, а у оквиру њега и интернет преваре, представља један од највећих проблема за савременог човека, јер свако ко има електронску адресу, банковни рачун или било коју приватну и другу осетљиву информацију јесте потенцијална мета сајбер напада или онлајн обмане, а то има утицај на друштво чија се штетност мери великим бројевима. Преваре на вебу развијају своју успешност крупним корацима јер се у кратким временским роковима сајбер криминалци прилагођавају променама које се дешавају у свету, као што је непредвидиво велики миграциони талас људи избеглих из кризних жаришта афроазијског комплекса, али и напретку информатичких технологија попут појаве виртуелне реалности интернета ствари.

Већина корисника интернета не разуме или несвесно потцењује сајбер криминалну претњу и константну потенцијалну изложеност обманама на вебу због чега не размишља о потреби да заштити своје податке од онлајн превара. Просечан корисник интернета би требало да буде упознат са постојањем злонамерних апликација, лажних веб страница, спамованих порука које садрже вирусе, фишинга и спир-фишинга на вебу и значајем заштите својих података, а пре свега корисничког имена и лозинке.

У овом раду, управо зато, истакнута је неопходност планирања ради заштите од сајбер напада и штетних утицаја и последица превара на вебу. Ипак, добро планирање се не може извести без анализе постојећих околности и корелације датих чињеница. Определили смо се за приказ података који се односи на период од 2016. до 2020. године и налази се у вези са анализом учесталости интернет превара у таргетираним државама.

У току 2016. године сајбер криминал је био у сталном порасту због све већег броја корисника комуникације и других врста услуге на вебу. Успостављене су густе мреже разних врста интеракција, као што су пословне, купопродајне, забавне или интимне. Ово је било омогућено креирањем великог броја апликација и уређаја који су превазишли статичност корисничких рачунара у виду паметних телефона, лаптопова, таблета, нетбука односно ноутбука. Следствено томе, виртуелна област за извођење сајбер напада се проширила, добила динамику и постала мобилнија. Према извештају америчке компаније за сајбер безбедност Symantec, Сједињене Америчке Државе су 2016. године биле земља најизложенија фишинг нападима. У поређењу са 2015. годином, индекс опасности од интернет превара је са 18,89% порастао на 23,96% у 2016. години (Cook 2017).

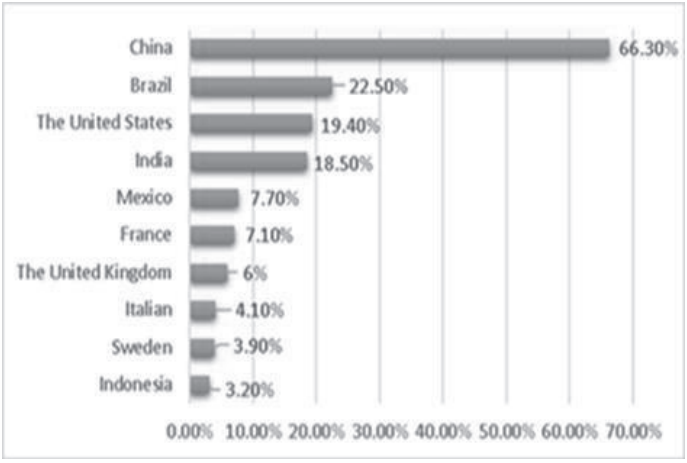
Разлог за ширење утицаја сајбер криминалне претње је у пласирања на веб малвера Mirai, чији изворни код је иницирао истовремене DdoS нападе широког обима на различите циљеве. Ови напади били су испрва усмерени на одређене информатичке уређаје које су компромитовали, да би потом њима биле изложене читаве рачунарске мреже јер су извођени у форми ботнета са међусобно повезаних небезбедних уређаја, од којих су злоупотребљени били чак и паметни монитори за чување беба (Crane 2020).



Графикон број 1: Десет земаља у којима су интернет преваре биле најчешће у 2016.

Малвер Mirai је злоупотребио информатичко окружење интернета ствари, у коме су корисничка имена и лозинике клијената предефинисани и чврсто везани за производну линију, што је омогућило сајбер нападачима да створе ботнет. Овај ботнет је чак пласиран против инфраструктурне веб компаније Dyn, која се бави безбедношћу апликација на вебу и обезбеђује администрирање унапређивања интернет локација ради заштите улазака корисника на мобилне друштвене мреже путем веб апликација, као што је нпр. Twitter (The Council of Economic Advisers 2018). Ова веб компанија је описала ботнет Mirai као један од примарних извора изузетно јаких сајбер напада, који су зауставили употребу веба на неко време 2016. године (Krebs on Security 2016).

У 2017. години забележен је неочекивано велики напад на веб позиције корисника и компанија. Интензитет и број интернет превара умножио се на до тада незапамћеном нивоу. Ово је био тежак период за одређивање стратегије безбедности у онлајн окружењу (Symantec 2018). Широки замах сајбер напада злоупотребом информатичке технологије интернета ствари остварио је раст од 600% што указује на активну употребу ботнета (Zawya 2020). На графикону број 2 приказано је десет држава које су биле најтеже погођене интернет преварама, са штетом која је достигла 22,5 милијарди долара. У просеку, 2017. године, свака жртва сајбер преваре изгубила је 142 долара.



Графикон број 2: Десет земаља које су биле погођене интернет преварама у 2017.

Само у периоду од априла до септембра 2017. године, стотине хиљада комуникација било је предмет обмане у Кини, а последица тога била је штета у висини од преко 100.000.000 јуана и више десетина хиљада жртава интернет превара (Morgan 2017).

Исте године у Сједињеним Америчким Државама извршено је хаковање на претраживачу Yahoo. То је утицало на 3 милијарде корисничких налога. Истовремено, хаковање америчке мултинационалне агенција за извештавање о потрошачким кредитима Equifax оштетило је 143.000.000 њених клијената, што је био највећи отворени сајбер напад до тада (Morgan 2017). Интернет преваре најчешће су биле вршене путем сајбер напада у виду ширења различитих врста малвера. У том смислу, 2017. године, активни су били следећи информатичких вируси: WannaCry, NotPetya и KRACK (Marshall 2017).

WannaCry је рансомвер (ransomware) односно криптовирус који напада оперативне системе Microsoft Windows. Овај вирус заразио је око 200.000 корисничких рачунара у 150 држава у свету. Била је нападнута старија верзија Windows оперативних система путем злоупотребе њеног мода осетљивости EternalBlue exploit. Преко ове рупе у систему заштите старије верзије Windows оперативних система криптовирус је заразио корисничке рачунаре, да би се потом дуплирао и непрестано се уможавајући брзо и невидљиво ширио путем рачунарских мрежа и система (Marshall 2017).

Нажалост, WannaCry је оштетио капиталне пословне захвате и многе базичне институционалне информатичке оквире у великом броју држава. Тешко су биле погођене велике националне телекомуникационе компаније као што су шпанска Telefonica и руски MegaFon. Нападнут је производни погон аутомобилске компаније Nissan у Великој Британији, као и француска аутомобилска кућа Renault. Криптовирус је заразио информатичке системе Руских железница, немачког железничког оператера Deutsche Bahn, руску Сбербанку, кинеску Bank of China, ланац сингапурских тржних центара, рачунарске системе центара за дистрибуцију брзе

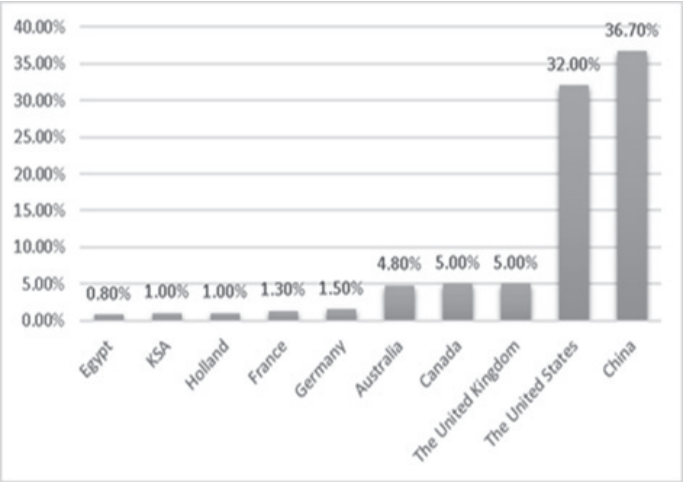
поште FedEx и шведску информатичку фирму Sandvik. Неке од компанија су успеле да успешно одбију овај сајбер напад, али су многе државне институције закасниле у заштити старије верзије радног оперативног система Windows које су користиле у свакодневном вођењу административних послова и комуникације. На овај начин, су из наведених разлога, били су заражени здравствени центри у Великој Британији, руско министарство унутрашњих послова, неки делови индијске националне полицијске службе, велики број рачунара у полицијским станицама широм Кине, бројни бирои имиграционих служби у свету, бразилско министарство спољних послова, системи социјалног осигурања и правосуђа, те Централна банка Русије, а све због коришћења незаштићене старе верзије Windows оперативног система. Процена глобалне штете коју је нанео WannaCry износи преко 4 милијарде долара (Fullbright 2017).

Нешто касније уследио је напад рансомвером NotPetya, који се појавио истовремено у Украјини, Француској, Немачкој, Италији, Пољској, Великој Британији, Русији и Сједињеним Америчким Државама. Овај вирус је преплавио веб странице банака, министарстава, електродистрибутера и медијских кућа. Само у Украјини заражени су рачунарски системи 80 компанија и организација, укључујући и Народну банку Украјине. Мултинационалне компаније Both FedEx и Maersk оштећене су за по 300.000.000 долара овим сајбер нападом (Prescatore 2020).

Крајем 2017. године истраживачи сајбер безбедносних система су на белгијској високошколској установи у граду Leuven пронашли критичну слабу тачку у свим стандардним WiFi уређајима. Ова слаба тачка, у ствари, представља безбедносни процеп у оквиру WiFi протокола и омогућава сајбер нападачу да прочита кодиране податке који се налазе на WiFi уређајима, како би остварио пробој у информатичку мрежу. Тачка пробоја назива се KRACK, што је скраћеница од израза кључни напади поновне инсталације (Key Reinstallation Attacks), јер се ова врста сајбер напада стално и изнова понавља преко тачке пробоја (Marshall 2017).

Током 2018. године у свету је било више од 300 случајева упада у заштићене системе у којима се налазе похрањени осетљиви подаци. Посебно су били погођени рачунарски системи здравствених служби и медицинских установа. Уочено је да су регистри са подацима пацијената лака мета за сајбер нападаче јер је у односу на здравствено питање сајбер заштита потпуно у другом плану, из истог разлога из кога је терапија пацијената примарна у поређењу са заштитом њихових података у информатичком систему здравствене организације (Prescatore 2020). Наравно, овакав однос према сајбер безбедности допринео је да електронска комуникација буде изложена фишингу за 250% више него претходне 2017. године. Начини вршења ових врста интернет превара су еволуирали, обзиром да су сајбер криминалци били принуђени да избегну све активне информатичке алате и технологије за сузбијање фишинга (Truta 2019).

Глобално посматрано, Кина је била 2018. године држава која је била најизложенија интернет преварама, како је приказано на графикону број 3, привлачећи чак 36% од укупног броја сајбер напада у свету, док су за њом следиле Сједињене Америчке Државе са 32% изложености овим криминалним активностима на вебу (Hao 2019).



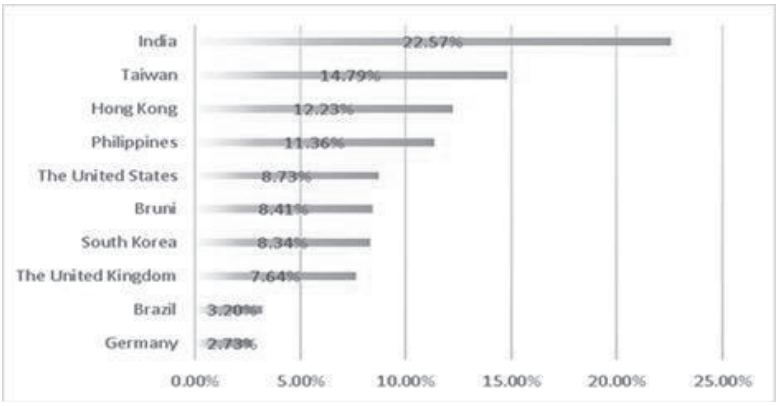
Графикон број 3: Раст глобалне дистрибуције нападнутих интернет адреса у 2018.

Надлежни органи Саудијске Арабије објавили су да је преко 160.000 сајбер напада у виду интернет превара било присутно на серверима њене телекомуникационе инфраструктуре на дневном нивоу. Уочена је нова верзија малвера на вебу под називом Shamoon 2, која је највише била усмерена на системе Саудијске Арабије у поређењу са осталим државама југозападне Азије и Блиског Истока (Oxford Business Group 2020). Овај малвер довео је до уништења података на више десетина хиљада корисничких рачунара. Shamoon 2 је дизајниран да избрише и замени податке са хард диска оштећеним фајловима са сликама, да би потом пријавио адресе заражених рачунара повратно на рачунар који се налази унутар мреже нападнуте компаније. Наведени малвер је имао логичку бомбу која је покретала покретање брисања већ похрањених података и њихову замену оштећеним фајловима са сликама (Aleyani, Kumar 2018).

У 2019. години забележен је највећи сајбер напад рансомвером на здравствени и јавни сектор. Реч је о DdoS нападу који је у првих шест месеци 2019. године достигао број од 580.000.000 пакета од по 1.500 бајтова у секунди. Према Кини је у овом периоду било усмерено 63,8% ових напада, а према Сједињеним Америчким Државама 17,5%. Ове две државе су на светском плану биле најугроженије DdoS нападима и преварама на вебу (Crane 2020).

Током 2019. године остварен је велики број сајбер напада на рачунарске мреже компанија у источној Азији. Од држава на том подручју, Индија предњачи по броју сајбер напада и онлајн превара, што је приказано на графикону број 4. Иначе, тада је регион источне Азије био мета за 77,7% свих DdoS напада на рачунарске мреже у свету (Avital–Zawoznik и др. 2019). У истом периоду сајбер криминалне активности биле су усмерене ка медијским подацима и осигуравајућим компанијама. Најчешће пласирани малвер био је Mirai и његова ботнет верзија, којима су сајбер криминалци таргетирали системе интернет ствари у бројним компанијама (Crane 2020). Саудијска Арабија предузела је мере заштите благовремено и успела да одбрани своје системе од Mirai малвера и пратећих превара на интернету (Rashad 2020).

У 2019. години технологија интернета ствари отворила је могућности за ботнет моделе сајбер напада, који су по обиму превазилазили оне их претходних периода. Оваквом стању је посебно допринела чињеница да су произвођачи паметних уређаја, који су функционално намењени за интернет ствари, наставили масовно да испоручују своје производе на уштрб њихове информатичке заштићености.



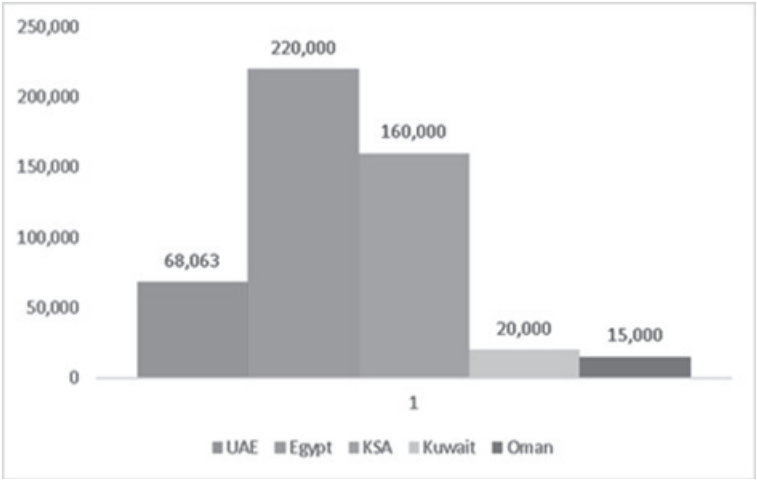
Графикон број 4: Првих десет земаља према броју мрежних напада у 2019.

Крајем 2019. године установљена је веза између уређаја из интернета ствари и DdoS напада, чије карактеристике су имале сасвим нове обрасце. Ово се, пре свега, односи на слабост WD заштитног протокола и употребу аутономних система бројева, који би требало да прате сајбер нападе до њихових извора. У току је истраживање утицаја увођења 5 G мреже на успешност DdoS напада (A10 Networks 2019).

Прошле 2020. године, интернет преваре су добиле на снази и замаху. Сајбер обманљивачи су максимално користили околности живота и рада у пандемијским условима и злоупотребљавали податке о корона вирусу како би подстицали кориснике интернета да своје податке учине доступним и незаштићеним. После приступања тућим подацима, сајбер криминалци су их користили за покретање других онлајн напада. Дакле, у овом случају су интернет преваре биле логистичка подршка за друге облике сајбер криминала, док су ранијих година оне углавном биле део пропратног ефекта других врста криминалних активности на вебу. Током 2020. године људски недостаци су били покретачки фактори у већем степену од системских недостатака и безбедносних процепа у сајбер зашити корисничких рачунара и мрежа, обзиром да је сада вирус био усмерен на здравље људи, а не на функционисање оперативних информатичких система, мрежну машинску комуникацију и оптималност рада рачунара (Okereafor, Adebola et al. 2020).

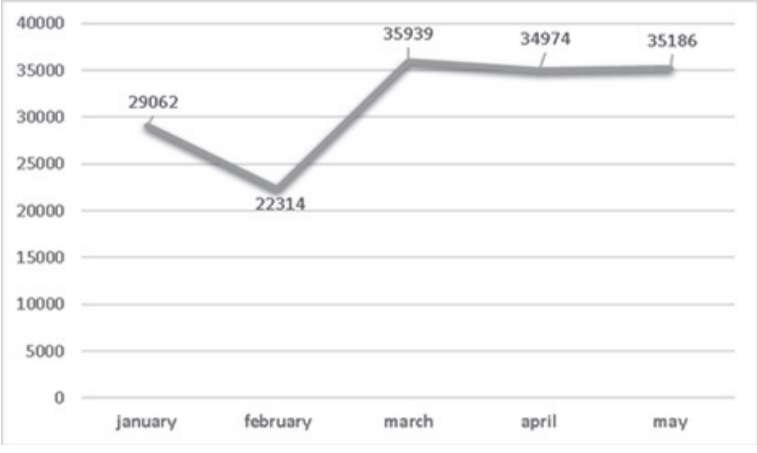
Интернет преваре највише су биле заступљене на веб страницама здравствених установа у вези са медицинским садржајима, саобраћајних организација, онлајн игара и оних образовног профила. Од успешних сајбер напада издвајају се DdoS напад на веб страницу грчке Владе и управе за ванредне ситуације, глобално ширење обмане путем електронске поште, DdoS напад на инфраструктуру здравствених установа у Паризу, Ddos напад на услуге доставе хране у Немачкој и Холандији, као и сајбер напад на Mebis платформу за учење на даљину у Немачкој (Kupreev, Badovskaya et al. 2020).

На графикону број 5 приказани су интернет преваре извршене над корисницима мобилних телефонских уређаја, током 2020. године, којом приликом је број сајбер напада највише био заступљен у Египту – 220.000 и Саудијској Арабији – 160.000, следе Уједињени Арапски Емирати са 68.063 напада, Кувајт са 20.000 и Оман са 15.000 (Zawya 2020).



Графикон број 5: Сајбер напади на кориснике мобилних телефона у арапским земљама у првој половини 2020.

Само у Саудијској Арабији, у датом периоду, извршено је 157.475 напада малверима на штету корисника паметних телефонских уређаја, што указује да изолација због пандемије није смањила ризик од превара на интернету већ да га је, напротив, повећала на 35.000 напада у месечном просеку (Saudi Gazette 2020).



Графикон 6: Интернет преваре на паметним телефонима у Саудијској Арабији у 2020.

Комерцијална експанзија и технолошки развој паметних телефонских уређаја су рапидни и очигледни, тако да сајбер нападачи више пажње обраћају на сам трансфер малвера и правце напада, повећавајући своју мобилност у пандемијским условима живота.

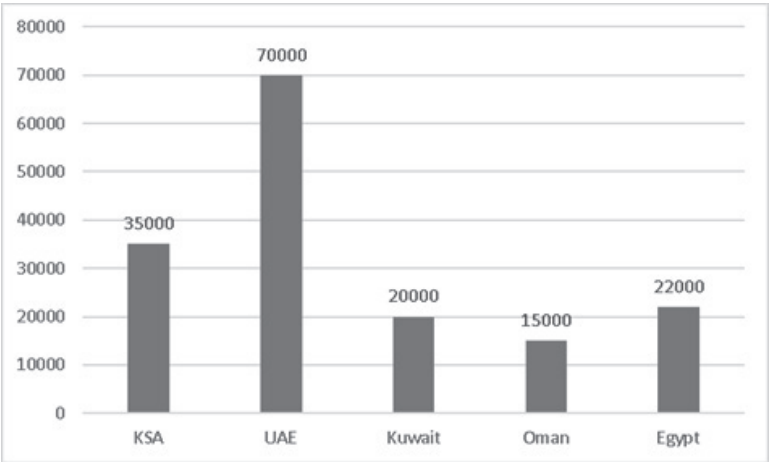


График број 7: Интернет преваре на паметним телефонима у земљама Блиског истока 2020

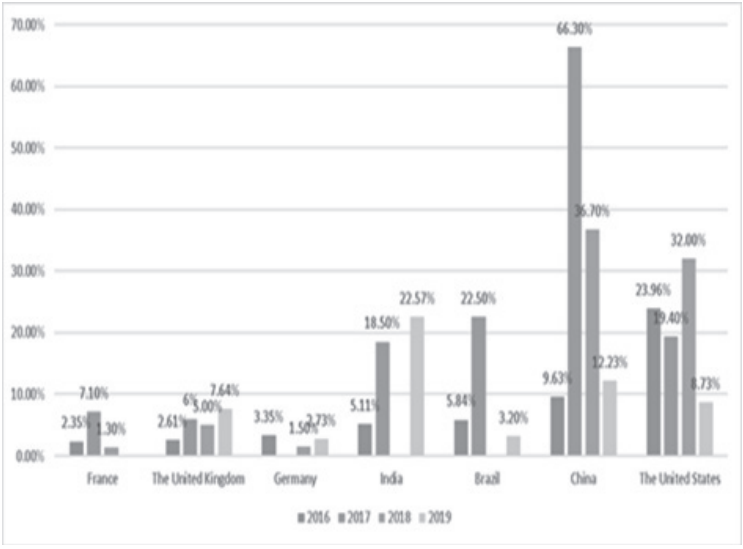
БЕЗБЕДНОСНИ ИЗАЗОВИ ОНЛАЈН ОКРУЖЕЊА

Интернет је постао везивно ткиво свих важнијих ствари у животу. Лепеза могућности његове употребе обухвата све секторе друштвеног живота укључујући тако разне области приватне и јавне сфере од државних транскација до онлајн образовног процеса и електронског пословања. У време пандемије чак 80% преноса финансијских и других средстава врши се путем интернета. Сајбер криминалци су у оваквим околностима, које им отварају могућности брзе и лаке зараде, константно присутни на вебу развијајући и унапређујући начине извршења својих илегалних активности. Ово подразумева разноврсне модусе пласирања малвера (злонамерних и штетних програма – malware) на веб, уз интензивирање интернет превара. Обзиром на све лукавије и вештије начине за обмањивање корисника интернета да учине доступним своје осетљиве податке, наметнула се потреба за заштитом информација у онлајн окружењу, која се пре свега односи на уочавање пропуста у информатичким системима кроз које сајбер нападачи врше неовлашћен приступ читавим базама података.

Најбитније је пратити начине извршења криминалних поступања на вебу, који су били фреквентни у претходном периоду релевантном за креирање и развој ефективне и ефикасне инфраструктуре сајбер безбедности. За наведени период опредили смо, у овом раду, петогодишњу временску секвенцу од 2016. до 2020. године, у којој је усмерена пажња на врсте интернет превара, њихову заступљеност и грешке сајбер нападача, које се недвосмислено морају узети у обзир.

Кретање у онлајн окружењу захтева опрез у односу на комуникацију путем електронске поште, а нарочито у вези са запримањем насумичних порука или нежељених порука са занимљивом или непознатом електронском адресом односно интригирајућим садржајем. На први поглед добронамерна комуникација, заправо је простор за вршење интернет преваре, тако да свака неочивана електронска активност усмерена на интернет корисника у себи носи ризик по његову приватну и пословну сајбер безбедност. Управо зато је веома важно обратити пажњу на извор информација и поуздане веб сајтове односно избегавати сумњиве интернет адресе и спамовану кореспонденцију у онлајн окружењу.

Преваре на интернету не би било могуће чинити без ослањања сајбер криминалаца на људске слабости због чега су напредни облици фишинга загосподарили вебом у време ширења корона вируса почетком 2020. године. Нуђење лажних података, злоупотреба онлајн пословања и социјална изолованост допринели су расту сајбер напада и олакшали могућност обмањивања корисника веба. Страх и узнемиреност обрнуто су пропорционални отварању могућности за приступ приватним подацима у онлајн окружењу. Све чешће ти подаци, до којих се прво долази преваром, само су пут до других података, који су примарни циљ сајбер преваре и других врста напада на интернету. Да би уопште могле да се планирају мера заштите, суштински је неопходно да корисници интернета опрезно приступају комерцијалним веб локацијама пре него што изврше уплате или било које друге електронске трансакције.



Графикон број 8: Стопа раста сајбер криминала
у одређеним земљама у периоду од 2016. до 2019.

Корисници морају бити сигурни да штите своје информатичке уређаје употребом и периодичним ажурирањем оригиналних антивирусних софтвера и програма за заштиту од малвера. Данашњи обим сајбер криминала укључује огроман број вируса и малвера. Постоје бројне различите врсте онлајн претњи које могу заразити

рачунаре и друге информатичке уређаје и омогућити интернет преварантима приступ осетљивим подацима корисника веба. Антивирусни програми, као што су нпр. Norton и Kaspersky, креирани су у сврху детекције параметара који указују на присуство сајбер криминалне претње због чега представљају својеврстан штит за корисничке рачунаре, разне паметне уређаје активне у онлајн окружењу, али и информатичке системе у целини. Не смемо изгубити из вида чињеницу да сајбер криминалну претњу, која се реализује нападима на вебу, у ствари чини укупност вируса и малвера активних у реалном времену.

Концепт функционалне и поуздане сајбер безбедности, као један од својих кључних чинилаца подразумева непрестану иновацију рачунарских софтвера, посебно у погледу заштитних антивирус програма. Ово унапређивање заштите на вебу у себи садржи више одбрамбених нивоа, како би се правовремено извршило откривање, блокирање и неутралисање свих потенцијалних програмских извора штетних последица по појединачне и мрежне рачунарске системе. Битна одлика антивирусног софтвера је да сталним проверавама прави разлику између добрих и лоших програмских садржаја који комуницирају са корисничким уређајима, тако да издваја податке о малверу и вирусима који улазе у рачунар, таблет или паметни телефонски уређај.

Због сталних безбедносних изазова на интернету корисници веб услуга морају бити опрезни са преузимањем датотека, нарочито ако су обимне. Сама активност у онлајн окружењу значи потенцијално излагање осетљивих података корисника који остварује комуникацију на вебу. Управо зато овај опрез мора бити још већи када је реч о технологији интернета ствари. У току 2016. године, управо у овој линији онлајн активности, злоупотребљена су подразумевана и предефинисана корисничка имена и лозинке како би био заражен велики број корисничких уређаја преко којих је у информатичкој форми ботнета (robot network – botnet) усмераван сајбер напад, широког опсега, ради остваривања DdoS активности, неовлашћеног приступа осетљивим подацима, слање спамоване електронске поште и интернет превара путем фишинга и спир-фишинга (Okereafor, Adebola et al. 2020).

У циљу спречавања губитка података, препоручљиво је прављење резервне копије на корисничком рачунару или на самом вебу. Потребно је периодично обновити резервне копије информација, како би се спречила могућност њиховог великог одлива у случају великог напада на информатички систем.

Статистичка анализа, у овом раду, указује на тенденцију раста појавних облика интернет превара, која прати повећање броја корисника веб услуга. На годишњем нивоу, посматрано у периоду од 2016. до 2020. године, број сајбер напада недвосмислено је у порасту, као и број напредних верзија превара на интернету. Није могуће одредити карактеристичне облике сајбер криминалних активности јер се оне непрекидно мењају и развијају, тако да их можемо разликовати само према основним елементима, који никако не чине њихове потпуне појавне облике. Такође, није изводљиво ни утврђивање у којој мери су конкретни кориснички рачунари били укључени у трансфер или само извршење интернет преваре, а у којој мери су били део примарне мете. Број активних сајбер нападача односно извршилаца интернет превара није мерљива категорија због услова онлјан окружења у којем делују. Ипак, може се закључити да је у периоду од 2016. до 2020. године до раста интернет превара дошло у сајбер

нападима на кориснике веба у Кини и Сједињеним Америчким Државама, те да се током 2017. године ова врста онлајн криминалних активности реализовала на глобалном плану подразумевајући већи број истовремено таргетираних држава у свету.

ЗАКЉУЧАК

Размере последица злоупотребе интернета су несагледиве. Сајбер криминал достигао је статус најистакнутијег ризика за сваку компанију у свету и представља један од највећих проблема за живот и рад савременог човека (Aldawood, Skinner 2019). Утицај на друштво који остварује сајбер криминална претња на годишњем нивоу, најбоље се види у висини штете коју су криминалне активности на интернету изазвале фирмама и појединцима, а која је 2015. године износила 3 трилиона долара, да би сваке наредне године до 2021. године износила по 6 трилиона долара. Ово је својеврсна потврда постојања најважније размене новчаних средстрава у савременој историји, која истовремено глобално угрожава покретачки дух и спремност на подухвате као основне чиниоце цивилизацијског напретка.

Поред наведеног, важно је истаћи да са позиције глобалних друштвено-економских токова илегалне активности на итернету доводе на макро плану до регресије и уништавања светског фонда знања, ометања технолошког прогреса, губљења продуктивних капацитета и преусмеравања енормних финансијских износа, док на микро плану узрокују крађу личних ствари и индивидуалних прихода. Такође, неизоставна је веза између сајбер криминала и вршења проневере, преваре, нарушавања традиционалних токова пословања, форензичких истрага, обнављања и брисања хакованих података и нападнутих система, као и штета по репутацију оштећених физичких и правних лица (Morgan 2017).

Сајбер криминал наноси изузетну штету и приватним и јавним подухватима и повећава буџете влада због успостављања мера за заштиту податке и система за спровођење сајбер безбедности, како у државним институцијама тако и приватним малим и средњим предузећима. Предвиђа се да ће улагања широм света у инфраструктуру и пратећу администартвину компоненту система сајбер безбедности премашити билион долара у периоду од 2017. до 2021. године. Годишњи раст развоја тржишта сајбер безбедности износи 12% до 15% у односу на сваку претходну годину посматраном периоду до 2021. Очекује се да ће се због сајбер криминалне претње, до 2021. године, утростручити број отворених радних места, за око три милиона позиција, у националним, регионалним и глобалним структурама сајбер безбедности. Овај број 2014. године није премашивао један милион радних места. Истовремено, стопа незапослености у области борбе против криминалних активности у онлајн окружењу остаће и даље на нула процената (Cybersecurity Ventures 2018).

Овај рад препоручује да је свест о сајбер безбедности и безбедности информација веома важна када се користи веб. Анализирајући нападе од 2016. до почетка 2020. године, утврђено је да су напади изведени кроз пропусте и празнине у информатичким системима које су се могле решити да је било више обзира и знања о тим недостацима у заштити података.

Неопходно је бити опрезан при коришћењу осетљивих информација. Морају се обезбедити подаци од електронских напада и идентификовати безбедносни процепи кроз које нападачи пролазе да би дошли до поверљивих и осетљивих података. Неопходно је бити свестан начина деловања и могућности које користе сајбер криминалци током својих напада у онлајн окружењу. Јасно је утврђено да су интернет преваре биле један од најчешћих облика испољавања сајбер криминалне претње током 2020. године.

Мора постојати више свести о томе како се безбедно врше претраге садржаја на интернету, како се на сигуран начин преузимају информатички програми и како се адекватно употребљавају паметни уређаји у светлу примене технологије интернета ствари, јер је у анализираном периоду од последњих пет година установљено да је та информатичка технологија најважнији замајац за ширење сајбер криминалне претње и напада у онлајн окружењу глобалне мреже интернета.

ЛИТЕРАТУРА

Avital, Zawoznik et al. 2019: Nadav Avital, Avishaj Zawoznik et al. *2019 Global DDoS Threat Landscape Report*. <https://www.imperva.com/blog/2019-global-ddosthreat-landscape-report/>. [19.12.2021]

Aldawood, Skinner 2019: Hussain Aldawood, Geoffrey Skinner. "Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal". *International Journal of Security*, Vol. 10, Issue 1, 1-15.

Aleyani, Kumar 2018: Salem Alelyani, Harish Kumar G.R. "Overview of Cyberattack on Saudi Organizations". *Journal of Information Security and Cybercrimes Research*, Vol. 1, No. 1, 32–39.

A10 Networks 2019: *Report The State of DDoS Weapons*. <http://presse.hbi.de/pub/A10_ Networks/5G_Pressetou r/A10_Networks- he_State_of_DDoS_Weapons.pdf>. [20.12.2021]

Gravrock 2019: Einaras von Gravrock. *Here are the biggest cybercrime trends of 2019*. <https://www.weforum.org/agenda/2019/03/here-are-thebiggest-cybercrime-trends-of-2019/>. [11.12.2021].

Zawya 2020: *UAE saw almost 70,000 cyberattacks on smartphones in 2020*. <https://www.zawya.com/mena/en/pressreleases/story/UAE_saw_almost_70000_cyberattacks_on _smartphones_in_2020-ZAWYA20200614092408/>. [21.12.2021]

Kabay 2008: Michel E. Kabay. *A Brief History of Computer Crime: An Introduction*. Northfield: Norwich University.

Krebs on Security 2016: *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*. <https://krebsonsecurity.com/2016/10/hacked-camerasdvrs-powered-todays-massive-internetoutage/#:~:text=A%20massive%20and%20sustained%20Internet,video%20recorders%2C%20n ew%20data%20 suggests>. [16.12.2021]

Kupreev, Badovskaya et al. 2020: Oleg Kupreev, Ekaterina Badovskaya et al. *DDoS attacks in Q1 2020 – 10 minute mail (may,2020)*. <https://disposableemail.org/index.php/tag/ddosattacks/>. [21.12.2021].

Marshall 2017: Emmanuel Marshall. *Cybercrime 2017: This Year's Big Stories*. <https://www.mailguard.com.au/blog/cybercrime-2017- headlines>. [18.12.2021]

Morgan 2017: Steve Morgan. *Cybercrime Report*. <https://cybersecurityventures.com/2015- wp/wp- content/uploads/2017/10/2017-CybercrimeReport.pdf>. [14.12.2021]

Nfuka, Sanga et al. 2014: Edephonce Ngemera Nfuka–Camilius Sanga et al. "The Rapid Growth of Cybercrimes Affecting Information Systems: Is this a Myth or Reality in Tanzania". *International Journal of Information Security Science*, Vol. 3, No. 2, 182–199.

Okereafor, Adebola et al. 2020: Kenneth Okereafor– Olajide Adebola et al. "Tackling the Cybersecurity Impacts of the Coronavirus Outbreak as a Challenge to Internet Safety Article". *International Journal in IT* & *Engineering*, Vol. 8, Issue 2, 1–11.

Oxford Business Group 2020: *Saudi Arabia works to enhance cybersecurity*. <https://oxfordbusinessgroup.com/analysis/secure-access-authorities-work-enhancecybersecurity-and- resilience-face-evolving-onlinethreats>. [18.12.2021]

Prescatore 2020: John Pescatore. *Infoblox*. <https://www.infoblox.com>. [15.12.2021]

Rashad 2020: Marwa Rashad. *Saudi Aramco sees increase in attempted cyber attacks*. <https://www.reuters.com/article/saudi-aramco-security-idUSL8N2A6703>. [21.12.2021]

Saudi Gazette 2020: *Saudi Arabia saw almost 160,000 cyberattacks on smartphones*. <https://saudigazette.com.sa/article/594321/BUSINESS/S audi-Arabia-saw-almost-160000- cyberattacks-onsmartphones>. [20.12.2021]

Symantec 2018: *Internet Security Threat Report*. <https://docs.broadcom.com/doc/istr23-2018-executive-s ummary-en-aa>. [17.12.2021]

Tabrez 2020: Ahmad Tabrez. "Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity". *Social Science Research Network*, 1–5.

Truta 2019: Filip Truta. *Microsoft: Phishing Attacks Increased 250% from January to December 2018*. <https://securityboulevard.com>. [15.12.2021]

The Council of Economic Advisers 2018: *The Cost of Malicious Cyber Activity to the U.S. Economy*. <https://www.whitehouse.gov/wpcontent/uploads/2018/03/The-Cost-of-Malicious-CyberActivity-to- the-U.S.-Economy.pdf>. [13.12.2021]

Fullbright 2017: Norton Rose Fulbright. *WannaCry Ransomware Attack Summary*. <https://www.dataprotectionreport.com/2017/05/wannacr y-ransomware-attack-summary/>. [20.12.2021]

Hao 2019: Mina Hao. *2018 DDOS Attack Landscape-8*. <https://nsfocusglobal.com/2018-ddos-attacklandscape- 8/>. [16.12.2021]

Cook 2017: James Cook. *The world's 10 biggest cybercrime hotspots in 2016, ranked*. <https://amp.insider.com/worlds-10-cybercrime-hotspotsin-2016-ranked-symantec-2017-5>. [19.12.2021]

Crane 2020: Casey Crane. *The 15 Top DDoS Statistics You Should Know In 2020*. <https://cybersecurityventures.com/the-15-top-ddosstatistics-you-should-know-in-2020/,Sybercrime magazine>. [20.12.2021]

Cybersecurity Ventures 2018: *Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021*. <https://www.prnewswire.com/newsreleases/cyberattacks-are-the-fastest- growing-crimeand-predicted-to-cost-the-world-6-trillion-annually-by2021-300765090.html>. [18.12.2021]

White 2013: Kelly White. *The Rise of Cybercrime 1970 through 2010*. <https://drive.google.com/file/d/0B_GoF8uQ95lGWU1R MXZ0WmV2YnM/edit>. [12/12/2021]

Đorđe M. MILOŠEVIĆ

FREQUENT OCCURRING FORMS OF INTERNET FRAUDS

Summary

The increase in the volume of electronic transactions has led to the need to strengthen data protection against criminal activities in the online environment. The author emphasizes that the perpetrators' goal is of a lucrative nature, might be gotten by disrupting the information system too, as well as offenders can be both individuals and legal persons. The profile of a cybercrime criminal, in general, implies excellent knowledge of digital proceedings, experience of acting in the online environment

and active performing of information technology skills. The Internet has become an integral part of today's way of life, which is why the scope of criminal activities in this worldwide network for communication and data exchange is constantly expanding. The author deems this as the reason for the growing need to strengthen information security, which he determines as the practical implementing of measures to protect data from external influences in the online environment. This paper presents a statistical analysis of the Internet frauds' frequency from 2016 to 2020, in order to show the real intensity of this modern kind of criminal threat.

Key words: Internet, Internet frauds, online environment, cybercrime, information system, information security, cybercrime threat.

Рад је предат 22. децембра 2021. године, а након мишљења рецензената, одлуком одговорног уредника *Баштине*, одобрен за штампу.