

ПОЛИЦИЈА И ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

– Примери из праксе и проблеми у раду МУП-а Републике Србије –

Др Владимир УРОШЕВИЋ¹, Мр Сергеј УЉАНОВ², Радоје ВУКОВИЋ³
Министарство унутрашњих послова Републике Србије

Апстракт: Развој информационих технологија утицао је на повећање броја појавних облика кривичних дела из области високотехнолошког криминалитета. Пораст броја кривичних дела из ове области посебно се односи на оне облике извршења кривичних дела са елементима прекограничног, организованог и транснационалног криминала. У многим државама широм света, које имају развијену информациону структуру која је по својој природи изузетно рањива на овакве видове напада, високотехнолошки криминал је означен као један од најштетнијих. Пред полицијске службе постављен је тежак задатак да претње по безбедност информационих структура и њихових корисника сведу на минимум. Министарство унутрашњих послова Републике Србије данас се све више суочава са различитим појавним облицима кривичних дела из области високотехнолошког криминала. У овом раду приказана су искуства везана за борбу против високотехнолошког криминала се којима се Министарство унутрашњих послова Републике Србије сусретало, као и проблеми са којима се оно суочава у свакодневном раду.

Кључне речи: Министарство унутрашњих послова Републике Србије, високотехнолошки криминал, злоупотреба информационих технологија, злоупотребе података

Abstract: Development of information technologies influenced on apperance of different forms of crimes in the area of high-tech crime. Increase of crimes in this area particularly applies to those forms of conducting of criminal acts with elements of cross-border, transnational and organized crime. In many countries around the world, that have developed information structure that is by nature extremely vulnerable to these types of attacks, a high-tech crime is classified as one of the most harmful. Police Services around the world have a difficult task to reduce security threats to information structures and their users down to a minimum. Ministry of Interior of the Republic of Serbia today is facing different manifestations of crimes in the area of high-tech crime. This article presents the experience related to the fight against high-tech crime and problems that the Ministry of Interior of the Republic of Serbia met, in its work.

Key words: Ministry of interior of the Republic of Serbia, high-tech crime, misuse of information technology, misuse of data

¹ vladimir.urosevic@mup.gov.rs

² sputnik970@gmail.com

³ radoje.vukovic@mup.gov.rs

1. УВОД

Научна и стручна јавност у Републици Србији препознала је опасност која прети од високотехнолошког криминала савременом информационом друштву у Републици Србији. Конвенција о компјутерском криминалу потписана је 2006. године.⁴ Високотехнолошки криминал у нашој држави дефинисан је као скуп кривичних дела где се као објекат извршења и као средство за извршење кривичног дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном и електронском облику. Код нас се тако данас разликују кривична дела у којима се рачунари појављују као средство извршења (Computer Related Crime) и као објекат извршења (Computer Crime), као и кривична дела у чијем се начину извршења појављују елементи незаконитог коришћења Интернета.

У Републици Србији се борба против високотехнолошког криминала сматра једним од најважнијих задатака који је поверен Министарству унутрашњих послова. У овом Министарству од 2008. године у оквиру Службе за борбу против организованог криминала налази се Одељење за борбу против високотехнолошког криминала. У саставу овог одељења оформљени су Одсек за сузбијање криминалитета у области интелектуалне својине и Одсек за сузбијање електронског криминала.

На основу досадашњег рада овог Одељења уочено је да извршиоци кривичних дела из области високотехнолошког криминала из Републике Србије не заостају по начинима извршења ових кривичних дела за извршиоцима у иностранству. У многим случајевима примећено је да постоје и елементи организованог и прекограничног криминала.

У току 2008. и 2009. године поднето је више десетина кривичних пријава Посебном тужилаштву за борбу против високотехнолошког криминала Окружног јавног тужилаштва у Београду за кривична дела из ове области. За различите облике кривичних дела која су извршена уз помоћ рачунара, рачунарских система и рачунарских мрежа кривичне пријаве су надлежним тужилаштвима на територији Републике Србије подносиле и друге организационе јединице МУП-а Републике Србије, а Одељење за борбу против високотехнолошког криминала пружало и стручну помоћ при вршењу истрага везаних за илегалну трговину дрогом, недозвољену трговину, тероризам, убиства, илегалну трговину ретким и угроженим животињским и биљним врстама и др.

2. КРИВИЧНО-ПРАВНИ И ОРГАНИЗАЦИОНИ ОКВИРИ ЗА БОРБУ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ И МЕСТО И УЛОГА МУП-а РЕПУБЛИКЕ СРБИЈЕ

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала који је објављен у Службеном гласнику Републике Србије број 61/05 од 15.07.2005. године успостављени су законски оквири за

⁴ Ова конвенција донета је од стране Савета Европе дана 23.11.2001. године у Будимпешти, Мађарска а ратификована је у Републици Србији Законом о потврђивању Конвенције о високотехнолошком криминалу који је дана 18.03.2009. године објављен у Службеном гласнику Р.Србије бр.19-09.

успостављање институција за борбу против високотехнолошког криминала и у њихову надлежност поверено је спречавање кривичних дела против безбедности рачунарских података, као и кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.

Кривични законик Републике Србије који је ступио на снагу 1. јануара 2006. године у глави XXVII под називом „Кривична дела против безбедности рачунарских података“ прописује следећа кривична дела:

1. Оштећење рачунарских података и програма
2. Рачунарску саботажу
3. Прављење и уношење рачунарских вируса
4. Рачунарску превару
5. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података
6. Спречавање и организирање приступа јавној рачунарској мрежи и
7. Неовлашћено коришћење рачунара или рачунарске мреже.

У наведеним кривично-правним и институционалним оквирима у току 2008. године у Министарству унутрашњих послова Републике Србије у Служби за борбу против организованог криминала формирано је Одељење за борбу против високотехнолошког криминала. Ово Одељење састоји се од два одсека: одсек за сузбијање криминалитета у области интелектуалне својине и одсек за сузбијање електронског криминала. У току 2009. године ратификована је Конвенција о компјутерском криминалу као и Додатни протокол уз конвенцију о сузбијању компјутерског криминала који се односи на кажњавање аката расизма и ксенофобије учињених путем компјутерских система.⁵ Законом о изменама и допунама Кривичног законика од 31.08.2009. године објављеним у Службеном гласнику Републике Србије број 72-09 (измене се односе на Кривични законик Републике Србије који је ступио на снагу 1. јануара 2006. године, објављеног у Службеним гласницима Републике Србије број 85/2005, 88/2005, 107/2005) домаће кривично законодавство усклађено је са препорукама из Конвенције о компјутерском криминалу. Законом о изменама и допунама закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала који је објављен у Службеном гласнику Републике Србије број 104-09 дана 11.12.2009. године створени су и додатни услови за ефикаснију борбу против високотехнолошког криминала проширењем надлежности на друга кривична дела.

⁵ Додатни протокол уз Конвенцију о сузбијању компјутерског криминала који се односи на кажњавање аката расизма и ксенофобије учињених путем компјутерских система донет је у Стразбуру дана 28.01.2003. године, а ратификован је Законом о потврђивању додатног протокола уз конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система који је објављен у Службеном гласнику Републике Србије број 19-09 од 18.03.2009. године.

3. ПОЈАВНИ ОБЛИЦИ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У ПРАКСИ МИНИСТАРСТВА УНУТРАШЊИХ ПОСЛОВА РЕПУБЛИКЕ СРБИЈЕ

Одељење за борбу против високотехнолошког криминала у току 2008. и 2009. године поднело је више десетина кривичних пријава Посебном тужилаштву за борбу против високотехнолошког криминала Окружног јавног тужилаштва у Београду за кривична дела из области високотехнолошког криминала. Истовремено, за различите облике кривичних дела која су извршена уз помоћ рачунара, рачунарских система и рачунарских мрежа кривичне пријаве су надлежним тужилаштвима на територији Републике Србије подносиле и друге организационе јединице МУП-а Републике Србије.

Поред подношења већег броја кривичних пријава за кривичних дела која се гоне по службеној дужности полицијски службеници МУП-а Републике Србије учили су и велики број кривичних дела која се гоне по приватној тужби, а које су им пријављивали грађани. Нека од тих кривичних дела везана су за крађу идентитета на Интернету, крађу налога на социјалним мрежама. Интернет сервис *Facebook* сматра се једним од најпопуларнијих друштвених мрежа на Интернету.⁶ Због начина на који функционише, овај Интернет сервис постао је погодан „амбијент“ за крађу и злоупотребу идентитета. Крађа идентитета почиње са присвајањем личних података о неком лицу, без пристанка и знања тог лица, путем обмањивања, крађе или преваре. Прикупљене информације могу да буду искоришћене одмах након крађе, да се складиште и чувају ради коришћења или да се препродају другоме уз новчану надокнаду. Крађа идентитета наставља се употребом прикупљених података за извршење кривичних дела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која злоупотребљавају украдени идентитет.⁷

Одељење за борбу против високотехнолошког криминала такође је пружало и стручну помоћ при вршењу истрага везаних за илегалну трговину дрогом, недозвољену трговину, тероризам, убиства, илегалну трговину ретким и угроженим животињским и биљним врстама и др.

Заштита интелектуалне својине

Различите службе Министарства унутрашњих послова Републике Србије у области борбе против високотехнолошког криминала највећи број кривичних пријава поднеле су против извршилаца кривичних дела којима се нарушава право интелектуалне својине. Начин извршења ових кривичних дела је углавном илегална продаја неовлашћено наснимљених примерака ауторских дела на мултимедијалне носаче и њихова даља препродаја крајњим корисницима (улична продаја, продаја преко организоване мреже препродаваца широм територије Републике Србије и др). Као пример може се навести да су у току 2008. године поднете кривичне пријаве против 35

⁶ E. Athanasopoulos et. al: Antisocial Networks: Turning a Social Network into a Botnet, Section: Network Security, Lecture Notes In Computer Science, Berlin, Република Немачка, стр. 146-160.

⁷ Милошевић М., Урошевић В.: Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53-64.

лица, одузето 53 рачунара и 49.000 оптичких дискова.⁸ У једном броју случајева Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала поднело је кривичне пријаве против извршилаца кривичних дела који су оглашавали продају неовлашћено наснимљених примерака филмова, серија, музике и рачунарских програма путем Интернета, најчешће на Интернет сајтовима путем огласа, а затим те примерке, без знања и овлашћења носилаца ауторских права дистрибуирала широм Републике Србије.

Наручивање је најчешће вршено путем електронских порука или мобилним телефонима, а испорука је вршена лично од стране извршилаца кривичних дела или путем поштанских пошиљки. У овим случајевима заплењено је више стотина хиљада електронских мултимедијалних носача звука и слике (ЦД, ДВД итд), као и више стотина рачунарских уређаја и осталих средстава неоподних за извршење ових кривичних дела.

Поред наведеног начина извршења Одељење за борбу против високотехнолошког криминала открило је и друге начине извршења као што је дистрибуирање заштићених ауторских дела (филмови, серије, музика, рачунарски програми) путем P2P мрежа (*Peer to Peer*) и путем FTP (*File Transfer Protocol*) сервера. Ово одељење је у неколико случајева открило и неовлашћено дистрибуирање различитих примерака уџбеника и приручника у електронском облику путем Интернета, након чега су против извршилаца кривичних дела поднете кривичне пријаве Посебном тужилаштву за високотехнолошки криминал.

Фалсификовање и злоупотребе платних картица

Злоупотребе платних картица појавиле су се у Републици Србији још у 2005. години, и од тада је забележено више од хиљаду случајева. У око 80 одсто случајева извршиоци кривичних дела су били страни држављани, претежно Бугари и Румуни. Групе од по десетак људи за неколико дана подизале су до 150 ЕУР-а до 200.000 ЕУР-а. Ова кривична дела се најчешће врше на тај начин што се на банкомате банака постављају тзв. скимери, уређаји за читавање магнетног записа, као и лажне тастатуре које меморишу ПИН код картице. Они се скидају са банкомата, прикључују се на рачунар који читава запис, пребацује се на нову платну картицу, којом се касније подиже новац, обично у иностранству. Иако је проценат откривања ових кривичних дела код нас на завидном нивоу, дугорочно, овај вид криминала је у порасту јер расте и употреба платних картица. На граничним прелазима од стране припадника граничне полиције МУП-а Републике Србије су такође откривене веће количине платних картица тзв. „беле пластике“ или „златне пластике“ које су страни држављани (најчешће Бугари и Румуни) припремили ради вршења злоупотреба на територији Републике Србије

У све већем порасту је и прекогранични криминал у овој области. Појавиле су се и организоване криминалне групе са територије бивших југословенских република који све више међусобно „сарађују“ када је у питању злоупотреба и фалсификовање платних картица. Организоване криминалне групе са територије Републике Србије ангажују лица која поседују завидна информатичка знања како би за њихов рачун прибављала

⁸ Лидија Комлен Николић et.al: Сузбијање високотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, стр. 231.

податке о платним картицама путем Интернета, лица која им праве лажне платне картице, као и лица која за њихов рачун подижу новац са банкомата.

Поред ових начина извршења у порасту је и број кривичних дела чији је начин извршења познатији као „*card not present*“ у којима се преваре врше без физичког присуства платне картице. Оваква кривична дела најчешће се врше преко Интернета, а у току 2009. године примећен је и пораст оштећених лица са територије Републике Србије.

Рачунарске преваре

У току 2006. године Министарство унутрашњих послова открило је једну од првих рачунарских превара и поднело кривичну пријаву против 53 особе због постојања основане сумње да су, као чланови организоване криминалне групе приликом наплате путарина оштетили државу за 6,5 милиона ЕУР-а на тај начин што су на аутопуту Београд-Ниш у периоду од 01.07.2004. године до маја 2006. године посебно направљеним уређајима и рачунарским програмом организовали систем за наплату путарине без евидентирања возила којима је путарина наплаћена у систему ЈП „Путеви Србије“.

Данас на територији Републике Србије извршиоци рачунарских превара врло често користе фалсификоване платне картице како би путем Интернета прибавили робу коју накнадно могу да продају и на тај начин остваре противправну имовинску корист. Податке о платним картицама најчешће прибављају коришћењем *phishing* алата, слањем нежељених порука (нпр. *SPAM* порукама) и коришћењем *SQL* ињекција за прибављање података из база података електронских продавница у иностранству. Електронски подаци са платних картица добијени извршењем кривичних дела преко Интернета најчешће се користе за наручивање робе преко Интернет сајтова електронских продавница, најчешће на територији Републике Србије, али и у иностранству. Извршиоци кривичних дела су, на основу досадашњих искустава, углавном била малолетна лица или млађи пунолетници, док се као саизвршиоци јављају и старија пунолетна лица.

Електронске продавнице преко својих Интернет страница на нашој територији углавном за наручивање робе захтевају неке основне податке као што су број телефона, име, презиме и адреса лица које ће преузети робу, електронска адреса и слично. Приликом уноса наруџбине траже се број платне картице и CVV2 број, као и лични подаци власника.

Извршиоци кривичних дела углавном наручују скупочену робу (мобилне телефоне, лаптоп рачунаре, злато, аудио и видео технику и др.) коју након извршења кривичног дела могу лако и брзо да препродају. Приликом наручивања робе извршиоци утичу на процес обраде података на тај начин што уносе податке о платним картицама у поља за унос података на Интернет сајту електронске продавнице, и дају лажне личне податке (име, презиме, адресу) представљајући се као да су они власници платне картице, а за евентуалне договоре око преузимања робе остављају бројеве мобилних телефона намењене само за ту сврху. Како би остали анонимни, као контакт електронску адресу остављају електронске адресе отворене на Интернет сервисима који омогућавају *Web* базирану пошту, где је тешко добити податке о власницима, пошто се сервери налазе у иностранству (нпр. *Gmail*).

Пошто се испорука робе најчешће врши путем поште тј. теренском доставом, за примаоце робе углавном се бирају лица која су пунолетна и поседују личне карте. Ова лица, најчешће под лажним именом и презименом, на отвореном простору, робу преузимају директно од доносиоца, након телефонског позива од стране достављача, како би избегли да буду откривени и ухваћени од стране полиције, и како би се избегло откривање стварне адресе испоруке пошиљака. Лица која преузимају робу најчешће нису и лица која су робу наручивала преко Интернета, већ робу преузимају за рачун наручиоца уз одређени проценат од продаје робе која је на овакав начин прибављена.

У току 2008. и 2009. године на територији Републике Србије откривено је више случајева рачунарских превара и злоупотреба платних картица на Интернету, у оквиру којих су покушане и извршене злоупотребе података са више стотина платних картица, а прибављена имовинска корист износила је преко пет милиона динара. Идентификовано је седам лица која су се бавила овим кривичним делима и против њих су поднете кривичне пријаве Посебном тужилаштву за високотехнолошки криминал Окружног јавног тужилаштва у Београду. Злоупотребљаване су углавном платне картице страних банака издавалаца са територије Сједињених Америчких Држава, а за прибављање података коришћене су технике *SPAM*-а, *phishing*-а и *SQL* ињекција.⁹

Вршење високотехнолошког криминала у начелу не подразумева присуство извршиоца на месту где се налази жртва. Ова независност места деловања и локације жртве ствара потешкоће приликом истрага високотехнолошког криминала.¹⁰ Поред наведених облика рачунарских превара присутне су и друге врсте превара које се врше уз помоћ рачунара, као што су тзв. „Преваре 419“ или „Нигеријске преваре“. „Превара 419“, као израз за „Нигеријску превару“, добила је назив по члану број 419 Нигеријског кривичног закона (који је део поглавља 38) под називом „Прибављање имовине помоћу преварних радњи: Превара“ који дефинише ово кривично дело.¹¹ Радња извршења „Нигеријске преваре“ углавном почиње убеђивањем „жртве“ преваре да учествује у подели одређених новчаних фондова ако унапред уплати одређени новчани износ који је у највећем броју случајева неупоредиво мањи од оног износа који би требала да добије као корист од тог фонда.

У току 2008. и 2009. године на територији Републике Србије од стране оштећених лица пријављено је десет случајева са елементима „Нигеријских превара“ против непознатих учинилаца. Овим кривичним делима оштећени су држављани Републике Србије и предузећа са наше територије, а укупна имовинска штета износила је преко 60.000 ЕУР-а. Оштећена лица су новац извршиоцима кривичних дела слали преко сервиса *Western Union* и *MoneyGram*. Преваре су углавном вршене помоћу *SPAM* порука уз коришћење методе социјалног инжињеринга, а комуникација је, након одговора од стране оштећених на *SPAM* поруку углавном вршена преко бесплатних налога за електронску пошту која је отворана на Интернет сервисима *Yahoo*, *Hotmail* и др. Такође

⁹ В. Урошевић: Злоупотребе платних картица и рачунарске преваре, Правни информатор, Београд, 2009. година, стр. 4.

¹⁰ РАСО Serbia-Пројекат за борбу против економског криминала у Републици Србији: Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе, 2008. стр.38.

¹¹ М. Chawki: Anonymity in Cyberspace: Finding the Balance between Privacy and Security, Revista da Faculdade de Direito Milton Campos, Nova Lima, Brazil, vol 11, 2006 година, стр. 39-64.

су употребљаване и лажне Интернет адресе на којима су се налазиле Интернет презентације постављене од стране извршилаца кривичних дела, са намером да обману наивне кориснике Интернета. Употребљавана је и фалсификована документација државних органа и предузећа Нигерије, Гане, Сенегала, Камеруна и других држава са територије Западне Африке.

Извршиоци кривичних дела преваре познатије као „Нигеријска превара“ углавном су ова дела вршили слањем нежељених тзв. *SPAM* порука. За скривање идентитета на Интернету извршиоци су користили приступе на јавним местима, као нпр. у *Cyber* кафеима, пошто се посетиоци ових сервиса често идентификују јединственом ознаком која представља само генерални идентификатор одређеног компјутера или места конекције. У комуникацији са оштећеним лицима са наше територије коришћени су идентитети званичника наведених држава, свештеника, адвоката и сл.

Коришћење Интернет сервиса и програма на Интернету, за прикривање *IP* адреса такође је веома распрострањено. Ови сервиси извршоцима омогућују анонимно слање електронских порука, без остављања трага о правој *IP* адреси извршиоца кривичног дела, на тај начин што целокупан Интернет саобраћај према одређеним Интернет адресама и страницама иде преко сервиса који потом као траг оставља своју *IP* адресу, а адреса правог корисника се налази на серверу ових сервиса.

Након сазнања да је извршена ова врста преваре и да је дошло до злоупотребе података који су од стране извршилаца кривичних дела прикупљени на напред описане начине полицијски службеници прикупљају доказе и трагове у виду електронских података о оствареној комуникацији која се одвијала између извршилаца кривичних дела и оштећених, као и податке о финансијским трансакцијама које је оштећени извршио према инструкцијама које је добио од извршилаца. Врше се провере лог фајлова у потрази за *IP* адресом, како би се лоцирао сервис преко кога је извршилац кривичног дела слао електронске поруке оштећеном, као и преглед целокупне електронске поште коју је оштећени примио, како би се уочили пропусти направљени од стране извршиоца који могу указати на постојање кривичног дела (нпр. у случају да је извршилац поставио лажни Интернет линк неке институције, провером места хостовања правог Интернет сајта институције и лажног сајта може се уочити да се ради о превари) и места одакле је извршена превара. Након изоловања *IP* адресе и времена слања електронских порука из лог фајлова преко Интерпола се, у зависности од државе са чије је територије извршено кривично дело, врше провере у вези корисника коме је она била додељена у тренутку вршења кривичног дела.

Како би се детекција електронских порука свела на што мањи ниво, данас извршиоци кривичних дела данас шаљу мање количине *SPAM* порука са рачунара заражених рачунарским вирусима, како би се обезбедило што дуже функционисање њиховог слања. Неки комерцијални *SPAM* сервиси укључују *botnet* мреже за слање ових порука, које помажу да се избегну анти - *SPAM* мере на рачунарима корисника и заштите на серверима Интернет провајдера, које функционишу на тај начин што се блокирају *IP* адресе које су постављене на „црне листе“. Данас постоји велики број *IP* адреса са којих је вршено слање ових порука и које су идентификоване као носиоци *SPAM* активности. „Црне листе“ се врло често ажурирају, па извршиоци кривичних дела који користе слање оваквих порука за прибављање података морају да ангажују *botnet* мреже како би избегли блокирање њиховог пријема. Овакав начин слања *SPAM* порука додатно отежава рад полицијских служби МУП-а Републике Србије, пошто корисници

Интернета на територији Републике Србије и не сумњају да поруке које им стижу могу бити штетне. Из наведеног разлога сматра се да постоји и велика „тамна бројка“ када су „Нигеријске преваре“ у питању пошто оштећена лица или нису свесна да су преварена, или их је срамота да пријаве да су оштећени због своје околине. Оштећени се често плаше да пријаве овакве случајеве и пошто их извршиоци кривичних дела убеђују да су сами криви за то што посао није могао да се реализује, прете им да ће их тужити и сл.

У случајевима „Нигеријских превара“ чије су жртве држављани Републике Србије радило се о преварама извршеним на неколико начина и то: слањем обавештења о лажним добицима на лутрији помоћу којих су жртве превара методама социјалног инжињеринга навођене да поверују да су добитници награда, након чега су уплаћивали одређене суме новца да би им се омогућило подизање награде и слањем обавештења о наследству помоћу којих су жртве превара методама социјалног инжињеринга навођене да поверују да су наследиле одређену количину новца, након чега су уплаћивали одређене суме новца да би им се омогућила исплата наслеђеног новца. Кривична дела су иницирана са подручја Нигерије, Сенегала и Бенина, а међународна полицијска сарадња са наведеним државама до данас није довела до значајнијих резултата. Такође су вршене и преваре везане за куповину различитих роба путем *On-line* куповине, након чега роба није испоручивана. Жртве ових видова преваре били су и наши, али и страни држављани, који су оштећени од стране извршилаца кривичних дела са наше територије.

Коришћење метода социјалног инжињеринга је веома присутно када је извршење ових кривичних дела у питању.¹²

Оштећење рачунарских података и програма

Полицијски службеници МУП-у Републике Србије у току 2008. и 2009. године поднели су више кривичних пријава везаних за оштећење рачунарских података и програма. Подносиоци кривичних пријава били су најчешће појединци чији су подаци или програми оштећени од стране извршилаца кривичних дела из различитих мотива, међу којима су најчешћи стицање противправне имовинске користи, освета и сл. Такође су се као оштећене стране појавила и предузећа са територије Републике Србије чији су подаци или програми оштећени од стране запослених лица са наведеним мотивима. Кривична дела су најчешће вршена брисањем рачунарских података и програма са рачунара оштећених, као и уклањањем одређених, битних компоненти програма (нпр. активационих кључева).

¹² Социјални инжињеринг је акт манипулације којим се људи наводе да одају поверљиве информације о себи. Ова техника заснива се на ометању пажње одређеног лица у циљу прикупљања информација које оно иначе не би одало, а како би се ти подаци касније злоупотребили (ради одавања корисничких имена, лозинки или, нпр. података о платним картицама). Све методе социјалног инжињеринга заснивају се на специфичним правилностима у процесу доношења одлука познатијем као „погрешна когниција“ која представља образац неправилног просуђивања људи који се појављују у одређеним, специфичним ситуацијама.

Неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података

Полицијски службеници Одељења за борбу против високотехнолошког криминала Службе за борбу против организованог криминала су због постојања основане сумње да су извршили кривична дела Неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података и фалсификовање исправе у 2009. години поднели кривине пријаве против три лица која су у дужем временском периоду “клонирала” СИМ картице за мобилне телефоне, од којих је већина била власништво већ постојећих постпејд корисника, тако да је овом приликом нанета имовинска штета домаћим мобилним оператерима у укупном износу од 62.800.405,00 динара.

Овако “клониране” картице користиле су се за позивање високотарифних сервиса (хотлајн сервиси, сервиси за забаву и друго) који се налазе углавном у државама континента Африке, а неки и у Молдавији и Украјини, чиме је овим сервисима неосновано омогућена наплата по основу непостојећих услуга.

Домаћи мобилни оператери исплатили су, у складу са постојећим међународним уговорима о пружању услуга, иностраним оператерима услуге роминга, као и услуге наведених сервиса.

С обзиром на то да су позиви упућивани са бројева који припадају наведеним мобилним оператерима, стварни власници картица нису имали сазнања о томе да су наведени сервиси позивани све до момента пристизања рачуна које су им доставили мобилни оператери са којима су закључили уговоре о постпејд услугама. Код осумњичених су пронађени хардверски и софтверски алати за клонирање СИМ картица, као и датотеке клонираних СИМ картица са којих су позивани високотарифирани сервиси у иностранству.

Неовлашћено коришћење рачунара или рачунарске мреже

Министарство унутрашњих послова Републике Србије поднело је више кривичних пријава проти лица која су ово кривично дело извршила на тај начин што су искористила непажњу својих познаника, корисника различитих Интернет сервиса, да прибављају податке (корисничка имена и шифре) о њиховим налозима, а затим да исте преузму како би вршили различите врсте притисака на оштећене да на своју штету, у корист извршиоца кривичног дела или на своју штету изврше одређене радње. Ово кривично дело такође се јављао у стицају са кривичним делом угрожавање сигурности, пошто су са преузетих налога познаницима оштећених лица упућивање озбиљне претње. Многи корисници непознају довољно добро начин функционисања рачунара, и врло често нису спремни и вољни да предузму мере заштите за које они сматрају да су сувише скупе, превише технички захтевне или да је потребно утрошити превише времена на њихову употребу.¹³

У једном случају у току 2008. године поднета је кривична пријава против два лица која су на рачунар оштећеног предузећа које се бави играма на срећу инсталирала рачунарски програм којим су вршене преправке добитних тикета за трке, након чега је од стране

¹³ М. Abrams, Н. Podell: Information Security: An Integrated Collection of Essays, Computer Society Press, Los Alamitos, CA USA, 1995, стр.117.

једног од извршилаца на наплату поднет фалсификовани тикет са добитном комбинацијом на износ од 400.000,00 динара.

Спречавање и ограничавање приступа јавној рачунарској мрежи

На територији Републике Србије више предузећа поднело је кривичне пријаве за наведено кривично дело а најчешћи облик извршења је вршење ДДОС напада. У овим нападима вршено је „засипање“ рачунара, и других мрежних уређаја, као што су нпр. рутери, многобројним захтевима (као што су *SYN* захтеви или *ICMP* захтеви) на које они могу да одговоре, али им се на такав начин онемогућавало да одговоре на праве захтеве који су им упућени од стране корисника. Оваквим радњама извршиоци кривичних дела блокирали су рад заражених рачунара тј. сервера.

Ови напади су коришћени за нарушавање пословног кредибилитета предузећа, за вршење освете према оштећенима, различите врсте изнуда, притисака и уцена итд. Објекти напада (најчешће предузећа чији је рад заснован на коришћењу Интернета за рекламирање, продају и др.) обавештавани су да су предмет напада. Након тога напади су вршени у релативно кратком времену, и у мањем обиму, како би се демонстрирало шта је све нападач у стању да уради са корпоративном мрежом предузећа и како корпоративну мрежу или Интернет сајт може да обори, тј. онеспособи на неко време.

Након демонстрације ових могућности, поставља се неки захтев (често и финансијске природе) од стране извршилаца кривичних дела, под претњом да ће доћи до много већег и јачег напада. Ако предузеће не може да плати тражену суму новца, или испуни оно што нападач тражи, онда услеђује јачи напад уз нове захтеве.

Овакви напади су вршени из иностранства на наша предузећа, али и од стране извршилаца са наше територије на преузећа и институције у иностранству.

Поред ових напада уочени су и напади на Интернет сајтове многих институција и предузећа на територији Републике Србије од стране извршилаца кривичних дела са територије Косова и Метохије који су у току 2008. и 2009. године ДДОС нападима њихове сервере краткотрајно онеспособљавали за рад.

Угрожавање сигурности и ширење расне, верске и националне мржње и нетрпељивости

Министарство унутрашњих послова Републике Србије поднело је више кривичних пријава за кривично дело Угрожавање сигурности. Ова кривична дела вршена су преко Интернет сајтова, на социјалним мрежама као што је нпр. *Facebook*, као и путем електронских порука. Поднето је и више кривичних пријава за кривично дело Ширење расне, верске и националне мржње и нетрпељивости која су извршена преко наведених Интернет сервиса. Овим путем су од стране извршилаца кривичних дела упућиване поруке чији садржај представља озбиљну претњу појединцима и групама.

На Интернету се пружа и могућност постављања истих Интернет страница на већем броју сервера широм света који се хостују у различитим државама да би се избегла

могућност скидања тј. укидања овог садржаја од стране државних органа.¹⁴ Овај проблем такође се појавио и у раду овог Министарства.

Злоупотреба деце у порнографске сврхе на Интернету

Полицијски службеници Министарства унутрашњих послова поднели су више кривичних пријава против извршилаца кривичних дела из ове области због постојања основане сумње да су извршили кривично дело Приказивање порнографског материјала и искоришћавање деце за порнографију ширењем оваквог материјала путем Интернета. Против једног од осумњичених поднета је и кривична пријава због постојања основане сумње да је лично учествовао у стварању оваквог материјала тј. да је извршио обљубу над дететом. У више случајева подношене су кривичне пријаве због дистрибуције наведеног материјала путем Интернета. Уочено је да постоји и већи број лица са наше територије која врше „скидање“ наведеног садржаја са Интернета, у време када наведена радња није била забрањена тј. инкриминисана у Кривичном законiku као кривично дело, о чему је Одељење за борбу против високотехнолошког криминала обавештавано од стране полицијских служби из иностранства путем Интерпола.

Амерички служба FBI (*Federal Biro of Investigation*), на основу података о мрежи интернет педофила у САД коју је открило Одељење за борбу против високотехнолошког криминала Министарства унутрашњих послова Републике Србије поднело је кривичну пријаву против свештеника - педофила из америчке државе Њу Џерси. Правосудни органи САД су прихватили оперативни полицијски материјал о мрежи педофила коју је доставио МУП Републике Србије и у фебруару 2009. године започео сопствену истрагу, која је довела до хапшења осумњиченог. Откривено је да ово лице своје активности обављало у оквиру неколико педофилских група, као и да је имао регистровано неколико лажних налога електронске поште и налога у тзв. „собама за четовање“, да се на Интернету лажно представљао као 13 - годишња девојчица или као женска особа и мајка од 25 година. Приликом претреса његове куће, пронађен је педофилски материјал на чије је постојање указивао МУП Србије, као и други докази.

Поред наведеног случаја, полицијски службеници Одељења за борбу против високотехнолошког криминала Службе за борбу против организованог криминала су остварили и сарадњу са другим полицијским службама широм света преко Интерпола, са којима се активно размењују оперативни подаци о Интернет сајтовима и сервисима на Интернету преко којих се објављује, размењује или продаје забрањени материјал.

4. ПРОБЛЕМИ У БОРБИ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Нови изазови које експанзија високотехнолошког криминала поставља пред полицијске службе састоје се у чињеници да је прикупљање тачних статистичких података о овим активностима на Интернету веома отежано. Статистика везана за број кривичних пријава и кривичних дела из области високотехнолошког криминала није довољно прецизан показатељ којим се могу исказати појавни облици, нити њихова коначна структура и обим. Она може представљати само тренутни показатељ и оријентир, а никако релевантан приказ трендова. Такође треба нагласити и да је тамна бројка везана за број кривичних дела најизраженија управо када је у питању овај тип криминалних активности. Чињеница је да великој тамној бројци доприноси и податак да су жртве

¹⁴ Y. Timofeeva: Hate speech online: restricted or protected? Comparison of regulations in the United States and Germany, J. Transnational law & policy, 2003., стр.256.

ових кривичних дела често несвесне да је над њима извршено кривично дело. Када су у питању предузећа која су оштећена код њих се јавља и додатни страх од пријављивања због могућности нарушавања пословног угледа и губитка поверења њихових клијената. Савремене информационе технологије, меморијски капацитети рачунарских мрежа и глобална дистрибуција података и информација додатно отежавају могућност откривања ових кривичних дела.

Неки од проблема који се појављују пред Министарством унутрашњих послова Републике Србије, када је откривање ових кривичних дела су:

1. Техничка опремљеност и оспособљеност полицијских службеника везана за откривање извршилаца у *On-line* окружењу.
2. Правна регулатива која није у складу са савременим облицима извршења кривичних дела из области високотехнолошког криминала, при чему се врло често јавља потреба за усклађивањем постојећих законодавних решења правним прописима који би пратили промене у техничкој структури и савремене токове у развоју информационог друштва.
3. Недостатак операционалних обука које би омогућиле да полицијски службеници који се баве спречавањем високотехнолошког криминала буду довољно обучени и технички опремљени за вршење ових задатака.
4. Веома велике потешкоће у откривању извршилаца кривичних дела који користе лажне идентитете у *On-line* окружењу, посебно када се у обзир узме чињеница да је у великом броју случајева међународна полицијска сарадња лоша, а да у неким чак и не постоји.
5. Потешкоће у откривању тачне локације извршења кривичног дела, пошто се ова кривична дела врше са многих места широм света, а у великом броју случајева извршиоци кривичних дела користе мреже са јавним проступом.

Министарство унутрашњих послова Републике Србије такође има и потребу за приснијом и ефикаснијом сарадњом са државним институцијама које се у свом раду сусрећу са високотехнолошким криминалом или се баве истраживањем ове појаве. Поред државних институција са којима Министарство унутрашњих послова има сарадњу, потребно је и укључивање додатних институција које својим ангажовањем могу знатно да допринесу истраживању ове појаве и успостављању ефикаснијег система спречавања кривичних дела из ове области. Посебан проблем је што недостаје ефикасан систем надгледања Интернета у циљу откривања кривичних дела из области високотехнолошког криминала, као и ефикасна платформа за пријављивање ових кривичних дела у *On-line* окружењу. У овом смислу потребна је и боља сарадња са факултетима, невладиним организацијама итд. У нашој држави још увек није установљен ефикасан *CERT* тим (*Computer Emergency Responce Team*) за спречавање ових кривичних дела, нити су одређене институције чији би представници требали да се ангажују у овом правцу. Успостављање *CERT* тима у великој мери би допринело ефикаснијем спречавању ових кривичних дела, бржем и одговорнијем приступу у истраживању ове појаве и обједињеном одговору на изазове и претње које ова појава доноси.

Нови напади на Интернету који нису усмерени на рачунарске системе (синтактички) већ на њихове кориснике (семантички), такође представљају велики проблем. У Републици Србији је уочен већи број оваквих напада (фишинг, Нигеријске преваре итд.), у којима су жртве саме себи нанеле штету након што су од стране извршиоца

кривичног дела доведене у заблуду помоћу рачунарске мреже и рачунара, који су били само оруђе у рукама извршиоца како би се жртва навела да изврши одређене радње у њихову корист. Како би се овакав вид кривичних дела из области високотехнолошког криминала ефикасно спречавао потребно је веће ангажовање државних институција, невладиног сектора, медија, као и шире друштвене заједнице.

5. ЗАКЉУЧАК

Искуства Министарства унутрашњих послова Републике Србије у борби против високотехнолошког криминала говоре о томе да се ради о кривичним делима чији се појавни облици мењају у веома кратком року са појавом нових техничко-технолошких решења, као и да се ова кривична дела врше у веома кратком временском року, готово свуда где постоји Интернет - па самим тим и у Републици Србији. Са феноменом високотехнолошког криминалитета су се, поред Одељења за борбу против високотехнолошког криминала, у оквиру Министарства унутрашњих послова суочиле и друге организационе јединице, а сузбијање великог броја појавних облика високотехнолошког криминалитета, посебно оних са елементима организованог и транснационалног криминала, на територији Републике Србије данас је веома сложен и тежак задатак, који из дана у дан представља све већи изазов за Министарство унутрашњих послова Републике Србије. Савремене информационе технологије, меморијски капацитети рачунарских мрежа и глобална дистрибуција података и информација додатно отежавају могућност откривања ових кривичних дела и проналажење извршилаца.

Поред државних институција са којима Министарство унутрашњих послова има сарадњу, потребно је и укључивање додатних институција, недостаје ефикасан систем надгледања Интернета у циљу откривања кривичних дела високотехнолошког криминала, као и ефикасна платформа за пријављивање ових кривичних дела у *On-line* окружењу. Као посебан проблем се јавља и потреба за бољом сарадњом са факултетима, невладиним организацијама итд. Потребно је да се установи ефикасан *CERT* тим (*Computer Emergency Responce Team*) за спречавање ових кривичних дела, и одреде институције чији би представници требали да се ангажују у овом правцу. Успостављање оваквог тима у великој мери би допринело ефикаснијем спречавању ових кривичних дела, бржем и одговорнијем приступу у истраживању ове појаве и обједињеном одговору на изазове и претње које ова појава доноси.

У Републици Србији је уочен већи број семантичких напада па је потребно веће ангажовање државних институција, невладиног сектора, медија и шире друштвене заједнице, како би се извршила ефикасна превенција. Превентивно деловање државних органа као што су полиција и тужилаштво има кључну улогу када је спречавање ове појаве у питању. Такође је потребно и што хитније деловати проактивно, искористити потенцијал медија и скренути пажњу домаћој јавности на финансијске губитке који настају као последица ових кривичних дела. Превентивна улога полиције у заштити корисника Интернета са територије Републике Србије оваквим активностима сигурно би била успешнија и сврсисходнија од репресивних активности које се предузимају након сазнања да је кривично дело извршено.

Литература:

1. E. Athanasopoulos et. all.: Antisocial Networks: Turning a Social Network into a Botnet, Section: Network Security, Lecture Notes In Computer Science, Berlin, Република Немачка, 2008. година, стр. 146-160.
2. M. Abrams, H. Podell: Information Security: An Integrated Collection of Essays, Computer Society Press, Los Alamitos, CA USA, 1995 година, стр.117.
3. Y. Timofeeva: Hate speech online: restricted or protected? Comparison of regulations in the United States and Germany, J.Transnational law & policy, Florida, USA, 2003. година, стр.256.
4. В. Урошевић: Злоупотребе платних картица и рачунарске преваре, Правни информатор, Београд, 2009. година, стр. 4.
5. M. Chawki: Anonymity in Cyberspace: Finding the Balance between Privacy and Security, Revista da Faculdade de Direito Milton Campos, Nova Lima, Brazil, vol 11, 2006 година, стр. 39-64.
6. РАСО Serbia-Пројекат за борбу против економског криминала у Републици Србији: Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе, 2008. година, стр.38.
7. Л. Комлен-Николић et.al: Сузбијање високотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010. година, стр. 231.
8. М. Милошевић, В. Урошевић: Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53-64.