



UNIVERSITETI I EVROPËS JUGLINDORE
УНИВЕРЗИТЕТ НА ЈУГОИСТОЧНА ЕВРОПА
SOUTH EAST EUROPEAN UNIVERSITY

ВТОР ЦИКЛУС НА СТУДИИ (ПОСТДИПЛОМСКИ СТУДИИ)

МАГИСТЕРСКИ ТРУД

ТЕМА: „ОБЛИЦИ НА КОМПЈУТЕРСКИ КРИМИНАЛ“

Кандидат:

Ѓорѓи Кочовски

Ментор:

проф. д-р Исмаил Зејнели

Тетово, мај 2020

Апстракт

Денешното информатичко општество се соочува со голем број на предизвици во борбата со организираниот криминал, а посебно со „компјутерскиот криминал и компјутерскиот тероризам“ како нови модели на закани во 21 век. Колку повеќе информатичката технологија станува софистицирана, толку повеќе стануваат комплексни методите и средствата кои се употребуваат во борбата против криминалните активности, посебно кај компјутерскиот тероризам.

Во овој магистерски труд се разгледани формите и облиците на компјутерски криминал и нивните карактеристики. Исто така како дел од истражувањето во овој магистерски труд се разгледани видовите на компјутерски криминал кои се појавуваат во Република Северна Македонија во текот на изминатите години, и е извршена анализа на облиците и формите кои се појавуваат во нашата земја. Исто така како придонес кон оваа тема е извршена анализа на форензичка алатка *FTK Imager* која се користи како средство за собирање на докази при појавен компјутерски криминал, и која служи како средство за анализата на собраните докази во правната регулатива. Како втора алатка која е анализирана, е алатка за следење на интрузии *Suricata* која може да дејствува како систем за откривање на упад (IDS) и систем за спречување на упад (IPS), или да се користи за следење на мрежната безбедност.

Клучни зборови: компјутерски криминал, дигиталната форензика, *FTK Imager*, *Suricata*.

Abstract

Today's information society faces a number of challenges in the fight against organized crime, in particular "computer crime and computer terrorism" as new patterns of threats in the 21st century. The more information technology becomes sophisticated, the more complex methods and tools are used to combat criminal activities, especially in computer terrorism.

This master's thesis examined the forms and forms of cybercrime and their characteristics. Also, as part of the research in this master's thesis, the types of cybercrimes that appear in the Republic of Macedonia over the past years have been reviewed and an analysis of the forms that appear in our country has been carried out. Also, as a contribution to this topic, an analysis of a type of forensic tool *FTK Imager* is used as a means of collecting evidence in an emerging cybercrime and serves as a means of analyzing the collected evidence in the legal regulation. The second tool that is analyzed is a *Suricata Surtivity Monitoring Tool* that can act as an Intrusion Detection System (IDS) and Intrusion.Prevention System (IPS), or be used to monitor network security.

Key words: cybercrime, digital forensics, FTK Imager, Suricata .

СОДРЖИНА

Апстракт.....	2
Вовед.....	6
Глава I.....	8
1. Форми и облици на компјутерски криминал.....	8
2. Компјутерска измама.....	9
3. Кражба на идентитет.....	12
3.1. Хакирање	13
4. Dark Web.....	15
4.1 VPN.....	17
Глава II.....	19
2. Кривични дела од областа на компјутерски криминал опфатени во кривичниот законик.....	19
2.1 Загрозување на сигурноста по пат на информатички системи.....	20
2.2 Злоупотреба на лични податоци	23
2.3 Спречување на пристап кон јавен информатички систем.....	25
2.4 Повреда на авторско право и сродни права.....	26
2.5 Покажување на порнографски материјал на дете.....	30
2.6 Производство и дистрибуција на детска порнографија	34
2.7 Оштетување и неовластено навлегување во компјутерски систем.....	36
2.8 Правење и внесување компјутерски вируси.....	39
2.9 Компјутерска измама.....	42

2.10 Изработка и употреба на лажна платежна картичка	44
2.11 Ширење на расистички и ксенофобичен материјал по пат на информатички системи.....	47
Глава III.....	51
3. Компјутерски вируси.....	51
3.1 Социјален инженеринг	56
3.2 Детска порнографија	62
3.3 Ddos Attack и Botnet.....	68
3.4 Phishing.....	74
3.5 Scam.....	79
3.6 Ransomware	81
3.7 Cyberbullying.....	88
Глава IV.....	88
4. Идентификација и заплена на дигитални докази.....	88
4.1. Идентификација и заплена на дигитални докази на персонален или преносен компјутер.....	90
4.2 .Идентификација и заплена на дигитални докази на мобилен уред.....	95
4.3. Идентификација и заплена на дигитални докази од уреди кои поседуваат меморија.....	97
Заклучок.....	102
Користена литература.....	105
Интернет извори.....	108

Вовед

Светот денес е во фаза на технолошки промени и иновации, што доведува до промени на сите делови од современиот живот и воспоставување на т.н. информатичко општество. Ако сакаме Република Северна Македонија да го достигне статусот на „напредно информатичко општество“, треба да се анализираат неколку прашања. Напредното информатичко општество се соочува со голем број на предизвици во борбата со организираниот криминал, посебно со „компјутерскиот криминал и компјутерскиот тероризам“, сегменти кои претставуваат нови модели на закана во 21-от век. Колку повеќе информатичката технологија станува посоефицицирана, толку повеќе стануваат комплексни методите и средствата кои се употребуваат за борба против криминалните активности, посебно кај компјутерскиот тероризам.

Република Северна Македонија не претставува исклучок од земјите кои зголемено се соочуваат со овој софистициран вид на организиран криминал. Целта на Република Северна Македонија е да биде дел од глобалната безбедносна мрежа во борба против перењето пари, организираниот криминал, финансирањето на тероризам и влегувањето на „валканите пари“ во економијата. Нашата земја презема напори за да се заштити од различните криминални активности, како што се кражба на личните податоци, високо безбедносни тајни, воени планови, но и измамнички активности од типот на „крадење пари“ од кредитни/дебитни картички и друго.

Компјутерскиот тероризам и криминалните активности имаат видливо неповолно влијание врз земјата, односно врз нејзината економија, безбедноста на граѓаните, јавниот живот и човековите права и слободи. Поради сите горенаведени причини, овој нов облик на организиран криминал треба да биде спречен од понатамошно ширење не само на територијата на РСМ, туку и во целиот свет.

Денешниот свет се соочува со голем број на предизвици во борбата со феноменот на организираниот криминал, особено „сајбер криминалот“ и „сајбер тероризмот“, како нови модели на закана во 21-от век.

Колку посоефицирана станува информатичката технологија, толку покомплексни стануваат методите и средствата кои се употребуваат за борба со криминалните активности, особено кај „сајбер тероризмот“. Република Северна Македонија не претставува исклучок од земјите кои зголемено се соочуваат со овој софистициран вид на организиран криминал. Како земја, нашата цел е да бидеме дел од глобалната безбедносна мрежа во борба против перењето пари, организираниот криминал, финансирањето на тероризам и влегувањето на „валканите пари“ во економијата.

Република Северна Македонија треба да преземе сериозни мерки за да го заштити својот безбедносен систем, посебно државните/владините (институции), со цел спречување на крајби на личните податоци, зачувување на високо безбедносни тајни и воените планови, како и спречување на измамнички активности, односно „крадење пари“ од кредитни/дебитни картички. Сајбер тероризмот и криминалните активности имаат видливо неповолно влијание врз земјата, т.е. врз нејзината економија, безбедноста на граѓаните, јавниот живот и човековите права и слободи. После повеќе од еден век постоење на електронската технологија, луѓето успеале да го прошират електронскиот нервен систем во глобален опфат, надминувајќи ги границите на просторот и времето. На тој начин успеале да ја покријат нашата планета секаде каде што се простираат нејзините физички граница. Интернетот го направи тоа што визионерот на комуникацијата Маршал Меклуан (Marshall McLuhan) го нарече глобално село, кое конечно стана реалност. Имено, Меклуан уште во 70-тите години на минатиот век го креирал концептот на глобално село, чишто делови биле меѓусебно поврзани со електронски нервен систем долго време пред тоа реално да се случи.

ГЛАВА ПРВА

1. Форми и облици на компјутерски криминал

Како што постојат големи можности за злоупотреба на компјутерите и информатичката технологија, така се различни и формите на можното противправно однесување, па оттаму постојат голем број класификации на кривични дела.¹ Компјутерите и информатичката технологија може да послужат вршење на традиционалните форми на криминал, но, исто така, и за сосема нови форми на злоупотреба на компјутерите, компјутерските системи и компјутерските мрежи поврзани со криминал. Традиционалните форми на криминал вклучуваат: компјутерска кражба, проневера, измама и фалсификат.²

Новите современи форми на компјутерски криминал вклучуваат специфични кривични дела што можат да се направат само со употреба на компјутери, компјутерски системи и компјутерски мрежи. Тоа се хакирањето, создавањето, и дистрибуцијата на вируси. Големите практични можности што се предвидени од страна на информатичката технологија, со себе носат ризик од ширење на масовната употреба на прислушувањето, кражбите на деловни тајни, повреда на приватноста, но во последно време и на реалната закана од терористички напади.³ Проф. д-р Владимир Водинелиќ⁴ при анализа на претходната работа на криминолози и адвокати поврзани со компјутерскиот криминал, а воедно обидувајќи се во поимот *компјутерски криминал* да вклучи повеќе модерни форми на криминални активности, истиот го поделил во четири групи:

1. неовластено користење на компјутери;
2. манипулирање со компјутери;
3. компјутерска шпионажа;
4. саботажа на компјутери.

¹ Jovičić, D., Bošković, M., Kriminalistika metodika, Banja Luka 2002, 446–449.

² Šarkiћ, N., Prlija, D., Damjanović, K., Marić, V., Tivković, V., Vodinelić, V., Mrvić-Petrović, N.: Pravo informacionih tehnologija, Beograd 2011, 3.

³ Jovašević, D., Hašimbegović, T., Krivičnopravna zaštita računarskih podataka, Beograd 2008, 3.

⁴ V., Vodinelić, Pravo informacionih tehnologija, Beograd 2011.

Оваа поделба е доволно широка, поради што може да покрие најголем дел од кривичните дела поврзани со компјутерскиот криминал, како што се: компјутерска кражба, измама, проневера на пари, фалсификување, нарушување на приватноста, шпионажа, тероризам, хакирање, пиратски софтвер, создавање на вируси, и дистрибуција на вируси. Овие кривични дела ќе бидат одделно предмет на разгледување во овој магистерски труд, токму поради нивната фреквенција во пракса.

2. Компјутерска измама

Компјутерските измами се извршуваат со намера за стекнување протиправна материјална корист за себе, или за некој друг, со тоа што кај нив не се доведува или одржува во заблуда некое лице, како што е во случаите со обичните измами од типот на материјалните кривични дела со кои се предизвикува штета, туку⁵ заблудата се однесува на компјутер во којшто се внесуваат неточни податоци, се пропушта внесувањето на точни податоци, или компјутерот се користи за остварување на измами во кривично-правна смисла на било кој друг начин. Компјутерските измами претставуваат најраширен облик на компјутерски криминал.⁶

Бројот на облици на измами, како и начинот на нивната реализација е практично неограничен, а во пракса се среќаваат „примитивни“ и „груби“ измами, но и измами за кои е користен висок степен на вештина и рафинираност.⁷ Во шемите за компјутерски измами секогаш се открива некој постар облик на измама којшто се користел претходно.⁸ Сите шеми на измами којшто се регистрирани на интернет, всушност се преработени и прилагодени верзии на шеми со коишто некогаш се „ставени“ во заблуда невнимателни и лесноверни жртви.

⁵ Directive on electronic commerce <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF> на 14.04.20 во 17:00 часот.

⁶ Feješ, I., Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti – izlaganje na konferenciji, 2000.

⁷ Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, <http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf> на 14.04.20 во 17:00 часот

⁸ www.ugd.edu.mk/private_UserFiles_biljana.kosturanova_Desktop_Trudovi_Jugoslav_Achkoski_Scientific_Papers_elektronska_verzija_Sajber_kriminal_i_zastita_na_digitalnite_podatoci_vo_kompjuterskite_mrezi, 34.

Компјутерските измами се карактеризираат со големо продирање заради обемот на интернетот како пазар и како медиум со којшто сè се случува многу брзо, но делумно и заради ниските трошоци за извршување на ваквиот вид на измами.⁹ Компјутерските измамници ги злоупотребуваат карактеристиките на *сајбер просторот* кој придонесува раст на електронската трговија, односно анонимноста/дистанцата помеѓу продавачот и купувачот, и моменталната трансакција.¹⁰ На тој начин тие ја користат и предноста на фактите дека измамата преку интернет не бара пристап до некој систем за исплата, како што во суштина за тоа бара секој друг вид на измама, а исто така и фактот дека дигиталниот пазар е сè уште недоволно уреден. Поради ваквата неуреденост на дигиталниот пазар се создава одредена конфузија за потрошувачите, што за компјутерските измамници создава идеални услови за компјутерски измами.¹¹

Компјутерските измами се најраспространетата форма на компјутерски криминал и се сретнуваат во секој дел од бизнисот, што може да влијае на протокот на стоки и пари. Компјутерските измами по својата природа се најблиску до економскиот криминал, а во литературата, речиси без исклучок, овие феномени се третираат како појава на економски криминал.

Компјутерските измами се најбројни во следните области:¹²

1. финансиски менаџмент;
2. осигурување;
3. даноци;
4. социјална сигурност;
5. прогласување банкрот;
6. перење на пари.¹³

⁹ Petrović R. S., *Kompjuterski kriminal*, op. cit. 35.

¹⁰ Petrović R. S., *Kiberterorizam*, *Vojno delo*, god. LIII, br. 2/2001, 25.

¹¹ Petrović R. S., *Neki aspekti nacionalne bezbednosti u informacionom dobu*, *Nauka, Tehnika, Bezbednost (NTB)*, Rad po pozivu, UDC: 681.324; 65.012.8, Godina XI, Broj 1, Septembar 2001, 52.

¹² Petrović, R. S., *Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije: Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd 2000, 25.

Општа карактеристика на оваа активност е доведување на неког во заблуда, со цел да се стекне противправна имотна корист. Бројот на формите на компјутерска измама, како и начинот на нивното остварување е практично неограничен, а во пракса се среќаваат од многу примитивни и груби компјутерски измами, па се до оние измами во кои сторителот има голем степен на вештина и префинетост.¹⁴ Најпозната форма на компјутерска измама е „нигериската измама“, којашто и припаѓа на групата измами кои се направени со инвестирање одредени суми на пари од страна на измамени лица во одредени работи, се разбира, со претходно дадено ветување од престапникот дека ќе оствари значително поголема парична добивка.¹⁵ Овој вид измама за прв пат се појавил во 1980-тите години, и е поврзан со забрзаниот економски раст во Нигерија.¹⁶ Измамите во голема мера се вршеле со испраќање деловни понуди за трговија или експлоатација на нафта на странци, благодарение на што Нигерија економски зајакнала.¹⁷

Измамите се вршеле со испраќање на лажни пораки преку компјутер или електронска пошта за наводна добивка во игри на среќа, пораки поврзани со хуманитарни придонеси, пораки поврзани со „љубов и бизнис понуди“, пораки поврзани со преземање на наследство од некои непознати роднини итн.¹⁸

Измамата била спроведувана со првичен избор на жртвата и нејзино последователно убедување со методите на социјален инженеринг, за истата да уплати однапред одредена сума на пари.¹⁹ Оваа сума на пари во повеќето случаи била многу помала од износот што ќе требало да се добие како добивка од некој фонд, или пак од испраќачот на пораката.²⁰

¹³ Matijašević, J., Krivičnopravna regulativa računarskog kriminaliteta; Pravni fakultet za privredu i pravosude, Novi Sad 2013, 166.

¹⁴ Urošević, V., „Nigerijska prevara u Republici Srbiji“, Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Beograd, 145-156.

¹⁵ European Committee on Crime Problems, European Committee of Experts on Crime in Cyber-Space, Draft Convention on Cyber-crime, April 2000., <http://europa.eu.int>, 166.

¹⁶ Jovićić, D., Bošković, M., Kriminalistika metodika, Banja Luka 2002, 250.

¹⁷ Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.oun.org, 25.

¹⁸ Македонско сонце 501/ 06.02.2004, 166.

¹⁹ Drakulić, M., Drakulić, R., CYBER KRIMINAL, , Fakultet organizacionih nauka u Beogradu, 166.

²⁰ Веб сајтови на: Претседател Ѓорѓи Иванов (www.president.gov.mk); Бившиот Претседател Бранко Црвенковски, 2004-2009 (www.president.gov.mk); A1 (www.a1.com.mk); Телма (www.telma.com.mk); Музеј на Македонија (www.musmk.org.mk) на 14.04.20 на 17:00 часот.

Со помош на е-поштата на примачот се барала помош за да се добијат големи суми на пари, од неколку стотици илјади, до неколку десетици милиони долари, а по уплатата би се добил одреден процент од ветената заработка.²¹

Според одредени личности коишто биле жртви на овој вид измама, извршувањето на дејството се вршело на неколку начини: а) со испраќање на известување за лажни добивки од игри на среќа по што жртвите требало да уплатат одредена сума пари за да им се овозможи да ја подигнат наградата; б) известување за наследство со коешто жртвите на измамата со методи на социјален инженеринг се наведувале да веруваат дека наследиле одредена сума на пари, по што тие уплаќале суми на пари што ќе овозможат исплаќање на наследството.²²

3.Кражба на идентитет

Кражба на идентитет е форма на крадење податоци за лична идентификација на друга личност, а со тоа некој лажно се претставува дека е друга личност, притоа преземајќи го идентитетот на личноста која е лажирана, најчесто со цел да пристапи до ресурсите на таа личност, или да добие средства и други бенефиции во името на таа личност.²³ Жртвите од кражба на идентитет (тука се вбројуваат лицата чии идентитети се преземени од страна на крадец на идентитети) може да претрпат различни последици ако бидат одговорни за делата кои ќе ги изврши крадецот. Организации и индивидуи кои се измамени или ограбени од страна на крадец на идентитет можат да претрпат и најразлични последици и загуби, до мера да станат и жртви. Терминот кражба на идентитет бил воведен во 1964 година, но сепак, бидејќи идентитетот не може буквално да биде украден, двосмислени термини се измама на идентитет, или присвојување на идентитет.²⁴

²¹ Активности за превенција и справување со последици од сајбер тероризам. Министерство за информатичко општество <http://www.mio.gov.mk/?q=node/1911>, 250.

²² Petrović R. S., Globalno informaciono ratovanje, Zbornik radova (CD-ROM), YU INFO '99, Kopaonik, 22–26.marta 1999; Petrović R. S., Kiber prostor - peta dimenzija ratovanja, Vojni informator, br. 4, julavgust 2001, 156.

²³ https://mk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B0%D0%B6%D0%B1%D0%B0_%D0%BD%D0%B0_%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%82%D0%B5%D1%82 на 14.04.20 на 17:00 часот.

²⁴ <https://hbogo.mk/filmovi/krazhba-na-identitet> на 14.04.20 на 17:00 часот

Утврдување на врската помеѓу повреда на податоците и кражба на идентитет претставува предизвик, пред сè, бидејќи жртвите при кражба на идентитет често не знаат како нивните лични податоци се добиени. Според извештајот направен за FTC, кражбата на идентитет не е секогаш забележлива од страна на индивидуалните жртви.²⁵

Измама на идентитетот често е (но не секогаш) последица на кражба на идентитет. Некој може да украде или присвои лични податоци, без притоа да изврши кражба на идентитет со користење на информации за некое лице, ако на пример бидат пробиени големи количини на податоци.

Студијата на Accountability Office на Владата на САД утврдила дека „повеќето прекршувања не резултираат со откриени случаи на кражба на идентитет“. Подоцна, необјавена студија на Карнеги Мелон Универзитетот, истакнала дека „најчесто, причините за кражба на идентитет не се познати“.²⁶

3.1 Хакирање (hacking)

Основна карактеристика на хакирањето е нарушување на системот за заштита и неовластено навлегување во информациските системи. Зборот *hacking* потекнува од англискиот јазик, а во слободен превод значи „човекот против компјутерот“. Постојат неколку форми на реализација на оваа активност.

Најчесто хакерите со користење на различни методи и техники, ги набавуваат сите информации потребни за успешен упад во туѓ информациски систем, или благодарение на претходно дефинирани програми кои се дизајнирани за да се избегнат вообичаените параметри на заштита, навлегуваат во туѓи информациски системи. За да се постигне оваа цел, потребно е големо предзнаење од математика и електроника.²⁷

²⁵ Federal Trade Commission – 2006 Identity Theft Survey Report, на 14.04.20 на 17:30 часот.

²⁶ Federal Trade Commission – 2006 Identity Theft Survey Report, на 15.04.20 на 17:00 часот.

²⁷ http://en.wikipedia.org/wiki/Hacker_%28computer_security%29 на 15.04.20 на 17:00 часот.

Основни карактеристики на хакирањето се:²⁸

1. неовластен пристап до информацискиот систем;
2. насилан пристап или пробив на системот за заштитата;
3. пристапот се остварува со упад во информацискиот систем;
4. потребно е високо професионално знаење за да се постигне упадот;
5. местото на нападот е оддалечено од местото на напаѓачот;
6. хакерите прават и други работи, како шпионажа, измама, проневера, кражба на услуги, саботажа, дистрибуција на вируси итн.;
7. хакерот дејствува независно или во група.

Најчестите последици од хакерството се:

1. нарушување на системот за заштита;
2. забавување или блокирање на функциите на системите;
3. неовластен пристап;
4. оштетување;
5. модификација или уништување на податоци;
6. нелегална дистрибуција на програми;
7. кражба;
8. ширење на вируси.

Дифејсмент е напад врз веб-страница со којшто се менува визуелниот изглед на сајтот, или на веб-страницата. Овие се типични функции на дефајсори, кои се пробиваат во веб-сервер и го заменуваат веб-сајтот хостиран со еден од нив.²⁹

Одредувањето е генерално наменето на електронски графити, и како и другите форми на вандализам, се користи за ширење на пораките од политички мотивирани „сајбер-демонстранти“ или активисти.³⁰

²⁸ Zirojević, M., Upotreba novih informatičkih i komunikacionih medija u svrhe terorizma – Revija za bezbednost Centar za bezbednosne studije, Godina II, br. 11/2008 Beograd 161.

²⁹ Drakulić, M., Osnovi kompjuterskog prava, Beograd, 1996, 449.

Најдобриот пример кој покажува колку се опасни хакерите доаѓа од Велика Британија, каде што програмерите на една банка откриле дека хакерите непречено, повеќе од две години, пренасочувале мали парични средства на нивните сметки. Кога тоа се открило се информирани другите финансиски и банкарски институции, и надлежните органи утврдиле дека станува збор за хакерска група од Русија, при што се оштетени повеќе од стотина финансиски и банкарски институции, со вкупна вредност од над 650 милиони фунти. Хакирањето е сериозен проблем, бидејќи последиците можат да бидат големи.³¹

4. Темна мрежа (Dark Web)

Постојат и делови од *Deep/Invisible Web* кои се достапни само преку специјализиран софтвер односно пребарувач, а ова е најчесто познато како *Dark Web*, или *Dark Net*. *Dark Web* најдобро може да се опише како „недоволно сеено“ на интернет. Тука може да се најдат сомнителни зделки и незаконитости, но исто така ваквите специјализирани софтвери стануваат рај за новинарите и свиркачите, како што е Едвард Сноуден. Според експертите за безбедност, Едвард Сноуден го користел пребарувачот Tor за да испрати информации на програмата за надзор PRISM на Вашингтон пост и на Гардијан во јуни, 2013 година.³²

Како да стигнам до Dark Web?

За да ја посетите „темната мрежа“, корисниците мора да инсталираат специјален софтвер, односно прелистувач што ги анонимизира нивните мрежни врски. Најпопуларниот прелистувач е наречен *Tor*.³³ „*Tor* е слободен софтвер и отворена мрежа која ви помага да се одбраните од анализата на сообраќајот, односно форма на мрежен надзор кој ја загрозува личната слобода и приватноста, доверливите деловни активности

³⁰ Petrović, R. S., *Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd 2000, 180.

³¹ <http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worldsbiggestbank-raid.html> на 14.04.20 на 17:00 часот.

³² Prlja, D., Reljanović, M., Ivanović, Z., *Krivična dela visokotehnološkog kriminala*, Beograd 2011, 111.

³³ Petrović R. S., *Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd 2000, 112.

и односи и државната безбедност".³⁴ Откако ќе ја преземете и инсталирате *Tor*, вашата анонимност на прелистување е безбедна, што е од клучно значење за посета на кој било дел од *Dark Web*.³⁵ Поради анонимноста на пребарувачот, вашето користење на „темната мрежа“ е целосно анонимно и невоможно е да се следи, односно многу луѓе го користат за да се вклучат во активности кои се полу-легални, или нелегални. Овде се вообичаени дрогата, оружјето и порнографијата.

Датотеките може да се шифрираат, а сертификатот може да се користи и како сад за држење на копчињата за декрипција на информациите. „Ако повеќе не можеме да ја заштитиме нашата приватност од разузнавачките агенции, „длабоката мрежа“ е сосема поинаква од ова.“ Како Едвард Сноуден ги заштитил неговите информации и неговиот живот? Ако некогаш сте слушнале за компјутерски криминал, веројатно ќе знаете дека денес сајбер-криминалците се повеќе од пари. Тие се буквално нешто со голема вредност, односното истите претставуваат информации за кредитни картички, лични информации, и многу повеќе.³⁶ Сите овие работи се предмет на трговија на „темната мрежа“, која треба да се купи, продаде, или да се препродава.³⁷ Освен тоа, постојат и деловни зделки што се нелегални и што не можат да се спроведат на површината. Речиси сè може да се купи на „темната мрежа“, за одредена цена. Достапните предмети може да вклучуваат огнено оружје, нелегални дроги, нелегални диви животни, па дури и изнајмување на убиец!³⁸ Конечно, има и личности коишто се занимаваат со најслаби и најизненадувачки видови на порнографија, што е нелегално во речиси секој дел од светот.³⁹

³⁴ <https://www.smartportal.mk/novosti/veb/temna-mreza/> на 14.04.20 на 17:00 часот.

³⁵ Ivanović, Z., Prlja, D., Reljanović, M., Krivična dela visokotehnološkog kriminala, Beograd, 115.

³⁶ <https://mk.eyewated.com/%D1%88%D1%82%D0%BE%D0%B5%D1%82%D0%B5%D0%BC%D0%BD%D0%B0%D1%82%D0%B0-%D0%BC%D1%80%D0%B5%D0%B6%D0%B0/> на 25.04.20 г во 17:30 часот.

³⁷ <http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html> на 14.04.20 на 17:00 часот.

³⁸ <https://forum.it.mk/threads/piratite-ja-chinat-domashnata-ikt-industrija-14-milioni-dolari.10278/> на 20.04.20 на 17:00 часот.

³⁹ <https://www.webhostingsecretrevealed.net/mk/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/> на 25.04.20 г во 17:00 часот.

4.1 Виртуелна приватна мрежа (VPN)

Виртуелна приватна мрежа е сметачка мрежа којашто ја користи јавната телекомуникациска инфраструктура, како што е интернет пристапот за оддалечени канцеларии или поединечни корисници, со цел осигурување на сигурен пристап кон мрежата на нивната организација. Таа има за задача да избегне скап систем на сопственост, или изнајмени линии кои може да се користат од страна на само една организација.⁴⁰

Концизира трансфер на податоци помеѓу два или повеќе мрежни уреди кои не се на иста приватна мрежа, за да се задржи пренесувањето на податоци од други уреди на една или повеќе интервенции на локалната мрежа, т.е. Wide Area Network. Постојат многу различни класификации и имплементации кои се користат за виртуелни приватни мрежи.⁴¹

До крајот на 1990-тите години мрежните компјутери биле поврзани преку скапи изнајмени линии и/или dial-up телефонски линии. Виртуелните приватни мрежи ги намалуваат трошоците на мрежата, за да се избегне потребата од многу изнајмени линии кои поединечно се поврзани на интернет.⁴²

Корисниците можат да разменуваат приватни податоци безбедно, така што поскапите изнајмени линии се непотребни.⁴³

VNP технологиите имаат огромен број на протоколи, терминологи и маркетинг влијанија кои ги дефинираат.⁴⁴

На пример, VNP технологиите можат да се разликуваат во:⁴⁵

⁴⁰ <https://www.it.mk/vpn-shto-e-kako-funktsionira-i-kako-mozhe-da-go-koristite/> на 17.04.20 на 17:50 часот.

⁴¹ https://mk.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B5%D0%BB%D0%BD%D0%B0_%D0%BF%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%BD%D0%B0_%D0%BC%D1%80%D0%B5%D0%B6%D0%B0 на 14.04.20 на 18:00 часот.

⁴² Зврлевски., М., Прирачник за компјутерски криминал, Скопје, 115.

⁴³ Активности за превенција и справување со последици од сајбер тероризам. Министерство за информатичко општество <http://www.mio.gov.mk/?q=node/1911> на 14.04.20 на 17:00 часот.

⁴⁴ Интегралниот текст на одредбите од Кривичниот Законик кои се однесуваат на компјутерски криминал на 14.04.20 на 17:00 часот.

1. Протоколите што ги користат за да се пробијат во сообраќајот;
2. Тунелот е крајната точка, односно клиент раб, или оператор раб;
3. Дали тие нудат сајт - на сајт, или имаат далечински пристап на поврзување;
4. Нивото на безбедност што е предвидено.

Безбедната VPN користи криптографски протоколи на пристап за да обезбеди доверливост, овозможувајќи му на испраќачот проверка за блокирање на лажен идентитет и интегритет на порака.⁴⁶

Безбедните VPN протоколи го вклучуваат следново:⁴⁷

1. IPsec (Internet Protocol Security), којшто првично беше развиен за IPv6. Овој стандард се користи и за IPv4.⁴⁸
2. Безбедносниот пренос може да пристапи до сообраќајот на целата мрежа, како што тоа го прави во проектот OpenVPN, или да обезбеди индивидуална врска. Голем број на производители обезбедуваат далечински пристап (VPN) преку SSL способности. На SSL VPN може да се поврзе и од локации каде што IPsec има проблеми со мрежната адреса и со firewall правилата.⁴⁹
3. Безбедната школка (SSH) VPN нуди VPN пристапи за безбедни далечински врски до мрежните, или интер-мрежните линкови. Ова не треба да се меша со порт пренасочување.⁵⁰

⁴⁵ Legal Aspects of Computer-related Crime in the Information Society – COMCRIME study, <http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf> на 14.04.20 на 17:00 часот.

⁴⁶ CASX – податоци што се наоѓаат во активната меморија на компјутерот, 25.

⁴⁷ Directive on electronic commerce <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF> на 14.04.20 на 17:00 часот.

⁴⁸ Интегралниот текст на одредбите од Кривичниот Законик кои се однесуваат на компјутерски криминал, 116

⁴⁹ Зврлевски., М., Прирачник за компјутерски криминал, Скопје 2014, 365.

⁵⁰ Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, <http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf> на 14.04.20 на 17:00 часот.

ГЛАВА ВТОРА

2. Кривични дела од областа на компјутерскиот криминал опфатени во кривичниот законик

Голем временски период бил потребен за да се воспостават дефинициите за компјутерски криминал во текот на неговите зачетоци, но додека процесот на дефинирање се развивал, во исто време се појавува нов феномен - сајбер криминалот.⁵¹

Обидите за разјаснување на размерите на овој криминал и неговата опасност во документот „Криминал во спрега со компјутерски мрежи“ (engl. crime related to computer networks) од десетиот конгрес на Обединетите Нации посветен на превенцијата од криминал и третирањето на сторителите од април 2000-та година. Експертската работна група под терминот *сајбер криминал* подразбира „криминал кој се однесува на било кој облик на криминал што може да се изврши со компјутерски системи и мрежи, во компјутерски системи и мрежи, или против компјутерски системи и мрежи“.⁵²

Тоа е криминал којшто во суштина се одвива во електронска околина.⁵³ Под компјутерски систем се подразбира „секој уред, или група меѓусебно поврзани уреди со кои се врши автоматска обработка на податоци (или било која друга функција)“, како што е дефинирано во Конвенцијата за сајбер криминал (engl. Convention on Cyber crime), Совет на Европа, тогаш е јасно дека без електронска околина нема да постои ваков тип на криминал.⁵⁴

⁵¹ Според Американска комисија за заштита на критичната инфраструктура (http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci771061,00.html) на 14.04.20 на 17:00 часот.

⁵² (“ Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding ...”) . на 14.04.20 на 19:00 часот.

⁵³ „некој кој се обидува да се пробие во компјутерскиот систем“. (http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci212220,00.html) на 14.04.20 на 19:00 часот.

⁵⁴ Според Федералното биро за истрага – ФБИ (http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci771061,00.html) на 14.04.20 на 19:00 часот.

2.1 Загрозување на сигурноста по пат на информатички системи

Објектот на заштита е психичкиот мир на човекот и неговото спокојство, како претпоставка за другите негови слободи. Човекот се чувствува слободен само тогаш кога не стравува за својата егзистенција и кога не му се заканува опасност, односно кога е безбеден.

Есенцијата на неправото на ова дело се состои токму во исфрлањето на човекот од состојбата на психички мир и неговото доведување до чувство на неспокојство и страв. Супституирање на споменатите чувства со спротивни чувства на несигурност кое доведува до дострел на користење на личните слободи. Од друга страна, ова дело по својата слобода е и „деликт – пречка“ по однос на други потешки упади во основните права на човекот.

Делото се состои во загрозување на сигурноста на некое лице со сериозна закана дека ќе се нападне врз неговиот живот или тело, или пак животот или телото на негово блиско лице. Дејствие на извршување е заканата насочена кон загрозување на сигурноста на друг. Ефектот на закана се состои во создавање чувство на загрозеност, несигурност и страв. Тука, заканата не е средство за влијание врз слободата на одлучување, и треба да биде објективно подобна за да предизвика чувство на загрозеност и страв кај пасивниот субјект. Оваа одредба ја заштитува пречувствителноста и страшливоста што е поголема од просечната, така што подобноста на заканата може да предизвика чувство кое треба да се оценува пеку објективен критериум, т.е. со уважување на сите конкретни околности на случајот. Делото постои и кога сторителот нема намера да ја оствари својата закана.

Нашата судска практика вели дека постои загрозување секогаш кога сторителот има во раце оружје, опасно орудие, или друго средство што е подобно за да се реализира злото со кое се заканува.

Пасивен субјект е лице што е способно да ја оцени сериозноста на заканата кај кој може да биде создадено чувство на несигурност, меѓутоа потребно е да се земат во

предвид и некои објективни критериуми за ситуациите кога пасивниот субјект нема свест за сопствената сигурност.

Според некое објективно стојалиште би требало да се земе во предвид дека постои загрозување на сигурноста ако самото дејствие е подобно кога кај еден просечно плашлив човек ќе предизвика чувство на несигурност и загрозување на спокојството. Едно субјективно битие кај кое загрозувањето на сигурноста е умислена, сторителот неможе да оди подалеку од загрозување на сигурноста.

Доколку дејството на сторителот е субјективно насочено кон повреда, или лишување од животот на пасивниот субјект, тогаш би се работело за обид за тешка телесна повреда или пак убиство. Гонењето се презема по приватна тужба (ст. 5) поради посебната природа на делото за чие постоење во прв ред е релевантното чувство на загрозеност.

Оваа инкриминација има три квалификациски облици: првиот облик е кога делото е сторено при вршење на семејно насилство, вториот облик е насочен кон службено лице, или повеќе лица, и третиот облик е кога заканата е извршена преку информатички систем.

Потешкиот облик на делото претпоставува постоење на свест кај сторителот дека ја загрозува сигурноста на службено лице во вршење на службата, или на повеќе лица. Во првиот случај свеста за таквото нормативно обележје на законското битие треба да го опфати социјалното значење на поимите „службено лице“ и „вршење на службата“, но не и нивното законски определено значење.

Битието на потешкиот облик на закана по пат на информатички систем ги содржи следниве посебни елементи кои го разликуваат од основното дело: закана по пат на информатички систем, закана со сторување на потешко казнено дело, и мотивираност на таквата закана со односот на припадноста на жртвата кон определена национална, етничка и расна група, или верска определба.

Казната за основниот облик на ова дело е парична, или затвор до шест месеци. За другите облици е од три месеци до три години, и од една до пет години.

Загрозувањето на сигурноста по пат на информатички системи ги опфаќа следниве дејства:

1. Тој што ќе ја загрози сигурноста на друг со сериозна закана дека ќе нападне врз неговиот живот или тело, или животот или телото на нему блиско лице, ќе се казни со парична казна, или со затвор до шест месеци.
2. Тој што ќе го стори делото од став 1 при вршење семејно насилство, ќе се казни со затвор од три месеци до три години.
3. Со казната од став 2 ќе се казни тој што делото од став 1 ќе го стори кон службено лице во вршењето на службата или спрема повеќе лица.
4. Тој што по пат на информатички систем ќе се закана дека ќе стори кривично дело за кое е пропишана казна затвор од пет години или потешка казна против некое лице поради неговата припадност кон определена национална, етничка или расна група или верска определба, ќе се казни со казна затвор од една до пет години.
5. Гонењето за делото од став 1 се презема по приватна тужба.⁵⁵

Карактеристики на загрозување на сигурноста по пат на информатички систем:

1. Сторителот и жртвата најчесто се познаваат доволно.
2. Сторителот по пат на информатички систем, или сет апликации и се заканува на жртвата дека ќе стори кривично дело кое е казниво со затвор повеќе од 5 години.
3. Многу сторители не се свесни за тоа кривично дело, и најчесто го прават од невнимание, особено кога коментираат на објави на социјалните мрежи против етничка припадност, јазик, државјанство и религија.
4. Сторителите се закануваат дека ќе сторат кривично дело кое е казниво со казна затвор од пет години, и повеќе.

⁵⁵ Член 144 „Загрозување на сигурност“ <https://www.wipo.int/edocs/lexdocs/laws/mk/mk/mk018mk.pdf> на 14.04.20 на 17:00 часот.

2.2 Злоупотреба на лични податоци

Социјалниот и технолошкиот напредок е поврзан со потребите на државниот апарат за зголемување на безбедноста и контрола на поединецот. До појавата на интернетот, мобилната телефонија и социјалните мрежи, следењето на поединци претставувало физичка работа, односно следење од место до место, интервјуирање и набљудување. Се проценува дека тајната полиција на Источна Германија соработувала со над 500.000 соработници – информатори, односно добавувачи, а имала 10.000 вработени само на контролната преписка на граѓаните, и прислушување на истите.⁵⁶

Информатичката технологија овозможува складирање на огромни количини на податоци за поединци. Податоците се собираат и складираат во електронски бази на податоци, кои подоцна овозможуваат брза обработка и пребарување. Развиените земји водат во користењето и развојот на технологии за широка контрола на населението, и надзор. Утврдено е дека сајтови од 64-тата Федерална агенција на САД неовластено земале податоци од лица, кои потоа ги користеле и вршеле контрола на нивната историја на прелистување на интернет. Безбедносните служби на државата под изговор на безбедност, секојдневно ја нарушуваат приватноста на е-поштата на граѓаните. САД отишле најдалеку по тоа прашање за нарушување на приватноста од страна на Националната агенција за безбедност на САД (НСА).⁵⁷

Благодарение на специјализиран софтвер кој што ги пребарува сите пораки кои биле испратени од САД во странски земји, и сите пораки кои се испраќаат во САД од странство, при што како критериум на пребарување клучни зборови се: бомба, оружје, напад, итн., се пребаруваат и се наоѓаат податоци, а сите пораки се чуваат во случај на некоја понатамошна обработка или потреба.

Со подобрување на софтверските решенија се прави инвазија на приватноста на граѓаните, иако масовната употреба на социјалните мрежи тоа значително го олеснува

⁵⁶ <http://www.britannica.com/topic/Stasi> на 14.04.20 на 17:00 часот.

⁵⁷ <http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email> на 14.04.20 на 17:00 часот.

(сродство, телефонски броеви, итн.), и истите можат да бидат злоупотребени од страна на хакерите.

Луѓето, не размислувајќи, ги оставаат речиси сите нивни информации на социјалните мрежи (име, презиме, датум и место на раѓање, податоци за вработување, семејство, сродство, телефонски број, фотографии од сопствените домови, слики од семејството и пријателите, политички ставови итн.), а истите подоцна можат да бидат злоупотребени од страна на хакерите. Злоупотребата на лични податоци ги опфаќа следниве дејствија од Кривичниот законик според член 149:⁵⁸

1. Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.
2. Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера, користејќи ги за себе или за друг да оствари некаква корист, или на друг да му нанесе некаква штета.
3. Ако делото од ставовите 1 и 2 го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години.
4. Обидот е казнив.
5. Ако делото од овој член го стори правно лице, ќе се казни со парична казна.⁵⁹

⁵⁸ Пречистениот текст ги содржи следните измени и дополнувања на законот објавени во „Службен весник на Република Македонија“ број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11, 185/11, број 142/12, број 166/12, број 55/13, број 82/13, број 14/14, број 27/14, број 28/14, број 115/14 и број 132/14. на 14.04.20 на 17:00 часот.

⁵⁹ Член 149 „ Злоупотреба на лични податоци“ <https://www.pravdiko.mk/wpcontent/uploads/2013/11/Krivichen-zakonik-integralen-prechisten-tekst.pdf> на 14.04.20 на 17:00 часот.

2.3 Спречување на пристап кон јавен информатички систем

Објект на заштита - кај оваа инкриминација примарно е правото на слободен пристап кон информациите и слободата на примање и на пренесување информации, загарантирано со УРМ. Јавните информатички системи се јавен сервис за сите граѓани, што подразбира нивна обврска да овозможат пристап во користење на информациите со кои располагаат, и пристап за пласирање на информации со кои располагаат граѓаните.

Делото го врши лице што неовластено спречува или ограничува друг во пристапот кон јавен информатички систем.

Како дејствие на извршување на делото неовластено *спречување или ограничување* се подразбира преземање на различни умислени дејствија кои имаат последица од која поединецот не може, или огранично може да користи или да дава информации. Како посебен елемент на дејствието се подразбира постапувањето спротивно на законите во областа на јавното информирање, и во нив определените исклучоци од правото на слободен пристап. Статусот на извршителот како службено или одговорно лице во правното лице е квалификаторна околност. Правното лице одговара за ова дело под општите законски услови за негова одговорност. Поради субјективниот карактер на објектот за заштита поврзан со индивидуалното чувство на повреда на правото, гонењето се презема по приватна тужба.

Спречувањето на пристап кон јавен информатички систем ги опфаќа следниве дејствија од Кривичниот законик според член 149-а:

1. Тој што неовластено спречува или ограничува друг во пристапот кон јавен информатички систем, ќе се казни со парична казна или со затвор до една година.
2. Ако делото од став 1 го стори службено лице во вршење на службата, или одговорно лице во јавен информатички систем, ќе се казни со парична казна или со затвор од три месеци до три години.
3. Ако делото од овој член го стори правно лице, ќе се казни со парична казна.
4. Гонењето се презема по приватна тужба.

Оваа може да се прикаже со примерот кога Стојанче Ангелов го тужеше поранешниот главен јавен обвинител Марко Зврлевски за злоупотреба на службената положба и овластување, и спречување на пристап кон јавен информациски систем.

Во продолжение ќе го презентираме примерот со лидерот на Достоинство, Стојанче Ангелов:

Лидерот на Достоинство, Стојанче Ангелов, во четврток, поднесе кривична пријава против јавниот обвинител Марко Зврлевски за злоупотреба на службената положба и овластување, и спречување на пристап кон јавен информациски систем.

Пријавата против Зврлевски следува по соопштението на Обвинителството, кое забрани емитување на т.н. *бомби на опозицијата*.⁶⁰

Ангелов вели дека е свесен дека оваа пријава нема никој да ја процесуира, но таа ќе остане во Обвинителството, а кога на чело на Обвинителството ќе дојде легитимен обвинител, тогаш Зврлевски ќе мора да каже зошто го издал тоа соопштение.

Ангелов повеќе денови пред зградата на МРТВ се обидува да го натера уредништвото на јавниот телевизиски сервис да ги објавува `бомбите` на опозицијата, а од таму му одговорија дека не го прават тоа, затоа што обвинителството забранило објавување на материјали кои се можни докази во судски процес.

2.4 Повреда на авторско право и сродни права

Објект на заштита на ова дело се уставно загарантираните права што произлегуваат од научното, уметничкото, или друг вид интелектуално творештво (УРМ,47). Овие права се поблиску уредени со Законот за авторското право и сродните права⁶¹.

Дејствие на неовластено извршување е кога во свое име или во име на друг се врши објавување, прикажување, репродуцирање, дистрибуирање, изведување,

⁶⁰ Makfax.com.mk <https://makfax.com.mk/makedonija/stojance-angelov-so-krivicna-protiv-zvrlevski/> 06.04.20 во 10:00 часот

⁶¹ Пречистен текст од 2005 г,Сл.Весник на РМ,бр.4/05,115/10 и 51/11 на 14.04.20 на 17:00 часот

емитување, или на друг начин неовластеното посегание по туѓо авторско право, или сродно право.

Сите поими кои влегуваат во составот на Законското битие на делото имаат правно значење. Авторското дело е индивидуална интелектуална творба од областа на книжевноста, науката, уметноста и од други области на творештвото, независно од видот, начинот и формата на изразување. Како авторско дело не се сметаат прописи и службени материјали на државни органи и институции кои вршат јавни овластувања, како и поднесоци и одлуки во судската и управната пракса. Поимот на сродни права кои се преносливи опфаќаат интелектуални творби како изведби, емисии, фонограми и видеограми. Одредбава разликува неколку потешки облици во зависност од начинот на извршувањето и прибавената корист, која инаку не е конститутивен елемент на основното дело: сторување на делото преку компјутерски систем, и прибавување поголема имотна корист.⁶² Поради опасноста на самото започнување со извршување на делото се казнува и самиот обид, или самата помисла да се направи нешто. Предвидено е и задолжително одземање на предметите на делото. За одговорност на правното лице е потребно исполнување на општите законски услови.⁶³

Гонењето за повреда на моралното право се превзема по предлог, а под морално право се подразбира правото на авторот да одлучува за објавување на делото, признавање на авторство над делото, соочување на целината на делото (забрана на плагијат) итн.⁶⁴

Со овој закон се уредуваат правото на авторите над своите авторски дела (во натамошниот текст: авторското право, правата на уметниците - изведувачи, на произведувачите на фонограми, на произведувачите на видеограми (филмски продуценти), на радио-телевизиските организации, на издавачите, и на изготвувачите на бази на податоци над своите предмети на сродни права (во натамошниот текст: сродните

⁶² Член 122 од Кривичниот законик на страна 2,3 и 4.

⁶³ Член 28-а од Кривичниот законик страна 5,6 и 8.

⁶⁴ Казнено право – посебен дел Владо Камбовски, Никола Тупанчески Скопје 2011, 171.

права), остварувањето и заштитата на авторското право и сродните права, и важењето на законот.

Остварувањето и заштитата на сродните права, според овој закон, не го повредува, и на ниеден начин не влијае на остварувањето и заштитата на авторското право.

Авторското право и сродните права уживаат кривична, граѓанска, и прекршочна заштита согласно прописите кои ја уредуваат правната материја за која се бара заштита (кривична, граѓанска или прекршочна). Заштитата на авторското право и сродните права ја вклучува и заштитата на технолошките мерки од повреда на правата.

Согласно Законот за авторското право и сродните права, лица кои имаат право на заштита се авторот, носителот на право, лице овластено да го користи правото, и организацијата (носители на право).⁶⁵

Лице чие право е повредено, кога постои оправдано сомневање дека ќе му биде повредено правото, и кога се заканува вистинска закана од повреда на правата, има право да поднесе барање за:

1. заштита на правото, и
2. времени и други мерки.

Постапката по тужбените барања е итна.

Кога некое право определено со овој закон е повредено, секој од носителите на тоа право може од трето лице да побара заштита на правото како да е единствен носител.

Кога лицето кое го повредило правото ќе ги исполни барањата на еден од носителите на истото право, неговата обврска престанува и кон другите носители на правото.

⁶⁵ Член 157 од Кривичниот законик на 14.04.20 на 17:00 часот.

Доколку се работи за судска постапка која е во тек, носителите на истото право се сметаат за единствени сопарничари. Кога постојат повеќе сторители на повредата на некое право од овој Закон, секој од нив солидарно одговара за повредата.⁶⁶

Содржина на заштитата на правото.⁶⁷

Правото на заштита ги содржи следниве барања за:

1. престанок на дејствието на повреда;
2. надоместок на материјалната штета;
3. надоместок на нематеријалната штета;
4. зголемен надоместок;
5. означување на авторот;
6. враќање на користа стекната од недозволеното користење;
7. отстранување од промет на предметите од повредата на правото и
8. објавување судската пресуда.

Материјална штета

Доколку со повреда на право од овој закон е сторена материјална штета, лицето има право да побара надоместок за сторената материјална штета и за загубена добивка. Надоместокот се определува во износ што тужениот би го платил доколку побарал законско користење на правото (вообичаен надоместок), односно во износ пропишан со соодветни тарифи, односно со општ договор.⁶⁸

Нематеријална штета

При повреда на морално право, независно од изречениот зголемен надоместок при непостоење материјална штета, судот може да пресуди на авторот да му се исплати

⁶⁶ Боцевски, Д., Советување за сајбер криминал – Компјутерски инциденти и истражување на компјутерски криминал 175.

⁶⁷ Ачкоски, Ј., Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012, 199.

⁶⁸ Надица Мирчевска, научен труд Сајбер тероризам – современ облик на тероризмот колку Република Македонија е ранлива од сајбер тероризам, 155.

праведна парична оштета за претрпена душевна болка и страдање, како последица од повредата на моралното право, доколку утврди дека околностите на случајот, и особено степенот на повредата и нејзиното траење тоа го предизвикале.⁶⁹ Доколку правото е повредено со намера или крајна небрежност, лицето може да побара исплата на договорениот или вообичаениот надоместок за тој вид користење, зголемен до 200%, независно дали од повредата претрпел имотна штета (граѓанска казна).⁷⁰

При одлучувањето по барањето за плаќање на овој надоместок и одмерувањето на нејзината висина, судот ќе ги има предвид сите околности на случајот, особено степенот на вината на тужениот, износот на договорот или вообичаениот надоместок.⁷¹

2.5 Покажување на порнографски материјал на дете

Предмет на заштита на ова незаконско однесување е достоинството на личноста, и целосната слобода.⁷²

Малолетниците и децата се посебни заштитени групи, па заради тоа органите на следење големо внимание им посветуваат на содржините на интернет кои содржат експлицитни сексуални сцени со деца и малолетници.⁷³

Во суштина, тоа е кривично дело во законодавството, а постојат четири негови облици, и тоа:⁷⁴

1. производство на детски порнографски материјал,
2. негова продажба,

⁶⁹ Cyber terrorism: The World's First Internet War?: Stefan Nicola; August 8, 2007 (<http://www.govtech.com/dc/articles/12966>) на 14.04.20 на 17:00 часот.

⁷⁰ ЗАКОН ЗА АВТОРСКОТО ПРАВО И СРОДНИТЕ ПРАВА Сл. Весник на Р. Македонија, бр.115 од 31.08.2010 година <https://www.wipo.int/edocs/lexdocs/laws/mk/mk/mk015mk.pdf> на 14.04.20 на 17:00 часот.

⁷¹ <https://www.pravdiko.mk/pravo-na-sudska-zashtita-na-avtorskoto-pravo-i-srodnite-prava/> на 17.04.20 г во 17:00 часот

⁷² Davidson T., Sooryamoorthy R., Shrum W., Kerala Connections: Will the Internet Affect Science in Developing Areas?, 2002, <http://worldsci.net/EVERY4.pdf> ; Finholt A. T., Collaboratories: Science over the Internet, 2002, <http://www.aaas.org/spp/yearbook/2002/ch31.pdf> ; Guice J., Duffy R., The Future of the Internet in Science, USRA Research Institute for Advanced Computer Science, NASA Ames Research Center, USA, <http://ase.arc.nasa.gov/publications/pdf/2000-0174.pdf> на 20.04.20 на 17:00 часот.

⁷³ Internet Ad Revenues Continued to Grow in the Fourth Quarter, ClickZ News, March 1, 2006, <http://www.clickz.com/news/print.php/3588506>.

⁷⁴ Hakman K., E-Commerce Tutorial, <http://www.webmonkey.com/webmonkey/99/04/index0a.html> на 20.04.20 на 17:00 часот.

3. растурање, и
4. ставање на располагање.

Поради фактот дека порнографските материјали тешко го повредуваат моралот, и дека има постојана работа од надлежните органи и борбата за нивно уништување, несфатливо е дека пазарот на порнографски материјали постојано се шири.⁷⁵

Компјутерската технологија направила клучен придонес за тоа. Благодарение на интернетот, порнографијата е достапна во целиот свет во различни форми, како што се: слики, видеа, текстови, анимации и слично.⁷⁶

Со масовното ширење на употребата на интернетот, доаѓа до ширење на порнографски сајтови чијашто употреба е секојдневна дури и во земји како што се Саудиска Арабија, Кина и Турција, кои според денешните стандарди се сметаат за конзервативни земји.⁷⁷ Трговијата со сексуално-експлицитна содржина е еден од најраспространетите и најкористените онлајн активности.

Незаконските облици на порнографија (таму каде се употребуваат деца) стануваат сè повеќе распространети, особено во Азија,⁷⁸ а најмногу во земјите во Индокина, каде што поединци, и педофили желни за заработка, сексуално експлоатираат деца.

Децата најчесто се измамани и заблудени со нудење на големи суми на пари за да позираат голи, иако чести се случаите во кои родителите за пари ги продаваат децата на педофили. Таквите слики или видеа на специјални сајтови, или преку е-пошта, се шират понатаму. Дека педофилските мрежи и сајтови претставуваат закана која треба да се

⁷⁵ Recommendations for Research and Development in Information Technology in Education, Learning and Leading with Technology 2000-2001, ISTE (the International Society for Technology in Education, <http://www.iste.org/> на 21.04.20 на 17:00 часот.

⁷⁶ The Future of Information Technology in Education, 25.

⁷⁷ The Future of Information Technology in Education, An ISTE Publication, <http://www.uoregon.edu/~moursund/FuturesBook1997/index.html> на 14.04.20 на 17:00 часот.

⁷⁸ Advocat J., Internet clinical trials: examining new disciplinary experiments in health care, Monash University, Australia, Anthropology Matters Journal 2005, Vol 7 (1), <http://www.anthropologymatters.com>; Robinson C. J., Financing The Health Care Internet, Health Affairs ~ Volume 19, Number 6, 2000, <http://content.healthaffairs.org/cgi/reprint/19/6/72.pdf>; Warren M., The Internet and rural communities: implications for health care?, [http://www.plymouth.ac.uk/files/extranet/docs/HSC/abstract 2003 - Feb 13 health of rural communities.pdf](http://www.plymouth.ac.uk/files/extranet/docs/HSC/abstract%202003%20-%20Feb%2013%20health%20of%20rural%20communities.pdf) на 14.04.20 на 17:00 часот.

отстрани беше констатирано на неколку Меѓународни конференции. Интернетот има влијание врз ширењето и пазарот на детска порнографија.⁷⁹

Најчесто станува збор за поседување, но, исто така, и за ширење на материјали на кои се деца и малолетни лица. Овие кривични дела се многу специфични бидејќи со извршување на казнени дела од областа на сексуална злоупотреба и експлоатација на деца, се вршат тешки прекршувања на основните човекови права и слободи.⁸⁰

Трајно се нарушува развојот на личноста жртва заради примената на психолошко насилство како главен метод на работа. Жртвите во повеќето случаи се целосно беспомошни, и затоа лесно се предмет на различни форми на психички манипулации.

Во почетокот, полицијата и надлежните органи многу лесно ги откривале сторителите, меѓутоа денес ширењето на овој вид на порнографија се прави преку заштитени сајтови, и испраќање на шифрирани пораки.

Ова е така затоа што приходот од детска порнографија е огромен. Како сторители се појавуваат и други криминалци, а не само педофили, така што нивото на организираност се подига на повисоко ниво, а групата на луѓе на кои порнографските содржини им се достапни, се сè од позатворен тип.⁸¹ Постојат софтвери за цензура и блокирање на одредени содржини.

Софтверот за блокирање работи со:⁸²

1. Листа на сајтови за исклучување;
2. Клучен збор за блокирање од името на сајтот или страната;⁸³
3. Блокирање според клучен збор од содржината;
4. Блокирање на пренесени податоци.

⁷⁹ Đurčić, V., Jovašević, D., Krivično pravo: posebni deo, Niš, 2013, 79.

⁸⁰ Prlja, D., Reljanović, M., Ivanović, Z., Krivična dela visokotehnološkog kriminala, Beograd, 2011, 8.

⁸¹ Cirović, D., Janković, N., Lacević, M., , Cyber podzemlje u Srbiji, Reporter broj od 16.11.2005.godine, 33.

⁸² www.blic.rs/Vesti/Svet/438405/Na-Filipinima-zbog-decje-pornografije-uhapseno-11-ljudi на 14.04.20 на 17:00 часот.

⁸³ Cirović, D., Janković, N., Lacević, M., , Cyber podzemlje u Srbiji, Reporter broj od 16.11.2005.godine, 12.

Софтверот за блокирање може да работи на ниво на апликација, на ниво на протокол (врши контрола на сите мрежни конекции), или на самата мрежна инфраструктура.

Софтверот за блокирање се контролира од крајниот корисник, од сопственикот на компјутерот, од online-провајдерите, или од провајдер за широка мрежа.⁸⁴

Недостатоци на софтверот за блокирање се:

1. потреба од ажурирање на листите на забранети сајтови;
2. грешки на софтверот за блокирање - преширокост.

Како заштита на децата од недолични содржини, постои опција од оперативниот систем Windows од XP, CIPRA, за да се означат страните, и родителите да го поднесат профилот на детето за да го заштитат од насилни и порнографски содржини.

Исто така, постојат голем број на софтвери за филтрирање на податоци кои родителите можат да ги користат.

Некои од нив се:⁸⁵

Email For Kids - Родителите можат да ја уредуваат содржината на излезните/дојдовните пораки, записите во адресарот и времето на интернет. Ги спречува личните прикажувања, контролира испратени пораки, и регулира кој комуницира со децата;

Net Nanny 3.1 - Блокира непристојни сајтови, фрази, лични прикажувања, разговорници, gifs и jregs. Ги следи излезната/дојдовна е-пошта и други текстуални документи. Пријавува прекршоци, прилагодено уредување, единствени кориснички и мрежни верзии;

⁸⁴ <https://mk.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%81%D0%BA%D0%B0%D0%BE%D0%BF%D1%80%D0%B5%D0%BC%D0%B0&action=edit> на 21.04.20 на 17:00 часот.

⁸⁵ <http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html> на 24.04.20 на 17:00 часот.

Safe Surf - Функција на прелистувачот на „NetWatch“ на Netscape која користи SafeSurf стандард за рејтинг, и база на податоци за возрасни. Родителите можат да блокираат одредени сајтови и да ги прилагодуваат нивоата на содржини во различни категории, а обезбедува и листа на безбедни локации;⁸⁶

Chi-Brow 2.0 - Поедноставен прегледувач на деца, кој на родителите им дава целосна контрола врз одредувањето на соодветни веб-страници и блокирање на непристојни. Вклучува база на податоци за препорачани сајтови.⁸⁷

Иако на проблемот на детската порнографија не се посветувало доволно внимание во минатото, денес има ситуација во која оваа област е целосно правно регулирана, а кон тоа е насочено големо внимание од надлежните органи, што е потврдено со големиот број на полициски акции.⁸⁸

2.6 Производство и дистрибуција на детска порнографија

UNCRC обезбедува основа за меѓународни правни стандарди за заштита на децата од сексуална експлоатација. Член 34,⁸⁹ меѓу другите статии кои забрануваат понижувачки третман на децата, експлицитно бара земјите да преземат „секакви можни соодветни национални, билатерални и мултилатерални мерки за спречување на... наведување или принуда на детето да учествува во било каква незаконска сексуална активност ... [и] на експлоататорско користење на децата во порнографски претстави и материјали“. Комисијата на Обединетите Нации во Програмата за човекови права во акцијата за спречување на продажба на деца, детска проституција и детска порнографија, ги зајакнува UNCRC и меѓународните напори за санкционирање на оние кои експлоатираат деца за порнографски цели. Многумина имаат тврдено дека дистрибуцијата на непристоен материјал за возрасни е криминал кој не остава жртви, дека никој не останува повреден, и приватноста на одредена личност треба да остане како таква - приватна.

⁸⁶ <https://forum.it.mk/threads/piratite-ja-chinat-domashnata-ikt-industrija-14-milioni-dolari.1027> на 14.04.20 на 17:00 часот.

⁸⁷ <http://www.poslovni.hr/hrvatska/privreda-sad-a-godisnje-gubi-vise-od-200-mlrd-dolara-zbogpiratstva52710>

⁸⁸ www.hackingarticles.in на 11.04.20 на 17:30 часот.

⁸⁹ Член 34 од Кривичниот законик на 19.04.20 на 17:00 часот.

Во случај на детска порнографија, кога одредено дете е снимено или фотографирано, тоа секогаш станува жртва на тој чин. Распределбата на таа претстава ја повторува виктимизацијата одново и одново, долго време откако се има случено.

Исто така, кога лицето на некое дете е поставено на сексуално експлицитни фотографии, дури иако тоа дете нема никогаш учествувало во сексуалниот чин, дистрибуцијата на изменетите слики произведуваат сличен ефект.⁹⁰

Постојат два начини на кои децата потенцијално може да бидат повредени од детската порнографија, или со тоа што се снимени. Децата кои се изложени на порнографија се во опасност да бидат заведени, верувајќи дека порнографската активност е „нормална“ за децата.⁹¹

Влијанието врз детето кое е искористена жртва за да се произведе порнографија е прилично сериозно. Децата можат да доживеат голем број на симптони, вклучувајќи физички симптоми и болести, емоционално повлекување, асоцијално однесување, променливо расположение, депресија, страв и анксиозност. Во една студија на деца кои биле вклучени во секс-кругови и кои биле сексуално злоупотребени, 54,8% од децата биле искористени во создавањето на порнографија.⁹²

Кај овие деца има значителна врска помеѓу вклучувањето во чинот на порнографија и моделот на идентификација со експлоататор, заедно со девијантното и симптоматското однесување.

Децата кои се сексуално злоупотребени или експлоатирани имаат голем ризик да станат сторители, или насилници. Имајте на ум дека постојат и оние кои ја одбиле теоријата „циклус на злоупотреба“, бидејќи жените се оние кои сè почесто сексуално злоупотребени, а сепак мажите се одговорни за поголемиот дел од сексуална злоупотреба на децата во повеќето општества.

⁹⁰ U.S. Senate Report, *supra* note 7, at 44, 113.

⁹¹ EFCW Position Statement, *supra* note 22, at 3, 113.

⁹² Šarkiĉ, N., Prljā, D., Damnjanović, K., Mariĉ, V. , Ćivković, V., Vodinieliĉ, V., Mrviĉ-Petroviĉ, N.: *Pravo informacionih tehnologija*, Beograd, 2011, 115.

Оние учесници кои се фотографирани, можат да преземат драстични мерки од типот на палење на куќата каде што се наоѓаат фотографиите, или крадење на секој вид доказ за нивна експлоатација.⁹³ Медиумите во некои земји често ги заменуваат жртвите со сторителите преку објавување на фотографии од деца кои биле сексуално експлоатирани, и со замаглување на лицата на сторителите.⁹⁴

Оние експлоатирани деца кои уживаат во вниманието, или кои биле сексуално стимулирани, претставуваат срам со нивното учество во порнографскиот чин.⁹⁵

Мора да се нагласи дека без разлика дали малолетниците го прифаќаат чинот на сексуалната експлоатација, профитираат од неа, или уживаат во тоа, тие се секогаш жртви на незаконски, и често деструктивен чин.⁹⁶

2.7 Оштетување и неовластено навлегување во компјутерски систем

Кривичното дело „оштетување и неовластено навлегување во компјутерски систем“ припаѓа на првата подгрупа, односно КД кои извршителите ги извршуваат намерно и свесно, со цел противправно стекнување со имотна корист за себе или за друг, или пак, на друг ќе му нанесе имотна или друг вид на штета.⁹⁷

Карактеристично за извршителите на ова кривично дело е што тие се професионалци во својата област, односно поседуваат знаења и вештини од областа информатичките технологии.⁹⁸

Тоа се луѓе кои имаат искуство во ИТ секторот, познавање на програмски јазици, компјутерски системи, мрежи, и криминогена визија за противправно стекнување на

⁹³ Gillespie, A. A., Cybercrime: Key Issues and Debates Florence, Kentucky (USA), 2015, 200.

⁹⁴ www.ugd.edu.mk_private_UserFiles_biljana.kosturanova_Desktop_Trudovi_Jugoslav_Achkoski_Scientific_Papers_elektronska_verzija_Sajber_kriminal_i_zastita_na_digitalnite_podatoci_vo_kompjuterskite_mrezi, 256.

⁹⁵ <http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html> на 16.04.20 г во 16:00 часот.

⁹⁶ <http://www.usatoday.com/story/news/world/2013/08/14/israel-students-social-media/2651715/> на 16.04.20 г во 16:00 часот.

⁹⁷ Robinson J., Internet as the Scene of Crime, International Computer Crime Conference, Oslo, 2000., www.ccips.org на 20.04.20 на 19:00 часот.

⁹⁸ <http://www.maturiskiradovi.net/forum/Thread-kompjuterski-kriminal-na-17.04.20> г во 17:30 часот

имотна корист или нанесување на штета.⁹⁹ Кривичниот законик терминот компјутерски систем го дефинира како било каков уред, или група на меѓусебно поврзани уреди, од кои еден или повеќе од нив врши автоматска обработка на податоци според одредена програма, а под компјутерски податоци се подразбира презентирање на факти, информации или концепти во облик погоден за обработување преку компјутерски систем, вклучувајќи и програма подобна компјутерскиот систем да го стави во функција.¹⁰⁰ Кривичното дело „оштетување и неовластено навлегување во компјутерски систем“ е систематизирано во глава XXIII - Кривични дела против имотот од Кривичниот законик на Република Македонија.¹⁰¹ Тоа претставува кривично дело каде се опфатени повеќе инкриминации за кои се предвидени различни санкции во зависност од квалификацијата на делото.¹⁰² Структурата на кривичното дело во кривично-правната материја определено во објективно-субјективна смисла ја сочинуваат следните елементи: дејствие, предвиденост во закон, противправност, вина, и казнивост.¹⁰³

Имено, македонскиот законодавец за ова кривично дело ги инкриминира следните дејствија:¹⁰⁴

1. Тој што неовластено ќе избрише, измени, оштети, прикрие, или на друг начин ќе направи неупотреблив компјутерски податок, програма или уред за одржување на информатичкиот систем, или ќе го оневозможи или отежне користењето на компјутерскиот систем, податокот или програмата на компјутерска комуникација, ќе се казни со парична казна или со затвор до три години.¹⁰⁵
2. Со казната од став 1 ќе се казни и тој што неовластено ќе навлезе во туѓ компјутер или систем, со намера за искористување на неговите податоци или програми заради прибавување противправна имотна или друга корист за себе или за друг, или предизвикување имотна или друга штета или заради пренесување на

⁹⁹ <http://www.poslovni.hr/hrvatska/privreda-sad-a-godisnje-gubi-vise-od-200-mlrddolara-zbogpiratstva-52710> на 14.04.20 на 17:00 часот.

¹⁰⁰ Feješ, I., Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti – izlaganje na konferenciji, 2000. 25.

¹⁰¹ Urošević, V., „Nigerijska prevara u Republici Srbiji“, Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Beograd. 17.

¹⁰² Campbell E. D., Computer Terrorism, Syneca Research Group, Inc. Washington USA, 2011 godine str.33

¹⁰³ Hale Ligh, M., Case, A., Levy, J., Walters, A., The art od memories forensics, Wiley, 2014 <http://it-ebooks.info/book/3634/> на 14.04.20 на 17:00 часот.

¹⁰⁴ . Соколоски, Д., МВР и FBI заедно против компјутерски криминал, <http://it.com.mk/mvr-i-fbi-zaedno-protiv-kompjuterski-kriminal-24-uapseni-od-13-drzhavi/>, на 14.04.20 на 17:00 часот.

¹⁰⁵ Кривичен законик, пречистен текст, член 122, ст.26 и ст.27, достапен на: <https://jorm.gov.mk/wp-content/uploads/2016/03/Кривичен-законик-пречистен-текст.pdf>(пристапено 18 декември 2018) на 14.04.20 на 17:00 часот.

компјутерските податоци што не му се наменети и до кои неовластено дошол до неповиканото лице.¹⁰⁶

3. Со казната од ставот (1) на овој член ќе се казни тој што неовластено ќе пресретне, со употреба на технички средства, пренос на компјутерски податоци кои немаат јавен карактер до, од, и внатре, во одреден компјутерски систем, вклучувајќи и електромагнетни емисии од компјутерски систем кој поддржува такви компјутерски податоци.¹⁰⁷
4. Тој што делата од ставовите (1), (2) и (3) на овој член ќе ги стори кон компјутерски систем, податоци или програми што се заштитени со посебни мерки на заштита, или се користат во работењето на државни органи, јавни претпријатија или јавни установи, или во меѓународни комуникации, или како член на група создадена за вршење такви дела, ќе се казни со затвор од една до пет години.¹⁰⁸
5. Ако со делото од ставовите (1), (2) и (3) на овој член е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од шест месеци до пет години.¹⁰⁹
6. Ако со делото од став 3 е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од една до десет години.¹¹⁰
7. Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерска лозинка, код за пристап и сличен податок со кој целината или дел од компјутерскиот систем се оспособува за пристап, компјутерски програми или компјутерски податоци наменети или погодни за извршување на делата од ставовите (1), (2) и (3) на овој член, ќе се казни со парична казна, или со затвор до една година.¹¹¹
8. Обидот за делото од ставовите 1 и 2 е казнив.
9. Ако делото од овој член го стори правно лице, ќе се казни со парична казна.
10. Посебните направи, средства, компјутерски програми или податоци наменети за извршување на делото ќе се одземат.

¹⁰⁶ Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.oun.org, 25.

¹⁰⁷ Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.oun.org, 26

¹⁰⁸ Toren, J. P., Intellectual Property and Computer Crimes (Intellectual Property usiness Crimes Series) , New York USA, 2003, 55.

¹⁰⁹ Petrović R. S., Globalno informaciono ratovanje, Zbornik radova (CD-ROM), YU INFO, 31.

¹¹⁰ Повеќе за штетата во член 142 од Закон за облигациони односи, Сл.весник на Р Македонија бр. 18 од 5.03.2001 г. Штетата е намалувањето на нечиј имот (обична штета) и спречувањето на негово зголемување (испуштена корист), како и нанесувањето на друга физичка или душевна болка или страв (нематеријална штета). на 22.04.20 на 17:00 часот.

¹¹¹ Камбовски, В., Коментар на Кривичниот законик на Република Македонија, - Интегрален текст, Второ изменето издание, Матица, Скопје, 2015, 99.

2.8 Правење и внесување компјутерски вируси

Компјутерските вируси се мали програми, најчесто од неколку килобајти, кои имаат исклучиво за цел да направат штета на заразен компјутер. Се размножуваат воглавно на начини што се „вгнездуваат“ во други фајлови, а штета предизвикуваат така што ги бришат или менуваат фајловите на дискот.

Доколку се работи за информациски системи, вирусот од заразениот компјутер може да зарази друг компјутер во компјутерската мрежа, со цел да измени или оштети фајлови од оперативниот систем на компјутерот.

Оваа форма на компјутерски криминал е неизбежна во сите криминолошки поделби. Основна карактеристика на делото е создавање и дистрибуција на компјутерски програми - вируси, чија единствена цел е да предизвикаат штета на трети страни.¹¹²

Компјутерски вирус е програма која извршува недозволените дејства во системот на корисникот без негово знаење и дозвола.¹¹³

Со цел одредена програма да се смета за компјутерски вирус, таа мора:¹¹⁴

1. сама да се активира и да го внесе својот код на патот за извршување на друга програма.
2. да се реплицира себеси, односно да ги замени другите програми за стартување заразени со копии на вирусни датотеки. Вирусите ова можат да го прават и на персонални компјутери, и на сервери.
3. да има носител, за да може понатаму да се пренесува во контакт со трета страна.

Постојат два облици за извршување на ова дело, каде што прво е создавање на вирусот и е секогаш свесно дејство, додека дистрибуцијата може да биде и несвесно дејство.

¹¹² Prlja, D., Reljanović, M., Ivanović, Z., Krivična dela visokotehnološkog kriminala, Beograd, 2011. 101.

¹¹³ Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd 2000.godina, 44.

¹¹⁴ Ivanović, Z., Prlja, D., Reljanović, M., Krivična dela visokotehnološkog kriminala, Beograd, 2011. 51.

Компјутерските вируси можат да направат различни промени во системите, но најчести се:¹¹⁵

1. промена во големината на програмата;
2. забавување на програмите и системите;
3. погрешно извршување на програмата;¹¹⁶
4. оневозможување на функционирањето на системот и негово онеспособување;
5. промени во програмската датотека;
6. уништување на содржината;
7. копирање на непотребни и штетни програми и информации;
8. намалување на достапниот слободен простор во системот итн.

Постапката Pharming многу често користи вируси и пренасочување на погрешен веб-сајт.¹¹⁷

Вирусите не постоеле сè до средината на осумдесеттите години на минатиот век, а првите вируси биле создадени во Универзитетските центри во САД.

Масовната појава на вируси настапила со проширувањето на компјутерската писменост и употребата на компјутерите и брзиот развој на технологијата. Изработката на вируси благодарение на сè понапредните софтверски решенија е олеснета, така што и лице со просечно информатичко образование може да создаде вирус.

Се верува дека секој компјутер на мрежата дневно е нападат со еден вид на вирус, но програмите за заштита на интернет како Avast, Norton, Kaspersky, ги оневозможуваат, така што овие напади остануваат незабележани.¹¹⁸

¹¹⁵ Интернет страница <http://www.apisgroup.org/sec.html?id=7> 21.04.2020 г во 17:00 часот.

¹¹⁶ Prlja, D., Reljanović, M., Ivanović, Z., Krivična dela visokotehnološkog kriminala, Beograd, 2011. 157.

¹¹⁷ Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd 2000.godina, 185.

¹¹⁸ ICQ (engl. Seek You - „те барам“) е компјутерски програм наменет за размена на текстуални пораки помеѓу неговите корисници, преку користење на Интернет. Првата верзија е излезена во 1996 година, а називот е создаден од играта со англиските зборови. Со текот на времето се појавиле и можности за пренос на фајлови, слики, како и онлајн играње помеѓу корисниците. <http://en.wikipedia.org/wiki/ICQ> на 14.04.20 на 17:00 часот.

Вирусите можат да предизвикаат катастрофални последици, особено на системи од јавен интерес, како што се системи за управување со сообраќајот, осветлување, дистрибуција на електрична енергија, а посебно кај системи во користењето на одбраната и здравството.

Според податоците од антивирусната компанија Norton, најраспространетите вируси на сите времиња се:¹¹⁹

1. MYDOM, кој од 2004 година направил штета од над 38 милијарди долари, а се смета дека се нападнати повеќе од 2 милиони компјутери. Овој вирус е еден вид на црв и се шири преку е-пошта.
2. Sobig.F е еден вид на тројански вирус кој постојано се умножува и на тој начин го нарушува функционирањето на системот. Овој вирус од 2003 година направил штета во износ од над 37 милијарди долари и се смета дека биле нападнати околу 2 милиони компјутери.¹²⁰
3. I LOVE YOU е вирус којшто се шири преку e-mail, и како додаток во меилот има порака со вирус, кој корисниците сами го инсталираат во сопствениот компјутер. Овој вирус од 2000 година нападнал околу половина милион сметки и направил штета од над 15 милијарди долари.
4. CORE RED е црв кој ги напаѓа компјутерите кои користат Windows 2000 или NT. Тој ги напаѓа овие компјутери поради големите недостатоци на овие оперативни системи. Се смета дека од 2001 година, овој тип на вирус нападнал преку милион компјутери, и направил штета од 2,6 милијарди долари.
5. SLAMER или SAFIR е вирус којшто ја забавува работата на мрежата и ги напаѓа провајдерите. Досега нападнал околу 200 илјади компјутери и направил загуба од 1,2 милијарди долари.

За успешна одбрана од компјутерски вируси е потребно да се зголеми нивото на заштита, и едукација на сите корисници заради поуспешна превенција, но исто така, многу важна е употребата на лиценцирана антивирус програма.¹²¹

Заради успешна превенција, неопходно е да се преземат следниве мерки:¹²²

1. блокирање на вообичаените веб-страници на носителот на вирусот;

¹¹⁹ https://mk.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B5%D1%82%D0%B0%D1%87%D0%BA%D0%B8_%D0%B2%D0%B8%D1%80%D1%83%D1%81 на 24.04.2020 година во 17:00 часот.

¹²⁰ http://dimovski-darko.blogspot.com/p/blog-page_4235.html на 24.04.20 на 17:00 часот.

¹²¹ <https://forum.it.mk/threads/shto-se-virusi-kako-rabotat-i-kako-da-se-zashtitite.8623/> на 24.04.20 на 17:00 часот.

¹²² Wells, Joe (1996-08-30). „Virus timeline“. IBM. Архивирано на 24.04.20 на 17:00 часот.

2. блокирање на пошта или датотеки со повеќе наставки од видот doc.jpg.vbs;
3. редовно ажурирање на антивирусни програми;
4. редовно ажурирање на лични и деловни датотеки;
5. непреземање непроверени програми и податоци од инернет;
6. дејство врз секоја неочекувана е-пошта која е сомнителна.¹²³

2.9 Компјутерска Измама

Компјутерските измами се извршуваат со намера за стекнување за себе или за друг протиправна материјална корист, со тоа што кај нив во заблуда не се доведува или одржува некое лице, како што се случаите со обичните измами и како материјалните кривични дела со кои се предизвикува штета, туку заблудата се однесува на компјутер во којшто се внесуваат неточни податоци, или се пропушта внесувањето на точни податоци, или на било кој друг начин компјутерот се користи за остварување на измами во кривично-правна смисла. Компјутерските измами претставуваат најраширен облик на компјутерски криминал.¹²⁴ Бројот на облици на измами, како и начинот на нивната реализација е практично неограничен, и во пракса се среќаваат од примитивни и „груби“, до измами за кои е користен висок степен на вештина и рафинираност.¹²⁵

Но, во шемите за компјутерски измами секогаш се открива некој претходно постар користен облик на измама.¹²⁶

Сите шеми на измами регистрирани на интернет се преработени и прилагодени верзии на шеми со кои некогаш се „ставани“ во заблуда невнимателни и лесноверни жртви.¹²⁷ Компјутерските измами се карактеризираат со многу големо продирање заради големината на интернетот како пазар, бидејќи брзо се шират со интернетот како медиум

¹²³ Kaspersky Lab Virus list на 14.04.20 на 17:00 часот.

¹²⁴

¹²⁵ Ivanović, Z., Prlja, D., Reljanović, M., *Krivična dela visokotehnološkog kriminala*, Beograd, 2011. 168 i 169.

¹²⁶ <http://helpdesk.aek.mk/index.php/vasa-sigurnost/zastita-od-virusi-i-spaiver> на 24.04.20 г во 18:00 часот.

127 Petrović, R S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije: Uredništvo časopisa "Bezbednost" i lista "Policajac"/ Beograd 2000. 155.

со кој сè се случува многу брзо, а исто така и заради ниските трошоци за извршување на ваквиот вид на измами.¹²⁸

На тој начин тие ја користат и предноста на фактот дека измамата преку интернет не бара пристап до некој систем за исплата како за тоа што бара секој друг вид на измама, а исто така и фактот дека дигиталниот пазар е сè уште недоволно уреден, при што се создава одредена конфузија за потрошувачите, што за компјутерските измамници создава идеални услови за компјутерски измами. Постојат и измами со производи со „неверојатни карактеристики“. Голем број на истражувања, како и одржаните семинари за измами со производи со „неверојатни карактеристики“ укажуваат дека една од најголемите нелегални заработки на интернет се измамите со производи со „неверојатни карактеристики“. Врз основа на извештајот од Специјализираните агенции за заштита на купувачите на интернет во Сиднеј, Австралија, секои 44 секунди некој станува жртва на измама бидејќи се одлучува да купи производ со „зачудувачки можности“, запознавајќи го истиот производ преку интернет. Исто така, наведените агенции извршиле истражување на интернет, при што откриле 1400 сомнителни сајтови само во областа на здравството, а како резултат на истражувањето се покренати тужби против 18 компании и детални истраги кои се во тек, а опфаќаат уште 200 фирми во 19 земји широм светот. Колкава штета е предизвикана од нелегална трговија, во извештајот не е наведено, но доколку се знае дека таквите производи, како серијата „Виолетова хармонија“, од каде еден продукт наводно создава ново ниво на енергија во човечкиот организам, со цена од 30\$ и 1095\$, може лесно да се пресмета колку е заработувачката во милијарди долари секој ден.

На врвот на листата на производите со „неверојатни карактеристики“ кои се продаваат на интернет, се наоѓаат пилули кои им овозможуваат на своите корисници да пијат пиво колку што сакаат, а при тоа да не се здебелат (цена од 71\$ за 60 пилули), и појас за вежбање, кој кога не си во фотелја предизвикува ист ефект како направени 600 склекови за 10 минути (цена од 146\$), потоа луспи од јајца на птици кои наводно го

¹²⁸ Matijašević, J., Krivičnopravna regulativa računarskog kriminaliteta; Pravni fakultet za privredu i pravosude, Novi Sad, 2013.

зголемуваат либидито, односно течност која маснотијата од ткивото во текот на спиењето ја претвора во мускулна маса, хормони кои ја враќаат довербата во сопствената сила, магнети против несоница, вода која лечи аритрит, лекови за лечење на AIDS, а кои доаѓаат од Африка како решение на анегдотата зошто некои Афрички жени се имуни на оваа болест....¹²⁹

Наведените истражувања укажуваат дека „наивните купувачи“, односно жртвите, најчесто се постарите личности, болните, изнемоштените и сиромашните, оние кои бараат „трошка надеж за светлина во мрачниот бескраен тунел“.¹³⁰

2.10 Изработка и употреба на лажна платежна картичка

Основната карактеристика на овој облик е незаконското заплenuвање на нештата од страна на другите. Постојат многу различни и разновидни форми во кои се појавува ова дело, како и начините на кои тие се реализираат. Еден од можните начини на класификација е според предметот што е присвоен од овој дел.¹³¹ Во овој поглед, во областа на компјутерскиот криминал, постојат следниве типични форми на кражба:¹³²

1. Кражба на компјутери и компјутерски компоненти;
2. Кражба на податоци;
3. Кражба на компјутерски услуги;
4. Крадење на лозинки, на кодови и на идентификациски броеви.¹³³

Во основа има два начини за реализација на овој дел:

1. класичен облик, што значи физички влез во просториите и кражба на компјутери и компјутерска опрема, и други работи кои незаконски се присвојуваат;

¹²⁹ Urošević, V., „Nigerijska prevara u Republici Srbiji“, Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Beograd str.255

¹³⁰ Прирачник за компјутерски криминал-Марко Зврлевски-Јавен Обвинител на Р.М - Скопје : OSCE, 2014 str.25

¹³¹ National Academy of Sciences, „The Digital Dilemma. Intellectual Property in the information Age“, USA, National Academy Press, 2000, http://books.nap.edu/html/digital_dilemma на 14.04.20 на 17:00 часот

¹³² Zaponnidis, C., New trends in banking management, Physisca, Verlag, 2002 str.15

¹³³ Petrović, R S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije: Uredništvo časopisa "Bezbednost" i lista "Policajac",/ Beograd 2000.godina str. 117.

2. друг начин, што подразбира логички упад во компјутерски систем и незаконско присвојување на компјутерски податоци, кодови, итн.

Луѓето се свесни за вредноста на информациите, компјутерите и компјутерските компоненти, па заради тоа компјутерите и другите електронски уреди често се цел на денешните крадци.

Како што побарувачката за компјутери се зголемува, така процентот на кражби е поголем, бидејќи тоа е производ кој крадците брзо го продаваат. Во Велика Британија, во 2014 година било објавено дека над 183.523 компјутерски уреди биле украдени (лаптопи, паметни телефони, таблети, итн.). Најголем број на кражби биле пријавени во управниот дел Манчестер (21.811), потоа во Западен Јоркшир (17.120).

Голем проблем претставуваат чувствителни лични и деловни информации коишто можат да се најдат на уредите, така што администрацијата на градот Глазгов во Шкотска била казнета со 150.000 фунти, бидејќи не ги презела потребните мерки за заштита на 74 лаптоп компјутери кои биле украдени, при што на еден од украдените лаптоп компјутери се наоѓале податоци за банкарските сметки на повеќе од 6.000 жители на Глазгов.

Кражбата на податоци и трговијата со нив, особено оние што претставуваат деловни и државни тајни, не е нова, но проблемот е огромен. Техничките можности за крадење информации од компјутерите се огромни.

Интернетот нуди широк спектар на продажба или размена на украдените податоци. Заштитата од кражба на податоци е неопходност, бидејќи информациите во денешно време се клуч на успехот во бизнисот, и ако до доверливите информации дојде конкуренцијата, може да им донесе одлучувачка предност на пазарот на оние кои ги имаат добиено информациите без никаков труд.

Со употребата на напредни криптолошки методи, на крадците им се овозможува безбедна продажба на податоци во целиот свет. Анонимноста која „делумно постои“ на

интернет, го прави интернетот идеално место за продажба, или за размена на податоци.¹³⁴

Кетрин Аркулета се повлече од функцијата претседател на Федералната служба за управување со персоналот на САД, бидејќи е откриено дека од електронските бази на податоци и услуги се украдени податоци на над 21,5 милиони луѓе кои во периодот од 2000-та година до денес конкурирале за работа во Федералната администрација.

Податоците се особено чувствителни, бидејќи тие содржат човечки безбедносни проверки, како и податоци за здравствениот статус, и се предмет на регуларна заштита на приватни податоци.¹³⁵ Кражба на компјутерски услуги, односно неовластено користење на системот, е една од најчестите форми на злоупотреба во областа на информатичката технологија. Иако кражбата на компјутерски услуги спаѓа во поблаги форми на компјутерска кражба, штетните последици што може да ги предизвика не се занемарливи.¹³⁶

Целта на извршувањето на ова кривично дело е за објавување на свои активности, а истите да користат туѓи компјутерски ресурси. Последиците што можат да произлезат се: оптоварување на работата на деловната мрежа, забавување на извршувањето на редовната работа и неизвршување на работните задачи.

¹³⁴ <https://www.pravdiko.mk/krivichni-prijavi-za-izработка-i-upotreba-na-lazhna-platezhna-kartichka/> на 14.04.20 на 17:00 часот.

¹³⁵ http://www.rtv.rs/sr_lat/evropa/milionska-kradja-lozinki-u-nemacko_454999.html на 24.04.20 г во 18:00 часот.

¹³⁶ EMV Card Personalization Specification, Ver. 1.1", EMVCo Association, July 2007, 66.

2.11 Ширење на расистички и ксенофобичен материјал по пат на информатички системи

Оваа одредба има меѓународна основа во Дополнителниот протокол кон Конвенцијата за отстранување на компјутерскиот криминал од 2001 година кој се однесува на казнување на актите на расизам и ксенофобија извршена по пат на компјутерски системи, и Рамковната одлука на Советот на министри на ЕУ од 2008 година за спречување на одредени форми на изразување на расизам и ксенофобија со средствата на казненото дело.

Делото го врши тој што во јавноста преку компјутерски систем шири расистички и ксенофобичен пишан материјал, или слика, или друга репрезентација на идеја или теорија која помага, промовира или поттикнува омраза, дискриминација или насилство против било кое лице или група врз основа на раса, боја на кожа или етничко потекло, како и веројатно уверување.

Дејствието на извршување е ширењето во јавноста на истото преку компјутерски систем, расистички и ксенофобичен пишан материјал. Поимот расистички и ксенофобичен пишан материјал како објект на дејствието е преземен од Дополнителниот протокол. Ширењето во јавноста на расистички и ксенофобичен пишан материјал се врши преку компјутерски систем. Делото се извршува со умисла која содржи свест за природата на материјалот, и волја со неговото ширење да се помага и да се промовира или поттикнува омраза, како и дискриминација кон лице или кон група на луѓе. Покрај исполнувањето на другите обележја, посебниот облик се разликува од него според дејствието на извршување, каде што станува збор за ширење на расистички и ксенофобичен пишан материјал преку други средства за јавно информирање. Исто така, диференцирани се три потешки облици, и тоа: извршување на делата со злоупотреба на положбата или овластувањето, ако поради тие дела дошло до насилство или безредие кон луѓе, или ако е предизвикана имотна штета од големи размери. Казната е затвор од една до пет години, или пак една до десет години.

Ширење на расистички и ксенофобичен материјал по пат на информатички системи според член 394-г, ги опфаќа следниве дејствија:¹³⁷

1. Тој што преку компјутерски систем во јавноста шири расистички и ксенофобичен пишан материјал, слика или друга репрезентација на идеја или теорија која помага, промовира или поттикнува омраза, дискриминација или насилство, против кое било лице или група, врз основа на пол, раса, боја на кожа, род, припадност на маргинализирана група, етничка припадност, јазик, државјанство, социјално потекло, религија или верско уверување, други видови уверувања, образование, политичка припадност, личен или општествен статус, ментална или телесна попреченост, возраст, семејна или брачна состојба, имотен статус, здравствена состојба, или на која било друга основа предвидена со закон или со ратификуван меѓународен договор, ќе се казни со затвор од една до пет години.¹³⁸
2. Со казната од ставот (1) на овој член ќе се казни и тој којшто делото ќе го стори преку други средства за јавно информирање.
3. Тој што делото од ставовите (1) и (2) на овој член го врши со злоупотреба на положбата, или на овластувањето, или ако поради тие дела дошло до безредие и насилства кон луѓе, или до имотна штета од големи размери, ќе се казни со затвор од една до десет години.¹³⁹

¹³⁷ https://www.pravdiko.mk/krivichna-prijava-za-shirene-na-rasistichki-i-ksenofobichen-materijal-po-pat-na_kompjuterski-sistem/ на 24.04.20 г во 18:00 часот.

¹³⁸ <https://kanal5.com.mk/articles/352593/obvinenie-za-novinar-za-shirenje-rasistichki-i-ksenofobichen-materijal-na-socijalni-mrezhi> на 24.04.20 во 18:00 часот.

¹³⁹ Член 394 – г, „Ширење на расистички и ксенофобичен материјал по пат на информатички системи“ <https://www.pravdiko.mk/wp-content/uploads/2013/11/Krivichen-zakonik-integralen-prechisten-tekst.pdf> на 14.04.20 на 17:00 часот.

Овде ќе прикажеме слика со табела преземена од Заводот за статистика за обвинети полнолетни лица според кривичното дело и видот на одлуката по години, и тоа за 2017-та година, и за 2018-та година.¹⁴⁰

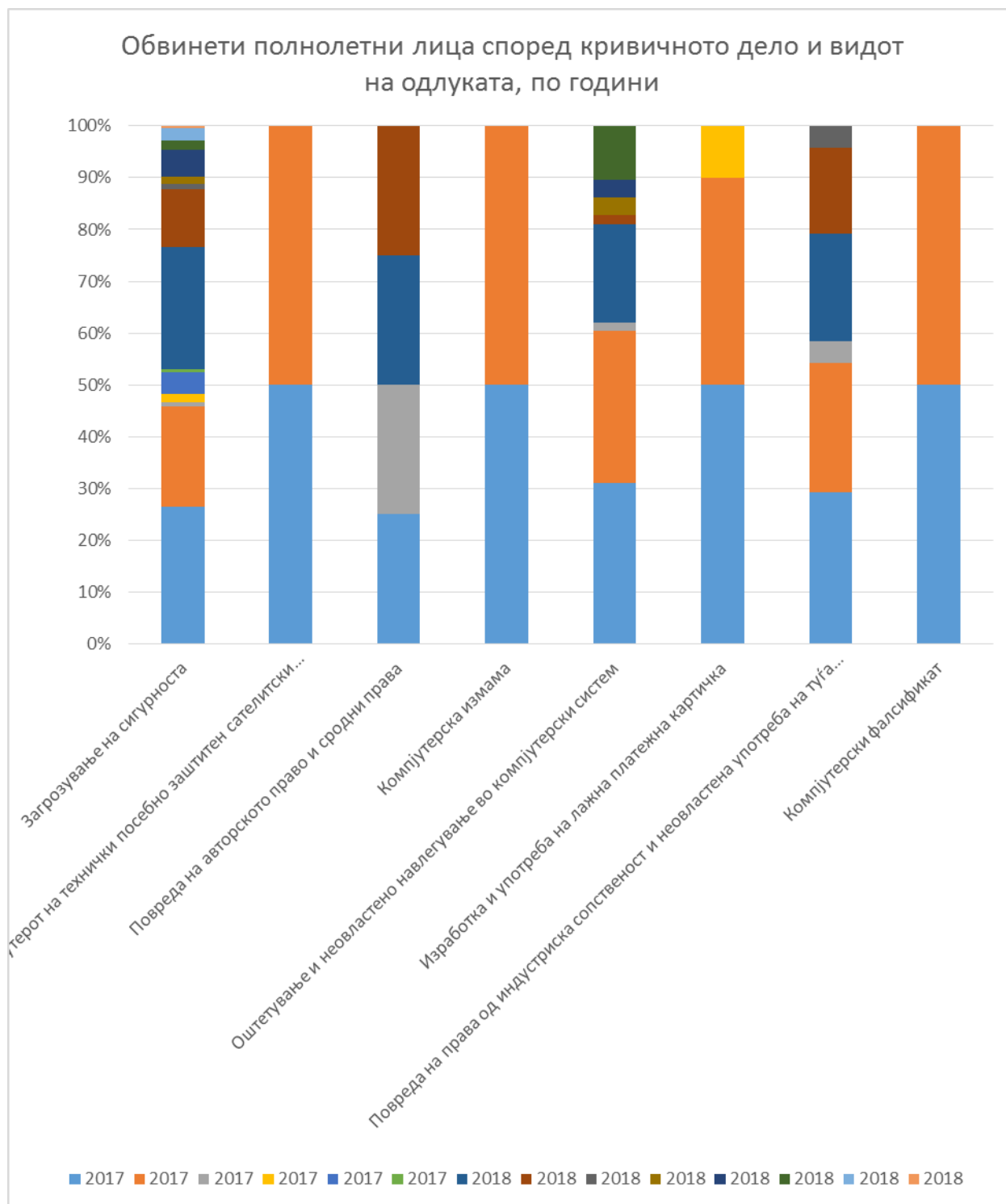
Обвинети полнолетни лица според кривичното дело и видот на одлуката, по години

	2017									2018								
	Вкупно обвинети лица	Осудителна пресуда	Ослободителна пресуда	Одбивателна пресуда	Пресуда врз основа на предлог-спогодба	Пресуда за издавање на казнен налог	Пресуда врз основа на признание на вина	Запрена постапка	Мерки на безбедност	Вкупно обвинети лица	Осудителна пресуда	Ослободителна пресуда	Одбивателна пресуда	Пресуда врз основа на предлог-спогодба	Пресуда за издавање на казнен налог	Пресуда врз основа на признание на вина	Запрена постапка	Мерки на безбедност
Загрозување на сигурноста	266	194	7	17	-	-	-	41	7	237	112	9	14	3	52	18	25	4
Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Повреда на авторското право и сродни права	1	-	1	-	-	-	-	-	-	1	1	-	-	-	-	-	-	-
Компјутерска измама	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Оштетување и неовластено навлегување во компјутерски систем	18	17	1	-	-	-	-	-	-	11	1	-	2	-	2	6	-	-
Изработка и употреба на лажна платежна картичка	10	8	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Повреда на права од индустриска сопственост и неовластена употреба на туѓа фирма	7	6	1	-	-	-	-	-	-	5	4	1	-	-	-	-	-	-
Компјутерски фалсификат	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Слика бр. 1. Обвинети полнолетни лица според кривичното дело и видот на одлуката, по години

¹⁴⁰

Извор: Државен завод за статистика
http://makstat.stat.gov.mk/PXWeb/pxweb/mk/MakStat/MakStat_Sudstvo/?rxid=46ee0f64-2992-4b45-a2d9-cb4e5f7ec5ef на
 30.04.20 на 17:00 часот.



Графички приказ бр. 1. Обвинети полнолетни лица според кривичното дело и видот на одлуката, по години, и тоа за 2017-та година, и за 2018-та година

ГЛАВА ТРЕТА

3. Компјутерски вируси

Вирусите се програми кои влијаат на програмата, така што работаат со основна програма или неконтролирано се копираат на компјутер и на тој начин влијаат на работата на компјутерот. „Тројанци“ или „тројански коњи“ се програмите кои се скриени во рамките на друга програма и се активираат со таа програма вршејќи несакани дејства во вид на вирус во компјутерот. „Црви“ се програми кои постојано се размножуваат, и тие се опасни бидејќи можат да се шират и на други компјутери во мрежата.¹⁴¹

„Дропери“ се програми кои ги отстрануваат и инсталираат вирусите, а „бомбите“ се програми кои активираат специфични вируси кои можат да бидат хибернација во компјутерскиот систем. Стеганографијата се користи за прикривање на информации за извршените кривични дела и се користи за да не може да се утврди сторено кривично дело со проста визуелна инспекција, туку за тоа да мора да користат специјални програми за откривање на стеганографски пораки. Со веб преземање корисниците се лишени од контролите на интернет прелистувачите или сајтовите и се пренасочени кон друга содржина. Саботерите имаат различни мотиви кои можат да бидат: политички, економски, воени, службени, или приватни. Нема милост во економската игра и често не се избираат начини и ресурси, па затоа сè почести се саботажи на компјутерските системи, мрежи и веб-сајтови на конкурентите. Програмер мотивиран од одмазда е казнет со затвор од триесет месеци, бидејќи во почетокот на 2008 година во американската федерална држава Њујорк, во компанијата каде што бил вработен, во фирмата MedicoHealth Solutions, се обидел да го саботира компјутерскиот систем, при што успеал да уништи и онеспособи повеќе од седумдесет сервери на компанијата.¹⁴²

Компјутерски вирус е програма која извршува недозволен дејства во системот на корисникот без негово знаење и дозвола.

¹⁴¹ Најпознат пример на логичка саботажа се поврзува за иранската нуклеарна програма. https://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=0 06.04.20 во 10:30 часот.

¹⁴² Cvetković, Z., Kompjuterski kriminal – članak, 2011, 7-8.

Со цел одредена програма да се смета за компјутерски вирус, таа мора:

1. сама да се активира и да го внесе својот код во патот за извршување на друга програма.

2. да се реплицира себеси, односно да ги замени другите програми за стартување на копии заразени со вирусни датотеки. Вирусите ова можат да го направат и на персонални компјутери, и на сервери.

3. да има носител за да може понатаму да се пренесува во контакт со трета страна.

Постојат два облика за извршување на ова дело. Прво е создавање на вирусот и е секогаш свесно дејство, додека дистрибуцијата може да биде и несвесно дејство.

Компјутерските вируси можат да направат различни промени во системите, но најчести се:

1. промена во големината на програмата;
2. забавување на програмите и системите;
3. погрешно извршување на програмата;
4. оневозможување на функционирањето на системот и негово онеспособување;
5. промени во програмската датотека;
6. уништување на содржината;
7. копирање на непотребни и штетни програми и информации;
8. намалување на достапниот слободен простор во системот, итн.¹⁴³

Компјутерските вируси се мали програми од неколку килобајти, кои имаат исклучиво за цел да направат штета на заразен компјутер.

Најчесто се размножуваат на начини со којшто се „вгнездуваат“ во други фајлови, а штета предизвикуваат така што ги бришат, или ги менуваат фајловите на дискот.

Доколку се работи за информациски системи, вирусот од заразениот компјутер може да зарази друг компјутер во компјутерска мрежа, со цел да измени или оштети фајлови од оперативниот систем на компјутерот.

¹⁴³ Petrović R. S., Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd 2000.godina, 185.

„Заразувањето“ на фајловите од оперативниот систем на компјутерот со вирус, црв, или тројанец, настанува на неколку начини:

1. преку разни медиуми кои се носачи на информации кои се заразени од компјутер со вирус, црв, или тројанец;
2. преку фајлови добиени преку имеил;
3. преку фајлови преземени од интернет;
4. посета на веб-страница на која е поставен вирус, при што таквите сајтови се главно поставени на бесплатен сервер, имаат долги адреси (<http://members.tripod.com/~ludnica/cool.html>), и содржат скрипта со која се уфрла вирус, или тројанец;
5. сигурносни дупки, односно безбедносни пропусти во самите софтвери и оперативни системи кои овозможуваат пенетрација на вирусите, тројанците, или црвите.¹⁴⁴

Антивирусни програми

За борба против вирусите се користат антивируси, програми кои спречуваат компјутерот да се инфицира, и кои ги уништуваат вирусите доколку дојде „инфекција“ на компјутерот. Антивирусните програми спречуваат „зараза“, така што ги скенираат фајловите кои се употребуваат во барање на кодот (со програма внатре во програмата) и доколку пронајдат присуство на вирус, тие го спречуваат стартувањето на програмата. Фајловите кои се заразени се чистат така што внатре, во заразениот фајл, се брише кодот за којшто се сигурни дека е вирус.

Антивирусите имаат база на кодови од вирусите за кои производителите на антивирусите успеале да набават заштита.

Доколку антивирусот е постојано вклучен, мануелното скенирање е непотребно бидејќи активниот антивирус го скенира секој фајл кој се стартува.

Освен што е потребно на компјутерот да има инсталирано антивирус, исто така е потребно да се обзбедуваат нови дефиниции за антивирусот, односно бази на податоци за новите вируси, за да може да се откриваат новите вируси.

¹⁴⁴ Интернет страница (<http://www.apisgroup.org/sec.html?id=7>) на 06.04.2020 г во 10:45 часот

Начинот на којшто се обезбедуваат новите дефиниции се нарекува абдејтување (engl. update), при што додека компјутерот е конектиран на интернет, е потребно на иконата на прозорот од антивирусот да се кликне на „Update“, а потоа антивирусот автоматизирано ги повлекува новите дефиниции од производителот на антивирусот.¹⁴⁵

Заштита од вируси

Универзалната заштита од вируси се состои во тоа што секој нов фајл којшто ќе се сними на дискот (преку USB, CD, ICQ62 итн.), задолжително да се скенира со некој антивирусен програм пред да се стартува.

Исто така, заштитна мерка е недозволувањето на снимање или копирање на фајлови и фолдери од друго лице, освен од сопственикот, односно корисникот на компјутерот.

Антивирусот, во согласност со мерки за заштита од вируси, потребно е да биде абдејтуван, така што со новите дефиниции да се спречи инфицирање на компјутерот.¹⁴⁶

Тројанци

Тројанци се програми коишто кога ќе влезат во некој компјутер, ги праќаат сите шифри и лозинки во сандачето на електронската пошта на оној кој ги уфрлил, со што му овозможуваат на лицето кое ги уфлило тројанците да пристапува до заразениот диск, што значи дека оној кој ги уфрлил тројанците може да чита, пишува, брише, или менува фајлови на заразениот компјутер дури и да добие потполн пристап во целокупната меморија на заразениот компјутер.¹⁴⁷

Како најчест случај се јавува гасење на заразениот компјутер, или пак користење на истиот за напад на друг компјутер, а истото се извршува без знаење на сопственикот на компјутерот. Тројанците своето име го добиле по познатиот коњ, кој за време на опсадата на Троја, која Грците безуспешно ја напаѓале 10 (десет) години, за на крајот да се повлечат

¹⁴⁵ <https://mk.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81>

На 06.04.2020 година во 11:05 часот.

¹⁴⁶ http://dimovski-darko.blogspot.com/p/blog-page_5627.html на 06.04.2022 година во 11:00 часот.

¹⁴⁷ https://mk.wikipedia.org/w/index.php?title=%D0%A1%D0%BC%D0%B5%D1%82%D0%B0%D1%87%D0%BA%D0%B8_%D0%B2%D0%B8%D1%80%D1%83%D1%81&action=edit на 14.04.20 на 17:00 часот.

оставајќи пред нејзиниот влез огромен коњ, како знак за признавање на поразот.¹⁴⁸ Тројанските војни, воодушевени од победата, го внеле коњот внатре во градот и се посветиле на прославувањето на својата голема победа.

Меѓутоа кога сите тројански војни заспале пијани, од коњот се отворила добро скриена врата и од неа излегол одред на грчки војни, кој ја отворил вратата на тврдината, пуштајќи внатре да влезат останатите Грци, кои повлекувањето го исценирале и го чекале моментот кога ќе се отворат вратите да влезат. Потоа Троја многу лесно ја зазеле. На ист начин денес е возможно неовластено да се пристапи во други компјутери, и да се украдат потребните фајлови, интернет лозинки, и слично.

Накратко речено, можна е злоупотреба на одреден компјутер без притоа сопственикот да е свесен. Некој друг, со програмата наречена „Тројански коњ“ има корисничка привилегија во неговиот компјутер. Последиците кои може да бидат катастрофални се однесуваат на уништување на документи на дискот или на некој проект на којшто е работено со години од страна на оној што извршил уфрлување на тројанец, или пак од истиот да се очекува префрлање на документите на друг компјутер итн.

Основни правила на заштита од вируси, црви и тројанци се следниве:

1. Потребно е скенирање на секој програм пред да се стартува компјутерот.
2. Потребно е скенирање на секој имејл или фајл кој ќе стигне преку ICQ или MIRC пред да се отвори, без разлика кој е испраќачот, бидејќи истиот не знае дека компјутерот е инфициран.
3. Да не се посетуваат страници чии адреси се добиваат од непознати лица.
4. Потребно е секогаш да се имаат нови антивируси кои ги откриваат вирусите во real time, пред истите да се копираат на тврдиот диск, без разлика дали се истите компресирани, вградени или слично.

¹⁴⁸ ICQ (engl. Seek You - „те барам“) е компјутерски програм наменет за размена на текстуални пораки помеѓу неговите корисници, преку користење на Интернет. Првата верзија е излезена во 1996 година, а називот е создаден од играта со англиските зборови. Со текот на времето се појавиле и можности за пренос на фајлови, слики, како и онлајн играње помеѓу корисниците. <http://en.wikipedia.org/wiki/ICQ> на 06.04.2020 година во 11:30 часот.

5. Потребно редовно да се врши „update“ на новите дефиниции за антивирусните програми, за да може да се соберат информации за новите вируси и тројанци.
6. Задолжително користење на Firewall.
7. Да се изврши енкрипција на датотеките за да се спречи нивната неовластена употреба.
8. Поставување и користење на password-е за влез во датотеки.
9. Недозволување на внесување на фајлови, освен од сопственикот.
10. Користење на легални софтвери, бидејќи во нелегалните софтвери се наоѓаат безбедносни пропусти или „bugs“, кои може да овозможат навлегување во компјутерот.¹⁴⁹

3.1. Социјален инженеринг

Под социјален инженеринг најчесто се подразбира уметност на манипулирање со луѓе во вршење на активности или откривање на доверливи информации. Иако е сличен со изневерувањето на довербата, или едноставна измама, терминот обично се однесува на изигрување или измама за целите на собирање на информации, измама, или пристап до компјутерски систем. Во повеќето случаи напаѓачот никогаш не доаѓа лице во лице со жртвите. „Социјалниот инженеринг“¹⁵⁰ како чин на психолошка манипулација беше популаризиран од страна на хакерскиот консултант Кевин Митник. Терминот претходно бил поврзуван со општествените науки, но неговата употреба се раширила меѓу компјутерските професионалци. Сите техники на социјален инженеринг, се базираат на специфични атрибути на човековото донесување одлуки, познати како когнитивни предрасуди.

Овие предрасуди, понекогаш нарекувани и „Бубачки во човечкиот хардвер“, се експлоатираат во различни комбинации за да се создадат техники за напад, од кои некои се наведени подолу.

¹⁴⁹ https://mk.wikipedia.org/wiki/%D0%97%D0%BB%D0%BE%D0%BD%D0%B0%D0%BC%D0%B5%D1%80%D0%B5%D0%BD_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC на 06.04.2020 година во 11:45 часот.

¹⁵⁰ [https://mk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D1%98%D0%B0%D0%BB%D0%B5%D0%BD_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D0%BD%D0%B3_\(%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82\)](https://mk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D1%98%D0%B0%D0%BB%D0%B5%D0%BD_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D0%BD%D0%B3_(%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82)) на 24.04.20 г во 18:00 часот.

Техника на изговор

Техника на изговор е чин на создавање и на користење на измислено сценарио (на изговор) за да се нападне обележана жртва на начин на којшто се зголемува шансата дека жртвата ќе открие информации, или ќе спроведе активности, кои во обични околности најверојатно не би ги направила.

Елаборираната лага најчесто вклучува некои претходни истражувања или подготвување и користење на овие информации за имитирање (на пример, датум на раѓање, бројот на социјално осигурување, износот на последната сметка), за да воспостави легитимност во умот на жртвата.

Оваа техника може да се користи за да се натераат компаниите да откријат информации за корисниците, а ја користат и приватните детективи за да добијат телефонски записи, корисни записи, банкарски записи и други информации директно од службата на претставници на компанијата.

Информациите потоа може да се користат за да се воспостави уште поголема легитимност под построги сослушувања со менаџер, на пример, да се направат промени на сметка, специфични состојби на сметка, итн.

Техниката на изговор може да се користи кога некоја личност сака лажно да се претставува како: свој колега, полиција, банка, даночна власт, свештенство, осигурителни истражители, или било која друга личност која би можела да изгледа авторитетно во умот на целните жртви, или со право да легитимира. Напаѓачот едноставно мора да подготви одговори на прашањата кои може да бидат поставени од страна на жртвата. Во некои случаи, сè што е потребно е глас што звучи авторитетно, сериозен тон, и способност брзо да се реагира.

Кражба преку правење диверзија

Кражбата преку правење диверзија, исто така позната како „игра во катче“, или „игра зад аголот“, потекнува од источниот крај на Лондон.

Накратко, кражба преку правење диверзија е „измама“ применета од страна на професионални крадци, вообичаено против транспортна или курирска компанија.¹⁵¹

Целта е да се убедат лицата одговорни за легитимна испорака дека пратката се бара на друго место, односно „зад аголот“.

Со пренасочениот товар/пратка, крадците го убедуваат возачот да ја остави пратката во близина на адресата, или далеку од адресата на примачот, во изговор дека таа „директно ќе пристигне“ или „итно се бара некаде на друго место“.¹⁵²

„Измамата“ има многу различни аспекти кои вклучуваат техники за социјален инженеринг со кои се убедуваат легитимните административци, или персоналот за сообраќај на транспортни или курирски компании да му издадат инструкции на возачот да ги пренасочи пратките или товарот.¹⁵³

Друга варијација на ваквата кражба е стационирање на безбедносно комбе пред банка во петок навечер. Елегантно облечен полицаец ја користи фразата „ноќе е побезбедно, господине“. Со овој метод продавачите лековерно го депонираат нивниот профит во комбето.

Тие добиваат потврда за примениот профит, но подоцна оваа потврда излегува дека е безвредна.

Слична техника беше користена пред многу години за да се украде концертно пијано од производителот Steinway од радио-студио во Лондон. Изговорот бил: „дојдовме да го сервисираме пијаното“.

¹⁵¹ Security engineering: a guide to building dependable distributed systems, second edition, Ross Anderson, Wiley, 2008 – 1040 pages ISBN 978-0-470.06852-6, 155.

¹⁵² The story of HP pretexting scandal with discussion is available at Davani, Faraz (14 August 2011). „HP Pretexting Scandal by Faraz Davani“, 25.

¹⁵³ „Something Every Consumer Should Know“. www.HandelontheLaw.com. 27 March 2009. Конс, 11.

Мрежно рибарење

Мрежно рибарење (или фишинг) е техника на добивање приватни информации преку измама.

Типично, напаѓачот праќа е-меил којшто се чини дека доаѓа од легитимна компанија, банка, или кредитна компанија, со барање за „верификација“ на информации и предупредување за некои сериозни последици, доколку информациите не се верифицираат.

Е-поштата обично содржи линк до лажни веб-страници, кои се чинат легитимни, со лого, содржина и форма на компанијата која бара сè, од домашна адреса, до ПИН на кредитна картичка.¹⁵⁴

На пример, во 2003 година е забележано зголемувањето на бројот на вакви измами, во кои корисниците добиваат е-меил, наводно од еВау, тврдејќи дека сметката на корисникот ќе биде откажана ако не се кликне на линкот што е даден за да се ажурира кредитната картичка (информации кои вистинскиот еВау веќе ги има).

Поради тоа што е релативно едноставно да се направи веб-страница која личи на страница на легитимна организација со имитација на HTML кодот, измамата ги наведува луѓето да мислат дека се контактирани од страна на еВау, а потоа, да мислат дека одат до сајт на еВау да ги обноват своите информации за сметката. Со спамирање големи групи на луѓе, „рибарот“ смета дека меилот ќе го прочитаат процент на луѓе кои веќе давале броеви на кредитни картички на еВау легитимно, па би можеле да одговорат.¹⁵⁵

ИГО или рибарење преку телефон

Оваа техника користи систем за интерактивен гласовен одговор, ИГО (говорен автомат) (анг. Interactive voice response, IVR), за да рекреира легитимна звучна копија на

¹⁵⁴ „The Right To Remain Silent“. www.almanacnews.com. 8 November 2011. конс. 18 November 2011.

¹⁵⁵ [https://mk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D1%98%D0%B0%D0%BB%D0%B5%D0%BD_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D0%BD%D0%B3_\(%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82\)](https://mk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D1%98%D0%B0%D0%BB%D0%B5%D0%BD_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D0%BD%D0%B3_(%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82)) на 06.04.2020 година во 12:00 часот.

IVR системот од банка, или од друга институција. Од жртвата е побарано (обично преку фишинг е-пошта) да се јави во „банката“ преку (идеално бесплатен) број, со цел да се „проверат“ одредени информации. Еден типичен систем ќе ја отфрла најавата постојано, обезбедувајќи на тој начин жртвата да го внесе ПИН-от или лозинките повеќепати, често откривајќи неколку различни лозинки. Повеќе напредни системи ја носат жртвата кај напаѓачот, кој се претставува како корисничка служба за понатамошно испитување.¹⁵⁶

Една од тие системи може да снима типични команди („притиснете еден за да ја смените лозинката, притиснете два за да зборувате со корисничката служба“) и да ги пушта рачно во реално време, давајќи изглед на говорен автомат без трошоци. Рибарењето (фишинг) преку телефон се вика вишинг.

Наведување

Наведувањето е како Тројанскиот коњ во реалниот свет, којшто користи физички медиуми, и се потпира на љубопитноста или алчноста на жртвата.

Во овој напад, напаѓачот остава инфицирани флопи дискети, CD-ROM или USB флеш дискови со малициозен софтвер на локација каде што може лесно да се најдат (бања, лифт, тротоар, паркинг), давајќи им љубопитен изглед, а едноставно чека жртвата да почне да го користи уредот.

На пример, напаѓачот може да креира диск со корпоративно лого, лесно достапен од веб-страницата на жртвата, и да напише „резиме за плата на извршителите Q2 2012“ на предната страна. Напаѓачот потоа ќе го остави дискот во лифт, или некаде во фоајето на целната компанија. Некој вработен може да го најде и потоа да го вметне дискот во компјутерот за да ја задоволи својата љубопитност, или некој добронамерен човек да го најде дискот и да го предаде во компанијата.

Во било кој случај, како последица, само со вметнување на дискот во компјутерот за да ја видите содржината, корисникот ќе инсталира штетен софтвер, најверојатно

¹⁵⁶ Goodchild, Joan. „Social Engineering: The Basics“, csoonline, 11 јануари 2010, 15.

давајќи му на напаѓачот непречен пристап до компјутерот на жртвата, и можеби, пристап до внатрешната компјутерска мрежа на целната компанијата.

Ако компјутерот не ја блокира инфекцијата, компјутерите на кои е поставено „автоматско отворање“ на додадените медиуми може да бидат компромитирани веднаш штом непријателскиот диск е вметнат.

Quid pro quo (значи услуга за услуга).¹⁵⁷

Напаѓачот се јавува на случајни броеви во одбрана компанија тврдејќи дека се јавува како техничка поддршка, за на крајот да најде некој со легитимен проблем, благодарен што некој одговорил за да му помогне. Напаѓачот ќе „помогне“ да се реши проблемот во процесот, и ќе побара од корисникот да типка команди кои му овозможуваат на напаѓачот пристап или стартување на малициозен софтвер. Во анкета за безбедноста на информациите од 2003-та година, 90% од канцелариските работници на истражувачите им ја дале нивната лозинка како одговор на анкетно прашање во замена за евтино пенкало. Слични истражувања во подоцнежните години добиле слични резултати, користејќи чоколади и други евтини мамки, иако тие не направиле никаков обид да ги валидираат лозинките.

Техника на искористување

Напаѓачот, кој бара влез на забрането подрачје каде што пристапот е без човечки надзор со електронска контрола на пристап, на пример со РФИД (радио-фреквенциска идентификација) картички, едноставно оди зад лице кое има легитимен пристап. Поради учтивост, легитимното лице обично ќе ја одржи вратата отворена за напаѓачот.

¹⁵⁷ Usenet sample citing moniker use-several examples. 1990s to present. 15-18.

3.2. Детска порнографија

Во членот 122 од Кривичниот законик¹⁵⁸ под детска порнографија се подразбира „порнографски материјал кој визуелно прикажува очигледни полови дејствија со малолетник, повозрасно лице кое изгледа како малолетник, или го прикажуваат малолетникот/повозрасното лице кое изгледа како малолетник во очигледна сексуална положба, или реални слики кои прикажуваат очигледни полови дејствија со малолетник и го прикажуваат малолетникот/повозрасното лице кое изгледа како малолетник во очигледна сексуална положба“.

Понатаму, во членот 193-а од овој законик, кој се однесува на детска порнографија, е пропишано и кривичното дело „производство и дистрибуција на детска порнографија“:

„Тој што произведува детска порнографија со цел за нејзина дистрибуција или ја пренесува, или ја нуди, или на друг начин ја прави достапна детската порнографија, ќе се казни со затвор од најмалку пет години. Тој што набавува детска порнографија за себе или за друг или поседува детска порнографија, ќе се казни со затвор од пет до осум години.¹⁵⁹ Ако делото е сторено преку компјутерски систем или друго средство за масовна комуникација, сторителот ќе се казни со затвор од најмалку осум години“, се пропишува во членот 193-а од Кривичниот законик.¹⁶⁰

Во Кривичниот законик, исто така, е пропишано кривичното дело „намамување на обљуба или друго полово дејствие на дете кое не наполнило 14 години“:

„Тој што преку компјутерско-комуникациски средства со закажување средба, или на друг начин намамува дете кое не наполнило 14 години на обљуба, или друго полово дејствие, или на производство на детска порнографија, и ако со таквата намера е остварена непосредна средба со малолетникот, ќе се казни со затвор од една до пет години“, се пропишува во членот 193-б од Кривичниот законик.

¹⁵⁸ Член 122 од Кривичниот законик на 06.04.20 на 12:45 часот.

¹⁵⁹ Член 193-а од Кривичниот законик.

¹⁶⁰ <https://akademik.mk/kaznite-za-detska-pornografija-sporod-krivichniot-zakonik/> на 06.04.2020 година во 12:45 часот.

Сведоци сме на многубројните обиди на сите владини и невладини тела да се маргинализираат порнографските содржини на интернет. Од сите порнографски содржини достапни преку сите видови на медиуми, детската порнографија е основна мета на законодавците. Детската порнографија е доказ за сексуалната злоупотреба на децата, освен во случаите кога се работи за псевдо-фотографии.

Постојат повеќе концепции (на реализам, на тенденција, и на објект) чијашто цел е да придонесат за разграничувањето на морално недопуштената, општествено штетната и казнива порнографија, од она што е уметнички, естетски, креативно и прифатливо.

Општ принцип што се применува во повлекувањето на „границата на толеранција“ е да се поаѓа од барањето уметничкото, или друго дело, да се оценува како целина, со сите негови реперкусии на претежно позитивно или претежно негативно влијание, да се поаѓа од тоа дали неговата генерална тенденција е естетското доживување, научно или друго корисно сознание, или пак исклучително сексуално доживување. Некои автори со право сметаат дека како казниви треба да се оценат повеќе сегменти од социјалниот живот меѓу кои најбитни се: самото контактирање преку компјутерско-комуникациски средства, или на друг начин, кое што има за цел заведување на малолетници кои не наполниле 14 години. Понатаму, овозможувањето пристап на малолетниците без пречки кон порнографски материјал, и детска порнографија, што подразбира производство, дистрибуција и поседување. Периодот од 1969-1979-тата година е периодот познат како „10 годишно¹⁶¹ лудило“ меѓу уживателите на ваквите материјали. Овој период се смета и за еден од најкобните за детската порнографија. Имено, во овој период скандинавските земји, особено Данска, ќе станат едни од светските произведувачи на вакви материјали.

Типични за овој период се и печатените материјали од кои многу весници ќе развијат силен бренд. Меѓу најпознатите ќе ги вброиме Children-Love, Lolita, Lollitots, Nudist Moppets, и Bambina-Sex. Оваа декада ќе заврши со мултимилионска заработка на производителите и на дистрибутерите на детска порнографија. Билионската заработка од

¹⁶¹ <https://akademik.mk/kaznite-za-detska-pornografija-sporod-krivichniot-zakonik/> на 25.04.2020 г во 18:00 часот.

2,4 билиони долари ќе следи во наредната декада, во која ќе бидат експлоатирани 1.2 милиони деца.

Терминот „порнографија“ за прв пат ќе биде дефиниран во Oxford English Dictionary во 1857-та година.

Овој поим ќе ги опфати француските ракописи во кои се опфатени проституција, безобразност, непристојност, бесрамност, безобразни/срамотни зборови итн. Поимот детска порнографија е дефиниран многу подоцна. Сеопфатноста на овој поим во светските законодавства е различна.¹⁶²

Во таа смисла, во американското законодавство овој поим е екстензивно определен, и истиот е дефиниран на следниот начин:

Под поимот „детска порнографија“ се подразбира секој визуелен приказ, вклучувајќи фотографија, филм, видео, слика, компјутерски произведена или модификувана слика, или фотографија, без разлика дали е произведена или направена електронски или механички, а која содржи очигледни сексуални дејства каде што:

(А) визуелниот приказ вклучува малолетник кој врши очигледни сексуални дејства;¹⁶³

(В) таквиот визуелен приказ е слика, компјутерска фотографија, или компјутерски произведена фотографија на која очигледно се гледа дека малолетник учествува во сексуални дејства; или¹⁶⁴

¹⁶² Според оваа концепција под порнографија се подразбира хереалистичен начин на прикажување на сексуалните појави, со што насилно се фалсификува суштината на сексуалното; Камбовски, В. Казнено право - Посебен дел, просвето дело, Скопје, 2003 година, 55.

¹⁶³ под поимот „малолетник“ било кое лице под возраст од 18 години, 200.

¹⁶⁴ —очигледно малолетно лице— е дефинирано како — (А) лице кое — (i) (I) лице кое било малолетник кога визуелната слика била создадена, креирана, адаптирана или модифицирана.

или(ii) чија што слика кога било малолетно е искористена за креирање, адаптирање, или модифицирање на визуелен приказ; и (ii) може да се распознае дека станува збор за одредено лице препознавајќи го по ликот, некоја особена карактеристика на 14.04.20 на 17:00 часот како на пример белег или сл.; и(В)нема да се бара да се докажеидентитетот на лице кое е очигледен малолетник.

(С) таквиот визуелен приказ е создаден, креиран, адаптиран, или модифициран за на него очигледно да се распознава дека малолетно лице учествува во полови дејства.¹⁶⁵

Поимот детска порнографија е дефиниран во член 2 од Факултативен протокол кон Конвенцијата за правата на детето, којшто се однесува на продажба на деца, детска проституција и детска порнографија на следниот начин:¹⁶⁶

„...детска порнографија значи преставување на дете вклучено во реални или симулирани експлицитни сексуални активности со било какви средства, или било какво претставување на половите органи на детето, пред сè за сексуални цели“.¹⁶⁷

Во македонското законодавство поимот детска порнографија за првпат е воведен со новелата на КЗ од 15.01.2008 година. Истиот е дефиниран во член 122 од КЗ на РМ:¹⁶⁸

„Под детска порнографија се подразбира порнографски материјал кој визуелно прикажува очигледни полови дејствија со малолетник, или очигледни полови дејствија со лице кое изгледа како малолетник, или реални слики кои прикажуваат очигледни полови дејствија со малолетник“.¹⁶⁹

Начини на пренесување на детска порнографија

Се поставува прашањето: кои се начините преку кои се дистрибуира, односно разменува детската порнографија, и дали истите можат да се идентификуваат, а со тоа и

¹⁶⁵ продуцирање|| значи производство, режирање, мануфактура, издавање, објавување или рекламирање;

¹⁶⁶ Ferraro, M., Casey, E., McGrath, M.: INVESTIGATING CHILD EXPLOITATION AND PORNOGRAPHY: THE INTERNET, THE LAW AND FORENSIC SCIENCE, Elsevier Academic Press, 2005, 9.

¹⁶⁷ поимот —очигледно|| кога се користи во однос на виртуелните слики, означува виртуелно несомнени слики, во смисла на тоа дека и просечен човек кој ја гледа виртуелната слика може да заклучи дека на сликата има малолетник инволвиран во очигледни полови дејства. Оваа дефиниција не се однесува на цртежи, цртани филмови, скулптури или уметнички слики. на 14.04.20 на 17:00 часот.

¹⁶⁸ (B) за целите на член 8(B) од оваа секција под поимот очигледни сексуални дејствија се подразбира — (i) графички сексуален однос, кој што вклучува однос гениталии со гениталии, орално – генитално, анално генитални или орално – анално, без разлика дали станува збор за лица од ист или спротивен пол, или симулиран сексуален однос, при што гениталиите, градите или „срамната— област е видлива; (ii) графички симулации; (I) Бруталност, грубост, Свирепост, противприроден однос; (II) мастурбација; или (III) садистичко или мазохистичко однесување; или (iii) графички или симулирани експозиции на гениталите или срамната област; на 14.04.20 на 17:00 часот.

¹⁶⁹ Stojanovic, B. Krivicno pravni aspekt pornografije, JRKK, 100.

да се зауздаат? За да може да се следи, а воедно и да се упрости комуникацијата при користењето на интернетот, секој компјутер при секоја трансакција којашто ја врши преку интернет мора да биде идентификуван. Од овие причини, интернетот примарно користи IP (Internet Protocol) адреси коишто се состојат од сет од броеви од 1 до 255.

Со овие IP адреси се идентификува интернет-конекцијата. Овие IP адреси можат да бидат статични и динамични.¹⁷⁰

Така на пример, серверите, како што е на пример www.missingkids.org, имаат статична IP адреса, додека dial-up корисниците имаат IP адреси кои што врз основа на принципот random, ги дава Банката на модеми којашто е управувана од Internet Service Provider (ISP).¹⁷¹

Овие адреси се динамични затоа што при секое поединечно приклучување на интернет, на корисникот му се дава различна IP адреса.

Генерално гледано, сите корисници кои користат кабелски оператори, DSL, или друга high-speed конекција, имаат динамични IP адреси.¹⁷²

Тоа практично би можело да значи дека не може да се идентификува IP адресата од која се посетувани сајтовите со детска порнографија, затоа што доколку таквите луѓе имаат познавања од компјутерска технологија, тогаш веднаш по посетата на таквите сајтови/форуми би го рестартирале модемот, и при повторното вклучување на интернет би добиле нова IP адреса. Меѓутоа, доколку интернет-провајдерите би се задолжиле со водење на евиденција која IP адреса ја имал секој корисник во одреден момент, тогаш би можеле да се и идентификуваат посетителите на ваквите сајтови, форуми и сл. Еден од начините на испраќање/примање на вакви содржини е секако e-mail-от, односно

¹⁷⁰ Според оваа концепција под порнографија се подразбира хереалистичен начин на прикажување на сексуалните појави, со што насилно се фалсификува суштината на сексуалното; Камбовски, В. Казнено право - Посебен дел, просвето дело, Скопје, 2003 година, 222.

¹⁷¹ За оваа концепција порнографијата е грубо прикажување на сексуалните нагони што предизвикува деградирање на човекот на ниво на обичен објект на половите желби; Ibid, 222.

¹⁷² Според оваа концепција одлучувачка е целта поради која се прикажуваат ваквите содржини односно дали целта е побудување на сексуалниот нагон или нешто друго; Ibid, 222.

електронската пошта. За придружување на комуникацијата помеѓу обожавателите на ваквите материјали, истите ги користат и т.н. Newsgroups, каде што повеќе корисници од сите страни на светот формираат група која ги обединува интересите, и ги задоволува потребите на нејзините членови.¹⁷³

Така на пример, групите како што се alt.binaries.pictures.erotica.children и alt.binaries.pictures.erotica.pre-teen (abpep-t), во своето членство вбројуваат педофили коишто разменуваат детска порнографија. Со цел да не бидат идентификувани овие групи, често го менуваат своето име, но скоро секогаш во својот назив содржат збор којшто алудира на содржината на материјалот кој се разменува во групата.¹⁷⁴ Newsgroups се слични на electronic bulletin board systems (BBS), или електронските огласни табли. Discussion board е слична на newsgroups во начинот на испраќање на пораките коишто центрифугално се движат околу зададената тема, и истите се несинхронизирани.¹⁷⁵

Единствената разлика е во местото каде што се чуваат пораките. Кај newsgroups, истите се чуваат во серверите кои што се администрирани засекаде во светот од различни луѓе, додека кај discussion boards пораките се наоѓаат на единствен сервер одржуван од креаторот на ваквите „огласни табли“.

Bulletin board systems се исто така слични на претходните два начини на комуникација. И овие „огласни табли“ имаат огромен придонес во распространувањето на детската порнографија. Истите постојат уште пред појавата на компјутерската технологија, а по појавата на првиот персонален компјутер тие се првото електронско медиумско средство коешто ќе биде искористено за препраќање на детска порнографија. Наредното популарно медиумско „катче“ за детска порнографија датира од 1989-тата година преку иновацијата на јазик за маркирање на хипертекст, или hypertext markup language (HTML) којшто го овозможил креирањето на Web страна.

¹⁷³ Jenkins, P.: 34.

¹⁷⁴ Според оваа концепција одлучувачка е целта поради која се прикажуваат ваквите содржини односно дали целта е побудување на сексуалниот нагон или нешто друго; Ibid, 222.

¹⁷⁵ Stojanovic, B. Krivcno pravni aspekt pornografije, JRKK, 100.

Web страната е сет од фајлови наречени „Web pages“ кои што се достапни¹⁷⁶ преку интернет. Овие фајлови содржат слики, текст, звук, видеа и комбинации од сите претходно наведени фајлови.

Секој Web сајт има своја адреса, Uniform Resource Locator, или скратено URL. Сопственикот на Web-страната ја резервира својата URL адреса преку сервис кој продава адреси. Повеќето земји имаат црни листи на web-сајтовите, кои ги укинуваат веднаш по утврдувањето дека на истите има порнографски материјал со деца.

Понов медиум којшто е во прилог на овој криминалитет се т.н. Chatrooms, или „соби за разговор“. Овој разговор е вистински, директен, помеѓу две или повеќе лица. Истиот се одвива во виртуелна соба за разговор.¹⁷⁷ Секој од учесниците има свој псевдоним. Овој разговор е сличен на телефонскиот во тоа што неговата предност е што можат симултано да учествуваат повеќе луѓе, или групи.

Instant Messaging (IM) е сличен медиум на претходниот и се состои во праќање и добивање на пишани пораки. Разликата со претходниот медиум е во тоа што овде примачот на пораките мора да се согласи со трансферот на пораки со одредено лице.¹⁷⁸

3.3.Ddos Attack и Botnet

Постои варијација на DoS, наречена „дистрибуирано негирање на услугите“ (или ДДОС), којшто го практикува својот напад од различни фокуси, значително зголемувајќи ја заситеноста на серверот. Вообичаено, т.н. *ботнет* ги извршува овие напади против а систем, со оглед на нејзината умерена сложеност, и фактот дека тие дејствуваат автоматски и автономно.

Од друга страна, треба да се разјасни дека тие можат да имаат конструктивна цел, бидејќи служат за верификување на границите на трансфер на информации на компјутер,

¹⁷⁶Ferraro, M., Casey, E., McGrath, M.: INVESTIGATING CHILD EXPLOITATION AND PORNOGRAPHY: THE INTERNET, THE LAW AND FORENSIC SCIENCE, Elsevier AcademicPress, 2005, 9.

¹⁷⁷ Факултативен протокол кон Конвенцијата за правата на детето кој се однесува на продажба на деца, детска проституција и детска порнографија Службен весник на РМ бр.44/2003 година, 11.

¹⁷⁸ На пример Candyman E – group на 14.04.20 на 17:00 часот.

за да можат да се воспостават пред да понудат производ или услуга на потрошувачите, со што се избегнуваат потенцијални нарушувања како што се губењето на информации и неочекувани прекини во комуникацијата.

DoS може да се претстави на различни начини, бидејќи постојат многу техники за да се генерираат, сепак, тие ја делат протоколната група TCP/IP за да ја исполнат својата цел.¹⁷⁹

Еден од овие напади е како што следува:

1. меморија за складирање, капацитет за обработка и ширина на опсег на еден, или на повеќе компјутери, се троши против волјата на нивните сопственици;¹⁸⁰
2. неговите податоци за конфигурација се модифицирани, почнувајќи од површина до оние што ја загрозуваат стабилноста на опремата;¹⁸¹
3. работата на некои уреди е прекината;¹⁸²
4. комуникациски канали што би овозможиле погодни корисници да се поврзат со давателите на услуги што се одземени или променети.¹⁸³

DDoS во основа е напад со брутална сила, што значи дека е напад на уред од повеќе други уреди во исто време. Таа работи така што се обидува да формира толку многу врски со целта, и да ги поплави со информации дека е преоптоварен и паѓа, па оттука и терминот „негирање на услугата“.

Со извршување на нападот и кршењето на¹⁸⁴ уредот, сајбер криминалот ја негира услугата на тој уред на други луѓе кои сакаат да го користат. Иако тоа е значајно, исто така треба да се забележи дека сајбер-криминалците, исто така, ги насочуваат и веб-сајтовите на поединци.

¹⁷⁹ Факултативен протокол кон Конвенцијата за правата на детето кој се однесува на продажба на деца, детска проституција и детска порнографија Службен весник на РМ бр.44/2003 година, 10.

¹⁸⁰ Со чл.1 од Законот за изменување и дополнување на Кривичниот закон (Сл.Весник на Р.Македонија бр. 7 од 15.01.2008 година) е додаден нов став 21 кој со Законот за изменување и дополнување на Кривичниот закон (Сл. Весник бр.114 од 14.09.2009 година) преминува во став 24 на 14.04.20 на 17:00 часот.

¹⁸¹ Ibid, 37.

¹⁸² На пример Candyman E – group на 14.04.20 на 17:00 часот.

¹⁸³ <https://mk.erf-est.org/187-denegaci-n.html> на 06.04.2020 година во 14:25 часот.

¹⁸⁴ Надица Мирчевска, научен труд Сајбер тероризам – современ облик на тероризмот колку Република Македонија е ранлива од сајбер тероризам.

Во претходните денови, ова ќе биде главен извор на загриженост, но за среќа, сега има опции кои им помагаат на поединците да ги заштитат своите сајтови.

Постојат четири заеднички DDoS стратегии кои сајбер-криминалците ги користат за да се обидат да ги симнат веб-сајтовите. Сите тие се напад со брутална сила, тие се преплавуваат во голем број.¹⁸⁵

1. Напад на TCP поврзување. Обидете се да ги заземете сите достапни врски што постојат на вашата веб-страница. Ова ги вклучува сите физички уреди кои служат на вашиот сајт, како што се рутери, firewalls и апликациски сервери. Физичките уреди секогаш имаат ограничени врски.
2. Волуметриски напади, поплави мрежа на вашиот сајт со податоци. Ова работи со надминување на вашиот сервер, или дури и со преземање на сите расположливи елементи на вашиот сервер. Размислете на тоа како на поплава, или на сообраќаен метеж, каде што ништо не може да се движи.
3. Напади за фрагментација. Испрати битови и парчиња, повеќе пакети на податоци на вашиот сервер. На овој начин, вашиот сервер ќе биде зафатен, обидувајќи се повторно да ги собере и да не може да се справи со ништо друго.
4. Напади на напади. Посебно се стремите кон еден аспект, или услуга што ја имате. Овие се поопасни, бидејќи со ограничено таргетирање, можеби нема да сфатите дека сте нападнати, додека не се уништи нешто.

Дистрибуиран напад за демант на услугата (DDoS) е злонамерен обид да се наруши нормалниот сообраќај на таргетираниот сервер, услуга, или мрежа, со преплавување на целта или околната инфраструктура со поплавување на интернет-сообраќај. Нападите на DDoS постигнуваат ефективност со употреба на повеќе компромитирани компјутерски системи како извори за напад на сообраќајот. Експлоатираните машини можат да вклучуваат компјутери и други мрежни ресурси, како што се IoT уреди.

DDoS заштита

Ако сте сопственик на мал бизнис и сте загрижени за вашата веб-страница што се наоѓа под напад, вие сте со право.

¹⁸⁵ а <http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal-na-25.04.20> г во 17:30 часот.

Секоја форма на напад е опасна, а не, да се каже DdoS. Таа има потенцијал да предизвика не само финансиска штета, туку и оштетување на брендот.

Имате многу опции за да можете да се заштитите себеси, па ајде да погледнеме во некои основи:

1. Користете прокси заштита. Прокси е тампон којшто го штити вашиот веб-сајт од интернет, нешто како ограда. Ова нуди дополнителен слој на заштита што може да послужи за да ви даде однапред предупредување за дојдовен напад. Таа, исто така ја крие вашата вистинска IP адреса, иако сето ова е невидливо за вашите легитимни веб-страници.
2. Заштита од загрозените IP адреси. Сајбер-криминалците сакаат да ги кријат своите вистински IP адреси со киднапирање на други, за нивна сопствена употреба. Многу популарни адреси можат да бидат заштитени со одржување на листата за контрола на пристап (ACL) за блокирање на пристапот од одредени IP адреси.
3. Има режим *пропусен опсег*. Иако пропусниот опсег е скап, многу домаќини денес нудат скалабилни планови кои може да ви помогнат.¹⁸⁶

Ботнет се однесува на група компјутери кои биле заразени од малициозен софтвер и биле под контрола на злонамерен глумец. Терминот ботнет е портманте од зборовите *робот* и *мрежа*, и секој заразен уред се нарекува бот.

Баскетите можат да бидат дизајнирани да постигнат нелегални или злонамерни задачи, вклучувајќи испраќање спам, крадење податоци, откупи на софтвер, измама со кликување на реклами, или дистрибуирани напади за негирање на услуга (DDoS).

Додека некои софтвери, како што е ransomware, имаат директно влијание врз сопственикот на уредот, малициозниот софтвер DDoS ботнет може да има различни нивоа на видливост. Некои малициозни софтвери се дизајнирани да преземат целосна контрола врз уредот, додека други малициозни софтвери работат тивко како процес во позадина, додека тивко чекаат за инструкции од напаѓачот, или од „стадација“.

¹⁸⁶ https://en.wikipedia.org/wiki/Denial-of-service_attack на 07.04.2020 година во 15:30 часот.

Саморазмножувачките ботнети регрутираат дополнителни ботови преку различни канали. Патиштата за инфекција вклучуваат експлоатација на ранливости на веб-страницата, злонамерен софтвер со тројански коњи и напуштање на слаба автентикација, за да се добие далечен пристап.

Откако ќе се добие пристап, сите овие методи за инфекција резултираат со инсталирање на малициозен софтвер на целниот уред, овозможувајќи далечински управувач од операторот на ботнет. Откако уредот е заразен, може да се обиде да го самопропагира малициозен софтвер на ботнет со регрутирање на други хардверски уреди во околната мрежа.

Ботовите често вклучуваат елементи на вештачка интелигенција. Типично, ботовите извршуваат едноставни и структурно-повторувачки задачи, со многу поголема брзина од човекот.

Најголема примена ботовите имаат во веб-индексирањето, при кое, автоматска скрипта презема, анализира, и сместува информации од веб-сервери со многу поголема брзина од човекот. Повеќе од половината од веб-сообраќајот произлегува од ботовите.¹⁸⁷ Серверите кои хостираат мрежни места им се спротивставуваат на ботовите на различни начини. Серверите може да изберат да имплементираат поддатотека со правила на однесување на интернетските ботови robots.txt. Оваа поддатотека е текст којшто ги наведува важечките правила за однесување на ботовите на тој сервер.

На секој бот кој комуницира со сервер, а кој не ги следи наведените правила, теориски, ќе му биде одбиен пристапот, или ќе биде отстранет од афектираното мрежно место. Доколку имплементирањето на текстуалната поддатотека е единствената мерка без поврзување со одреден програм/софтвер/апликација, тогаш придржувањето до наведените правила е целосно доброволно и реално не постои начин истото да се обезбеди, дури и да се осигура дека творецот или имплементаторот на ботот да ја прочита содржината на текстуалната поддатотека. Некои ботови се „добри“, на пример

¹⁸⁷ Ботнет: вистински ризик <https://www.it.mk/botnet-vistinski-rizik/> на 06.04.2020 г во 14:00 часот.

индексерите на пребарувачите, додека други може да се користат за злонамерни напади, особено во политички кампањи. Иако е невозможно да се посочат точниот број на ботови во одреден ботнет, проценките за вкупниот број ботови во софистициран ботнет се движат во големина од неколку илјади, до поголеми од милион.

Интернет ботот се интегрира на веб-локациите, при што со мрежата се однесува како со човек. Најчесто се применува за реклами или спамови, но и за корисни работи како што се техничка поддршка на корисниците, помош при телеобразование, итн. Едни од најзастапените интернетски ботови се чет-ботовите и спам-ботовите.

Чет-бот

Чет-ботот се обидува подржува чет-партнер. Постојат добронамерни и злонамерни чет-ботови. Добронамерните обично се користат како техничка поддршка за одредено мрежно место, односно производ, за да му се помогне на корисникот полесно да дојде до саканата информација. Скоро секогаш истите се претставуваат како бот за да му свртат внимание на корисникот дека разговара со машина. Значајна им е употребата во образованието каде што може да преземе улога на инструктор, или предавач. Злонамерните чет-ботови обично не сакаат да бидат откриени дека се машини, туку сакаат корисникот да мисли дека разговара со човек. Овие ботови главно имаат за цел да рекламираат одредена веб-локација и корисникот да го упатат на неа. Најчесто се појавуваат на веб-чет локациите или во вид на банер на одредени мрежни места.

Спам-бот

Спам-ботот спаѓа во категоријата штетни софтвери и може да служи за реклама на одредена веб-локација, односно производ, или за цел да има да ѝ наштети на одредена интернет-страница, корисник, или група корисници.

Може да прави автоматски налози на одредена интернет-страница, најчесто на форуми, и да остава голем број на пораки.

Тие пораки може да имаат за цел да рекламираат одредена веб-локација, односно производ, или да имаат задача да ја нарушуваат нормалната дискусија меѓу корисниците, така што ја прават помалку разбирлива и со тоа да ѝ го наруши рејтингот на таа страница.

Како една од најдобрите заштити од спам-ботови се користи капча (англиски: captcha), со која се одредува дали корисникот е човек или бот.

Играчки бот

Играчкиот бот се користи во компјутерски игри, каде поддржува противник на играчот. Добро познати примери се компјутерскиот шах и стратешките игри со повеќе противници. Исто така, широка примена имаат во тимските игри, односно кога на тимот му недостасува играч, ботот ја презема неговата улога.

Партиски бот

Во преносно значење, партиски ботови се нарекуваат членовите на политички партии (обично оние пониските), кои за мал надоместок пишуваат афирмативни коментари во корист на својата партија или нејзиниот лидер на оние веб-портали кои користат антибот проверки (капчи). Ваквите активности се најизразени во текот на предизборните кампањи.¹⁸⁸

3.4. Phishing (фишинг)

Фишингот е облик на измама кој опфаќа збир активности на неовластени корисници преку користење лажни пораки од е-поштата, и лажни веб страници на поголем дел од финансиските организации, обидувајќи се од корисниците да добијат доверливи лични податоци како што се ЕМБГ, корисничко име, ПИН броеви и сл. За жал, голем е бројот на корисници кои не се запознаени со овој вид на измама. Штом еднаш ќе дојдат до доверливите податоци, злонамерните испраќачи или сами ги користат, или ги продаваат. Во пораките најчесто се повикуваат на лажни веб страни, кои според изгледот целосно одговараат на веб-страниците на легитимните компании (фирми). При нападите на

¹⁸⁸ Zeifman, Igal. „Bot Traffic Report 2016“. Incapsula. На 06.04.2020 година во 14:05 часот.

рибарее се користи социјално инженерство и технички трикови, за да се украдат личните и финансиските податоците на корисникот.

Најчесто се користи е-поштата за да се наведат клиентите да посетат лажни мрежни места кои го имитираат изгледот на легитимни брендови, како банки и компании за е-малопродажба, или кредитни картички. Сличен е резултатот и кога се вршат измами преку системи за директен разговор (chat).

Шемите на техничките трикови претставуваат вметнување на криминален програм (crimeware) во компјутерот на жртвата за да се украдат податоците директно, често користејќи шпиунски програми, т.н. тројански коњи, со коишто се следи она што корисникот го пишува на тастатура (spyware, trojan horse, keylogger).¹⁸⁹

Фарминг-криминалните програми погрешно ги наведуваат интернет корисниците на лажни сајтови или прокси-сервери, типично, преку т.н. киднапирање на ДНС.

Меѓу сајтовите што биле погодени од вакви измами (scam) се и Yahoo, Microsoft, AOL, eBay, Paypal, Hotmail, Earthlink, Barclays iBank, Citibank, Halifax, Nat West Bank-Nationwide, MSN, FDIC (Federal Deposit Insurance Corporation), Lloyds TSB, AT&T, Fleet Homelink и US Bank. Некои од овие мрежни места ги нарекуваат фалсификати, измамнички, или сикривоколчени (spoof email) елементи.

Измамниците, овие пораки ги дистрибуираат како спам (spam), односно преку праќање пораки до масовни листи, без разлика на тоа дали примателите се корисници на одреден легитимен сајт чијшто идентитет се злоупотребува, или не се злоупотребува.

Тоа е поим што се користи кога се работи за присвојување на идентитетот на легитимна организација или на мрежно место, употребувајќи фалсификувана е-пошта, односно е-пошта и/или мрежна страница, со цел да се убедат корисниците да ги споделат своите кориснички имиња (usernames), лозинки (passwords) и личните податоци (име,

¹⁸⁹ https://dzlp.mk/mk/fising_na_25.04.20 г во 17:30 часот.

броеви на кредитни картички, матични броеви или броеви за социјално осигурување), за тие да бидат злоупотребени.

Ова се вика и кражба на идентитет. „Phishing“ е релативно нов термин, употребен во некои извештаи уште во 1996-та година, а во медиумите е споменат во 1997-та година.

Поголемиот дел од рибарските измами се состои од фалсификувана е-поштенска адреса, која е поврзана со фалсификувана мрежна страница или место.

Текстот на пораката ве наведува да пополните основна процедура со користење на врска, која отвора лажно мрежно место.

Таа основна процедура, покрај другите работи, вклучува потврдување на бројот на вашата сметка, информации за невалидни кредитни/дебитни картички, обид за киднапирање на вашата сметка, награди, суспендирање на вашата сметка итн. Во многу случаи е-пораката го вклучува и вирусот *црв*, како на пример Mimail worm.

Измамниците често користат дупки кај програмите за пристап на интернет, како „бубачката“ во разгледувачот интернет експлорер, која додека Мајкрософт не ја запре во февруари 2003-та година, овозможи огромен број на измами преку прикажување на лажна адреса на тековната страница.¹⁹⁰

Фалсификуваните, односно лажните мрежни места обично содржат формулар што треба да им ги обезбеди потребните информации на скемерите, за тие да направат измама. Ова обично значи злоупотреба на кредитните/дебитните картички на жртвите за отворање онлајн-сметки и киднапирање онлајн-сметки, со цел да украдат одредена сума на пари.

На овој начин на корисниците на eBay им беа украдени сметките, додека скемерите ги искористуваат сметките за понуда на скапи работи, односно добиваат и наплатуваат порачки од купувачи, но стоката никогаш не ја испорачуваат. На други жртви им бил уништен кредитниот и финансискиот статус (credit score) кога нивниот идентитет

¹⁹⁰ Фондација Метаморфозис, "ИКТ Водич бр.4: Безбедност на информациите и зошто да се заштитиме, 25.

бил употребен за собирање финансии, а некои жртви, пак, виделе дека некој ги искористил нивните кредитни или дебитни картички за онлајн-купување на стоки.

Најчести форми на фишинг се:

1. Лажно предупредување од банката или од друга финансиска организација во која од корисникот се бара да ги наведе личните податоци за да спречат да не дојде до укинување на сметката.
2. Измами од аукциски веб страни во кои корисникот се убедува да уплати одредена сума на пари за да купи одреден производ, а всушност корисникот мислејќи дека купува некој производ, врши уплата на лажна сметка.
3. Лажна порака од администраторот во која се бараат податоци од корисникот, како што е и лозинката.
4. Разни известувања во кои се обидуваат да изнудат пари за лажни добротворни цели.
5. Пораки со кои се намамува корисникот да уплати одредена сума на пари на лажна сметка (на пример, порака за драстично намалување на цената на одреден производ кој може да се купи само на интернет).
6. Пораки кои Ве известуваат дека сте добиле лотарија и дека им се потребни вашите лични податоци за да може да ја подигнете наградата.

Како да препознаете фишинг порака?

Измамниците често го копираат визуелниот изглед на вистинските веб страни на банките и на другите компании.

Во последно време лажните пораки се во целост идентични со оригиналите, меѓутоа постојат одредени детали кои ја откриваат измамата:

1. Правописни и граматички грешки;
2. Се бараат лични податоци;
3. Се бара инсталирање на програма за која се тврди дека ќе го поправи пронајдениот сигурносен пропуст;
4. Лажни линкови и пораки;
5. Некористење на SSL и дигитален сертификат;
6. Содржината на пораката е HTML образец;

7. Нереални ветувања;
8. Грешки во предметот на пораката;
9. Се бара итен одговор;
10. Не гласат на одредена личност.

Мотив на измамникот

Кога измамниците ќе дојдат до личните податоци на корисниците, тие ќе ги искористат на различни начини.

Иако некои ќе се задоволат со фактот дека го измамиле корисникот, најголем број од нив ќе сакаат да извлечат финансиска корист.

Ако измамникот дојде до броевите на кредитните картички или банкарските сметки, може истите сам да ги искористи, или да ги продаде информациите на други. Исто така, и помалку чувствителните податоци (како што се е-поштите, името, ЕМБГ) можат да се искористат и да се продадат на заинтересираните страни.

Како да се заштитите од фишинг?¹⁹¹

1. Никогаш не одговарајте на е-поштите кои бараат лични податоци. Финансиските институции ги имаат вашите податоци, а мала е веројатноста некоја реномирана компанија да ви ги побара личните податоци по пат на е-пошта;
2. Никогаш не ги следете (не кликувајте) сомнителните веб страни. Најчесто таквите линкови се дел од некој сомнителна е-пошта;
3. Никогаш не ги следете линковите ако не сте сигурен кој ги испратил. За оваа цел корисно е да се употребува дигитален потпис;
4. Користете програм за филтрирање на спам. Овие програми ги намалуваат несаканите пораки, кои најголем број од корисниците ги добиваат секојдневно;
5. Користете антивирус програма. Овие програми ги препознаваат малициозните софтвери кои исто така можат да се користат за собирање на лични податоци;
6. Користете личен firewall за да можете да го следите сообраќајот на интернетот во две насоки и да имате увид на евентуалните сомнителни активности;

¹⁹¹ <https://dzlp.mk/en/node/2173> на 25.04.20 г во 16:30 часот.

7. Користете antispyware софтвер;
8. Редовно ажурирајте го софтверот којшто го користите;
9. Следете ја состојбата на вашата сметка;
10. Користете добри лозинки, и често менувајте ги;
11. Проверете дали веб страната користи HTTPS протокол. Веб-адресите на финансиските институции би требало да почнуваат со: <https://> наместо <http://>
12. Бидете во тек, следете ги информациите за интернет, фишинг.

3.5 Scam

Измама е термин што се користи за да се опише секој измамен бизнис, или шема што зема пари или друга стока од несомнено лице. Со тоа што светот станува сè поповрзан благодарение на интернетот, измамите преку истиот се зголемија, а честопати зависи од вас дали може да ви се помогне да останете претпазливи со непознатите луѓе на интернет.

Денес има илјадници видови на измами поврзани со компјутерите и со интернетот, но повеќето се сведуваат на крадење пари, на имот или на информации. Подолу е прикажан преглед на вообичаени измами.¹⁹²

Ова може да се претстави со пример:

Станува збор за таканаречен wangiri scam, поим што потекнува од Јапонија, што во буквален превод значи „пушти да свони еднаш и прекини ја врската“ (one ring missed call). Се работи за измама од лица кои повикуваат од непознат број од странство, и веднаш ја прекинуваат врската штом засвони телефонот. „Жртвата“ ќе забележи само пропуштен повик на својот телефон.

„Измамниците“ се надеваат дека жртвата ќе им одговори, а кога ќе се случи тоа, жртвата слуша тон на бирање, или некоја снимка за да може разговорот да трае што е можно подолго. Жртвата врти на скапиот странски број, а трошоците за секоја помината

¹⁹² <https://www.computerhope.com/jargon/s/scam.htm> на 07.04.2020 година во 16:00 часот.

минута се зголемуваат. Колку подолго трае повикот, толку и телефонската сметка ќе биде повисока.

За да се заштитите од ваква евентуална измама, најдобро е да не одговарате на повикот и да не своните на непознати броеви од странство. Исто така, може и да се блокираат повиците од странство, а ова е особено корисно ако често ви случува да добиете вакви пропуштени повици од непознати лица

„Не постои друга мерка за заштита на крајните корисници, освен едукација и подигање на свеста за можните измами. Не постои ниту пак софистицирано техничко решение што операторите би можеле да го имплементираат за да може автоматски да спречат вакви појави. Единствено, системите за детекција на измами (fraud detection system) што ги имаат имплементирани операторите им овозможуваат рано откривање на ваквите појави и операторите преземаат мерки, како што е блокирање на серија броеви од коишто потекнуваат ваквите напади. Поради тоа и благодарение на брзото дејствување на операторите, за релативно кратко време поголем број од нападите беа спречени. Некои од операторите излегоа со свои информации за јавноста со коишто ја информираат истата да биде внимателна со ваквите пропуштени повици и да не се јавува“, велат од Агенцијата за електронски комуникации (АЕК) за МИА.

За оние корисници коишто веќе се јавиле на пропуштените повици, и во наредниот период ќе добијат повисоки сметки за електронски комуникации, од АЕК советуваат да се обратат до операторите и да поднесат приговор, бидејќи претходно операторите ги коригирале ваквите сметки по поднесен приговор.

Како што пишува МИА, повиците во земјава најчесто потекнуваат од Литванија, Естонија и од сателитскиот оператор Глобал стар. По преземените мерки за заштита од страна на операторите, како што се наведува, неколку часа по повиците беа блокирани најголем дел од броевите преку коишто се остваруваше ваквата измама, но, како што

предупреди АЕК, тоа не значи дека ваквата измама нема да се повтори од други броеви во иднина.¹⁹³

3.6. Ransomware

„Ransomware“¹⁹⁴ е вид на компјутерски вирус којшто ги заклучува или ограничува компјутерските хард-дискови сè додека не се исплати одредена сума (откуп) на илегална организација. Во Мај 1996 година Adam Young од Универзитетот во Колумбија презентирал документ Cryptovirology-extortion-based security threats and countermeasures на IEEE’s Security and Privacy symposium. Тој го опишал развојот на првиот прототип на ransomware. Од моментот на појавата на тој иновативен документ во 1996 година, истражувачите имаат опишано многу сценарија за појавата на овој malware. Еден од првите познати malware-и од фамилијата ransomware е Gpcode.ak, се појавил во 2008-та година. Malware-от има криптирано огромен број на фајлови на компјутерите на жртвите.

Ransomware е вид на малициозен софтвер којшто ги спречува или им го ограничува пристапот на корисниците до оперативниот систем. Овој вид на малициозен софтвер ги принудува жртвите да платат откуп преку соодветни електронски начини на плаќање, за да им овозможат пристап до нивниот оперативен систем, или враќање на нивните лични информации. Овие малициозни софтвери се најсериозната закана за персоналните компјутери досега.

Еден од најпознатите malware-и од фамилијата ransomware е CryptoLocker кој се има појавено во Септември 2013-та година. Дека станува збор за малициозна програма која е во пораст говорат и статистиките каде што активноста на ransomware во првото тромесечје од 2015-та година е зголемено за 165%. Особено забележливо е дејствувањето на оние вируси од фамилијата на CTB-Locker, со новите верзии на CryptoWall,

¹⁹³ <https://biznisinfo.mk/shto-e-wangiri-scam/> на 07.04.2020 година во 16:30 часот.

¹⁹⁴ https://www.gsws.com/downloads/knowb4/WhitePaper_Ransomware_KnowBe4.pdf на 25.04.20 г во 20:00 часот.

TorrentLocker и BandarChor. Исто така, во првото тромесечје од 2015-та година е забележан и нов вид на вирус од таков тип наречен Teslacrypt.¹⁹⁵

Овие видови на ransomware во најголема мера напаѓаат жртви од богатите земји, затоа што корисниците од овие земји се подготвени да платат поголема сума на пари.

Новата технолигија во последните неколку години го има направено ransomware многу моќен вирус, што се гледа преку следните карактеристики на истиот:

1. Виртуелен начин на плаќање. Користејќи виртуелен начин на плаќање, изнудувачите го избегнуваат традиционалниот начин на плаќање со цел да не остават некаква трага при трансферот на парите;
2. Tor network. Користејќи tor network, напаѓачите можат многу полесно да ја сокријат локацијата од каде што го контролираат серверот, односно од каде што и ги продаваат клучевите на жртвата. Овој вид на мрежа овозможува криминалната инфраструктура да се одржува долг период, па дури и да се изнајмува на други напаѓачи;
3. Можноста вирусот да се пренесе и на мобилен телефон: Во Јуни 2014-та година за првпат е откриен вирус од фамилијата ransomware кој ги има криптирано податоците на уредите со андроид систем;
4. Истиот, со помош на AES енкрипција ги криптира податоците на мемориската картичка на телефонот, и преку Tor, SMS и HTTP се поврзува со напаѓачот;¹⁹⁶
5. Заразување на различни уреди за складирање на податоци. Во Август 2014 година Synolocker почнал да ги таргетира мрежите на кои се имаат приклучено уреди за складирање на податоци. Malware-от искористувајќи ја ранливоста на овие уреди, од далечина, ги криптира податоците користејќи RSA 2,048-bit keys или 256-bit keys.¹⁹⁷

3.7. Cyberbullying

Интернет-злоупотребата или сајбер-злоупотребата е форма на малтретирање, или на вознемирување со користење на електронски средства. Интернет-злоупотребата и сајбер-злоупотребата се под терминот „малтретирање преку интернет“. Ваквата практика

¹⁹⁵ Извор: McAfee Labs, 2015 на 25.04.20 г во 17:00 часот.

¹⁹⁶ <http://www.removevirustoday.com/hr/Ransomware/Kako-ukloniti-ctb-locker-ransomware-20150305.html> на 25.04.20 г во 17:30 часот.

¹⁹⁷ Извор: McAfee Labs, 2015 на 25.04.20 на 17:00 часот.

станува сè почеста, особено кај тинејџерите, бидејќи дигиталната сфера се шири, и технологијата напредува. Интернет-злоупотреба е кога некој, обично тинејџер, е малтретиран, или малтретира други на интернет и на други дигитални простори, особено на страниците за социјални медиуми.

Штетното однесување со малтретирање може да вклучува објавување гласини, закани, сексуални забелешки, лични информации на жртвите, или етикети со пејораторство (т.е. говор на омраза). Малтретирањето и вознемирувањето може да се идентификува со повторено однесување и со намера некој да биде повреден. Жртвите на компјутерски напади може да доживеат помала самоверба, зголемена самоубиствена идеја, и најразлични негативни емоционални реакции, вклучително и исплашени, фрустрирани, лути и депресивни субјекти.

Видови на интернет-злоупотреба кој се користи за Cyberbully:¹⁹⁸

1. Социјалното исклучување на интернет е еден вид сајбер-малтретирање. Социјалното исклучување може да биде една од најблагите форми на сајбер-малтретирањето, но тоа може да предизвика сериозни неволји. Тоа е онлајн-еквивалент на напуштање на неког од групата на која треба да очекуваат автоматско членство. Ова може да вклучува цела класа која не прифаќа барање за пријател од одреден соученик.

Совет: Фокусирајте се на развој на реални односи, а не на односи зависни од виртуелните односи за социјална врска. Ако вие или вашето дете сте онлајн исклучени, тоа веројатно е показател за посериозен социјален проблем во реалниот живот.

Разговарајте со родителите, наставниците, или со советник ако сте во социјална исклученост на училиште. Исто така, корисно е да се вклучите во групи на интернет или во реално време врз основа на вашите интереси, вашето хоби или вашите активности.

2. Означување без дозвола. Селектирањето е начин на прикачување на името на лицето на онлајн сликата, така што нивното име се појавува на сликата, или

¹⁹⁸ <https://mk.reoveme.com/5-%D0%B2%D0%B8%D0%B4%D0%BE%D0%B2%D0%B8-%D0%BD%D0%B0%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B7%D0%BB%D0%BE%D1%83%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%B0/> на 25.04.20 г во 17:30 часот.

сликите на одредена личност може да се идентификуваат со пребарување на обележани слики со нивното име.

Означувањето на некое име против срамно, обесхрабрувачко или манипулирано лице, особено без негова дозвола е форма на злоупотреба на интернет, особено кога намерата е да се предизвика тоа лице да биде вознемирено или исмејано.

Совет: Ограничете ги и цензурирајте ги вашите слики што ги поставувате, и сликите коишто другите ги објавуваат од вас. Прилагодете ги поставките за приватност на Фејсбук или на веб-страницата што ја користите, така што обележаните слики од вас нема да можат да бидат видени од други. Блокирајте ги луѓето да пристапуваат до какви било информации за вас. Ако вашата слика е објавена на веб-страница, контактирајте го администраторот на веб-сајтот и побарајте истата да се отстрани.

Ако сликата е порнографска, можеби ќе можете да ја пријавите злоупотребата во полиција, иако некои тинејџери се наоѓаат во неволја токму поради објавувањето на други нивни слики на интернет.

3. Честа е практиката на објавување на навредливи коментари за друго лице. Тоа може да вклучи и друга личност, на пример откривајќи дека е хомосексуалец, иако тој не се појавил на истата. Атентатот на карактер со прекршување на нечиј лик преку преувеличување на неговите перцепирани грешки на неизбалансиран начин, или пак објавување на неистинити информации за некого служи за да се оштети неговата слика, или неговата репутација.

Совет: Иако злоупотребата никогаш не е грешка на жртвата, може да ја намалите веројатноста дека тоа ќе ви се случи преку соодветно спроведување на интернет, избегнувајќи ги и предизвикувајќи ги негативните реакции кај други лица со коментари што ги објавувате, и третирајќи се себеси и другите со почит. Во најмала рака, секоја околност којашто ќе се случи ќе биде неоснована и неубедлива.

Ако тоа се случи, пријавете злоупотреба на сопственикот на веб-страницата. Веб-администраторите сè повеќе се свесни за злоупотребата на интернетот и имаат модератори кои можат да ги отстранат навредливите материјали.

4. Повторно објавување на Секс (Sexting) е ризична активност, но кога сте во врска, можете да бидете вовлечени во секцирање слика за себе на вашата сакана личност

без да размислувате за потенцијалниот иден ризик од неговото користење против вас. Помладите корисници на интернетот, особено тинејџерските девојки, исто така можат да бидат поласкани во секирачки слики од себе, или да „трепкаат“ на веб камера од предатори, педофили и порнографи кои можат да ги користат овие слики за сајберсекс. Ова е познато како принуда, и е форма на злоупотреба на интернет.

Вие може да се чувствувате засрамени од такви слики кои се објавени за вас, но тоа не е ваша вина. Замовете ги администраторита да ја симнат сликата надолу, а ако не се направи тоа, пријавете го на веб-страницата, како испратена без ваша согласност.

5. Импресорирање и кражба на идентитет. Активноста на преправање дека сте некој друг, може да биде очигледно исмејување, што всушност е позајмување или крадење на нечиј идентитет, како што е нечие име, слика или идентификација на информации, и да ги извршува дејствата кои и се припишуваат на жртвата.

Совет: За површни имиња од типот на објавување на глупав онлајн коментар користејќи го вашето име, додадете коментар подолу наведувајќи дека тоа не е направено од вас. За посериозни имитации, како коментари кои изразуваат контроверзни ставови со коишто не се согласувате, контактирајте го веб-администраторот и побарајте истиот да се отстрани.

Ако вашите лични податоци се користат за извршување на кражба или друго кривично дело, вие треба се соочите со виновникот за да го исправите предметот, или да го пријавите случајот во полиција.

Превенција од сајбер криминалот

Сајбер криминалот заради спецификите, општествената опасност што ја предизвикува и високиот раст којшто го има, во голема мера станува сериозен општествен проблем и тоа не само во национални, туку и во меѓународни размери. Врз основа на наведените причини потребна е соодветна акција заради успешно спротивставување на новото општествено зло.

Постојат три типа механизми кои можат да помогнат во одговор на предизвиците на сајбер криминалот: алатки за заштита, етика и закони.

Овие механизми имаат превентивен и репресивен карактер, при што во нивната примена изразена предност мора да им се даде на превентивните мерки, во однос на репресивните мерки. Тенденција за зголемување на овој облик на криминал покажуваат и некои статистички податоци.

Врз основа на податоците претставени од експертите на компанијата Sophos, во текот на 2007-та година биле откриени 6.000 заразени веб-страници, од кои 83% припаѓале на компании.¹⁹⁹

Бројот на имеил заканите има тенденција на опаѓање, но обратнопропорционално се зголемува бројот на меилови коишто содржат линкови кои водат до малициозни интернет страни.

Голем проблем во сузбивањето на сајбер криминалот претставува фактот дека цел на извршителите е сè што се поврзува на интернет, односно, освен персоналните сметачи, тука се вбројуваат и мобилни телефони, iPhone, iPod Touch, терминали, и други уреди кои се конектираат на интернет постојано, или повремено.²⁰⁰

Според одредени сознанија, постојат и обвинувања дека одредени држави се појавуваат како нарачателите на сајбер криминалот.

Врз основа на претходно изнесеното, може да се заклучи дека сајбер криминалот во иднина се повеќе ќе биде застапен во споредба со останатите видови на криминал.²⁰¹

Земајќи го во предвид претходнонаведеното, потребно би било превземање на следните мерки:

1. заради општествената оправданост и целисходност, како и заради следење на општествените трендови и приклучувањето кон западноевропските држави, потребно е забрзување на активностите за донесување и усвојување единствени основи за заштита на автоматизираниот информациски системи;

¹⁹⁹ <http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ostriji-zakoni-za-sajberkriminal-69298.html> на 25.04.20 г во 18:00 часот.

²⁰⁰ <http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ost> на 25.04.20 г во 18:00 часот.

²⁰¹ European Committee on Crime Problems, European Committee of Experts on Crime in Cyber-Space, Draft Convention on Cyber-crime, April 2000., <http://europa.eu.int> на 14.04.20 на 17:00 часот.

2. од аспект на заштитата, една од најважните активности на која би требало да се посвети посебно внимание е изградбата и развојот на етички норми и принципи во доменот на информатиката;²⁰²
3. ревизија на кривичниот закон и негово прилагодување на новите облици на опасно општествено однесување предизвикано од информациската технологија;²⁰³
4. нова систематизација и трансформација на телата, или на органите кои ја следат состојбата во оваа област, коишто извршуваат анализи на појавите, ги истражуваат причините, извршителите и методите. Воедно треба да се предлагаат соодветни мерки и акции за спречување, откривање, разјаснување и докажување на овие видови на кривични дела²⁰⁴

²⁰² Интернет старница <http://www.nezavisne.com/nauka-tehnologija/internet/Potrebni-ostriji-zakoni-za-sajberkriminal-69298.html> на 07.04.2020 година во 18:30 часот.

²⁰³ Интернет страница <http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal> на 07.04.2020 г во 18:30 часот.

²⁰⁴ Интернет страница <http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal> на 07.04.2020 година во 18:30 часот.

ГЛАВА ЧЕТВРТА

4. Идентификација и заплена на дигитални докази

Дигиталниот компјутерски доказ се состои од множество на посредни реални докази, од кои ниеден не смее да се исклучи поради било која причина. Доказите мораат да бидат потполни, меѓусебно да се потполнуваат (да се испреплетени) и да ја немаат таканаречената пукнатина за донесување на заклучок, односно за утврдување на цврст доказ. Криминалниот акт може да се изврши на било кој компјутер поврзан во локална или светска мрежа, независно од неговата географска положба.

Исто така компјутерот напаѓач географски може да биде лоциран во било која точка од Земјината топка. Парот нападнат компјутер - напаѓачки компјутер може да биде во границите на една држави, или пак да бидат сместени во различни држави. Тоа значи дека тие можат да бидат сместени во иста држава или во различни држави, односно форензичарите често се приморани да собираат дигитални докази во едни држави, а да ги прикажуваат на суд во други држави. Самиот тој факт налага да се воведат одредени правила за прибавување, дистрибуција и презентација на дигиталните докази коишто ќе бидат релевантни за сите држави. Во таа насока, IOCE ги дефинира општите принципи за хармонизација на методите и праксата при работата со дигитални докази меѓу народите коишто гарантираат прифатливост на дигиталните докази во една земја, иако тие се собрани во друга земја.

Светската судска практика ги прифаќа компјутерски генерираните и компјутерски меморираните докази под соодветно дефинирани услови. Овие услови мораат строго да се почитуваат, бидејќи трансформацијата на податоците од серија на кодирани битови во судски доказ е апстрактен процес којшто може да предизвика сомнежи кај судиите и поротата, и да ги доведе во прашање автентичноста и интегритетот на компјутерски генерираните судски докази. Тоа особено е изразено кај

судиите/поротата кои се неедуцирани во областа на информатичко-комуникациската технологија. Затоа, потребно е да постојат процедури за ракување и чување, како и прописи за собирање, аквизиција и анализа на дигиталните докази, независно на каков медиум тие се запишани. Не смее податоците да се менуваат, да се оштетуваат или да се манипулира со нив во било кој чекор од истрагата. Собирањето на докази започнува со реконструкција на хипотезата за случајот. Доказите треба да се собираат на местото на случување на криминалната случка (на сцената на злочинот), бидејќи тоа може да биде единствен директен контакт со реалните докази. Треба да се работи методично, полека и да се собираат клучните нешта. Користејќи ги заклучоците за случката, потребно е со критички поглед да се вратиме на поставената хипотеза, односно да си поставиме прашање, како лично ние би ги прифатиле тие докази ако се наоѓаме на спротивната страна.

Потребно е да ги пронајдеме причините за некавалитетниот доказ, односно да утврдиме зошто доказот не е квалитетен, каде се изгубил некој важен факт, како да се пронајде доказен материјал кој ќе ја пополни празнината, што да направиме ако таков материјал се пронајде, итн. Во оваа фаза од истрагата од иста важност се докажувањето и негирањето на доказот.

Заедничка одбрана во сите компјутерски ситуации, најчесто е тезата дека криминалниот акт никогаш не се случил, односно дека тоа е само нормална компјутерска аномалија, итн. Значи, потребно е да се соберат сите посредни докази од местото на криминалниот акт, и тоа не само оние докази за кои дигиталните форензетичари мислат дека треба да се соберат, туку и сè она што може потенцијално да индицира што се случило.

Во процесот на аквизиција генерално е потребно да се снимаат листата на датотеки и логоата како докази, дури и ако немаме никаква идеја што навистина се случило. Треба да се има секоја датотека која потенцијално може да содржи определен доказ во доказниот материјал, пред истата да се изгуби, или да се промени.

После иницијалната истрага (без заплenuвање на компјутерот) потребно е да се насочиме кон првобитната хипотеза, и да ја доградиме подетално со собраните докази. Голема веројатност постои да е испуштен некој значаен доказ, што претставува добар аргумент компјутерот да се заплени во текот на истрагата, но при тоа мораме да имаме на ум дека тоа не е секогаш лесно.

Дигиталниот доказ е посреден доказ. Но, секој од посредните докази кои заедно го градат доказниот материјал треба да се третира како директен доказ кој води кон непобитно докажување на криминалното дејание.

Сите посредни докази потребно е да се третираат како докази кои директно водат кон непобитно докажување на извршените криминални активности.

Тоа се сите важни и критички докази за конкретниот случај.

Дури во тој случај почнува изградбата на доказ без пукнатини, односно изградбата на необорив доказ.

Значи, потребен е голем посреден доказен материјал за да се изгради еден мал цврст дигитален доказ.²⁰⁵

4.1 Идентификација и заплена на дигитални докази на персонален, или на преносен компјутер

Компјутерската форензика е гранка на дигиталната форензика, чијашто цел е да се соберат, обработат, складираат и анализираат електронски докази обезбедени од компјутерски систем од одреден електронски уред на законит начин, со цел да се употребат во судска постапка. Најголем дел од дигиталната форензика се однесува на компјутерската форензика, бидејќи персоналните компјутерски системи се најмногу распространети, и најмногу се користени од страна на извршителите на компјутерски криминал.

²⁰⁵ <http://eprints.ugd.edu.mk/7084/1/CITYR%202012Korporaciska%20istraga%20na%20kompjuterski%20kriminalen%20incident.pdf> на 07.04.2020 година во 18:35 часот.

Компјутерската форензика всушност опфаќа обезбедување и собирање на дигитални докази (електронски докази) од компјутер, хард диск или од уред кој вклучува компјутер, или се смета дека може да создаде или да преработи дигитални (електронски) податоци.

Компјутерската форензика претставува научно истражување и анализа на електронските податоци коишто се зачувани на т.н. тврди дискови (hard disk), меморија, системски фајлови и други мемориски локации каде што се складираат и зачувуваат електронските податоци во компјутерскиот систем, и истите во една легална постапка се користат како несоборливи материјални докази пред суд.

Предмет на истражување на компјутерската форензика е моменталната состојба на компјутерските системи и уредите за складирање на електронски податоци. Тука спаѓаат персоналните компјутери, системи со елементарни компјутерски процеси, вградени мемории, како и статички мемории (USB флеш меморија). Компјутерската форензика опфаќа широк спектар на информации коишто компјутерскиот систем ги процесуира, како што се историјата на прелистувачот (бидејќи истата е зачувана на некоја мемориска локација), и сите тие трајно се зачувани на дискот. Историски гледано, последните две децении персоналните компјутери доживуваат револуција. Тие стануваат достапни за цивилните корисници и нивната комерцијална употреба расте, а со тоа и употребата на персоналните компјутери во криминални дела.

Компјутерската форензика започнува да се користи токму во овој период, бидејќи нејзината цел е собирање на електронски (дигитални) докази за користење во легална постапка за докажување на судските процеси.²⁰⁶ Денес компјутерската форензика се занимава со истражување на компјутерскиот криминалитет, а најчесто се користи во областите опфатени со вклучен компјутерски систем во оштетувањето, односно неовластено навлегување на компјутерскиот систем.

²⁰⁶ Интегралниот текст на процесните одредби од Конвенцијата за компјутерски криминал е даден како посебен Прилог 2 на овој Прирачник, 55.

Процесот на обезбедување и на собирање на електронските податоци се одвива на начин којшто најпрво пристапува до хардверот и прави негова слика, односно копија што треба да се анализира. Потоа компјутерскиот форензичар ги користи повратените податоци со т.н. recovery софтвер, односно компјутерски форензички алатки како што се EnCase, Digital Forensics Framework, ILOOKIX, FTK, Open Computer Forensics Architecture, CAINE, Volatility, MailXaminer, Oxygen Forensic, X-Ways forensics.

Постојат многу начини одредени податоци коишто се зачувани да се сокријат, енкриптираат, да се алоцираат во секторите од хард дискот кои не се видливи за оперативниот систем, или да се изменат или избришат. Овие електронски податоци се предмет на компјутерско-форензичко истражување. Ваков вид на податоци, конкретно за кривичното дело „оштетување и неовластено навлегување во компјутерски систем“ претставуваат логови од електронска пошта, војр комуникација (Skype, Viber, Facebook Messenger, Telegram, социјални мрежи...), слики, историја на пребарувачот и разни други документи кои го поврзуваат извршителот со кривично-правниот настан и жртвата.

Овие податоци може да се повратат од хард дискот и доколку биле избришани од хард дискот и од кеш датотеките на пребарувачот и на оперативниот систем. Начинот на повраќање најчесто е по принципот пребарување по клучен збор, или пребарување по вид на екстензија (.jpg, .pdf, .txt...).

Одредени фајлови имаат специфичен сет на битови на почетокот и на крајот на бараниот фајл, кој може да послужи за полесно пронаоѓање и враќање на тие фајлови доколку се избришани. Софтверските алатки за компјутерска форензика функционираат токму на овој принцип, тие всушност на хард дискот пребаруваат сетови од единици и нули, и кога одреден сет се поклопува со бараниот, тогаш утврдува дека на таа мемориска локација претходно бил зачуван бараниот фајл. Всушност, најголем дел од овие форензички алатки работат на тој принцип, вршат препознавање на веќе познати датотеки за кои е познат нивниот специфичен сет од единици и нули. Затоа и електронските докази уште се нарекуваат и дигитални докази, бидејќи се што се зачувува на меморијата се запишува дигитално со единици и нули.

После успешното враќање на податоците, одредени информации се анализираат, и се реконструираат одредени настани и активности кои се направени на компјутерот. Компјутерската форензика опфаќа широк спектар на анализа на компјутерски системи коишто се имплементирани во различни области (автомобилска индустрија, безбедносни системи, медицина, системи за контрола на летање, радарски системи и сл.). При секој инцидент, несреќен случај или криминален напад, од електронските докази кои ќе бидат обезбедени со компјутерската форензика може да се направи реконструкција за конкретниот настан со точно време и место.

Од компјутерот на автомобилот, во зависност од видот на автомобилот, постои можност да се утврдат неодамнешните дестинации каде што возилото престојувало, омилени локации, навигаски информации, дури (во зависност од компјутерскиот систем) може да се утврди кога и каде се вклучени/исклучени светлата, отворање/затворање на вратата на возилото, каде се наоѓало возилото кога бил вклучен/исклучен Bluetooth уредот и многу други информации. Компјутерските форензичари кои се занимаваат со компјутерска форензика во криминалистичкото истражување неопходно е да се водат согласно одредбите од Упатствата за електронски докази и дигитална форензика издадени од Советот на Европа.

Криминалистичката истрага опфаќа широк спектар на истражни дејствија и форензички активности коишто ги истражуваат компјутерските инциденти чекор по чекор, со цел пронаоѓање на вистината за конкретниот кривично-правен настан, истражните мерки и активности, криминалистичката полиција ги спроведува согласно законските прописи и интерни прописи од Министерството за внатрешни работи и во една легална постапка обезбедува материјални електронски докази врз кои се темели докажувањето на сторителите, и кривичното дело во кривичната постапка. При секоја криминална ситуација, односно криминален инцидент најпрво се изработува хипотеза за нападот, којашто ги разработува информатичките аспекти и како е извршено неовластеното навлегување во компјутерскиот систем, односно што точно се случило. Ова подразбира анализирање на сите можни сценарија за компјутерскиот напад, односно пронаоѓање на

причинско-последичната врска меѓу сторителот и жртвата, и алоцирање на мемориските локации кај жртвата и кај сторителот, секаде каде што има електронски траги, односно електронски докази, коишто во легална постапка согласно со одредбите од Законот за кривична постапка ќе бидат соодветно обезбедени и подигнати. Потоа, за посспецифичните облици за неовластено навлегување во компјутерски систем се изработува реконструкција на криминалниот инцидент што подразбира правење на симулација за конкретниот кривично-правен настан. При овој чекор потребно е форензичкиот тест-компјутер за симулација на нападниот компјутер да се конфигурира, што е можно поблиску до реалната конфигурација на компјутерот.²⁰⁷ Обезбедувањето, подигнувањето и собирањето на дигитални докази во една легална постапка, т.н. аквизација на дигитални докази е од круцијално значење за кривичната постапка, бидејќи за разлика од класичниот криминалитет, каде што материјалните докази се основата на докажувањето, кај компјутерскиот криминалитет се користат дигитално-форензички методи и техники од страна на специјализирани стручни лица од Секторот за компјутерски криминал и дигитална форензика коишто на законит начин ги обезбедуваат, складираат и собираат дигиталните докази согласно со Законот за кривична постапка и Упатството за електронски докази издадено од Советот на Европа.²⁰⁸ Во текот на кривичните постапки, само електронски докази обезбедени во легална постапка, Судот ги прифаќа како доказен материјал и затоа е неопходно при обезбедување на електронските докази да бидат почитувани законските правила и прописи, односно благовремено, стручно и легално докажување на кривичното дело и на неговите сторители. Улогата на докажувањето, без разлика дали се работи за кривична, граѓански или управна постапка, во суштина претставува круна на пресудувањето.²⁰⁹

²⁰⁷ <https://resources.infosecinstitute.com/computer-forensics-tools/> (пристапено 12 Октомври 2018) <https://www.greycampus.com/blog/information-security/top-twenty-trending-computer-forensic-tools> на 07.04.2020 година во 19:05 часот.

²⁰⁸ Electronic Evidence Guide, March 2013, Council of Europe, 18.

²⁰⁹ <https://www.vecernji.hr/techsci/alat-za-digitalnu-forenziku-vozila-po-prvi-put-predstavljen-u-hrvatskoj1170438> на 07.04.2020 година во 19:00 часот.

Целта на доказната постапка е да се создаде убедување во вистинитоста на она што се тврди, односно му се става на товар на обвинетиот, т.е. вистинитоста на обвинението, што е и предмет на обвинение.²¹⁰

4.2. Идентификација и заплена на дигитални докази на мобилен уред

Форензиката на мобилни уреди се занимава со истражување и анализа на податоците коишто можат да се обезбедат од мобилните уреди. Со појавувањето на смарт мобилните телефони и можностите коишто ги нудат, се зголемува и обемот на информации коишто форензиката на мобилни уреди може да ги обезбеди. Социјалните мрежи (Facebook, Instagram, Twitter, LinkedIn...) направија технолошка револуција и бројот на нивни корисници во светот постојано расте. Поголем дел од популацијата на светското население ги користи социјалните мрежи, а со тоа свесно и самоиницијативно ги постираат своите лични податоци, фотографии, комуникации и сл., коишто многу лесно можат да бидат злоупотребени.

Целта на форензиката на мобилни уреди е да се обезбедат, обработат и складираат електронски докази во една легална постапка заради докажување на конкретен кривично-правен настан.

Смарт телефоните претставуваат истовремено и компјутерски систем со сопствена меморија за зачувување на податоци, и додатна меморија (мемориски картици) на која што се зачувуваат голема количина на електронски информации од коишто форензичарот обезбедува електронски докази.

Со масовната употреба на социјалните мрежи преку смарт телефоните, пропорционално се зголемуваат и криминалните активности коишто се извршуваат со мобилни телефони.

Паметните телефони може да содржат и текст пораки (смс, ммс), контакти, е-маил пораки (Gmail, Yahoo), податоци за чат-комуникација (Viber, Instant Messenger), GPS

²¹⁰ Николоска, С., оп. цит., 113.

координати, фотографии и видео снимки, историја од веб пребарување, информации од социјални мрежи (facebook, twitter, instagram, linkedin...), податоци и документи зачувани на телефонот, музика, потсетник и календар, информации за тековна банкарска сметка, историја на e-banking, информации за движење по интернет (gmail account, my activity и сл.) и други информации.

Истражувањето на мобилните уреди е слично на форензичкото истражување на персоналните компјутери, бидејќи и мобилниот уред претставува компјутерски систем.

Почетоците на форензиката на мобилните уреди започна со истражување не мобилниот уред и фотографирање на податоците кои можат да послужат како доказ во доказната постапка.

Овој начин на истражување се покажа како неефикасен поради времетраењето на самото истражување, кое беше премногу долго. Со појавата на современите смарт телефони, каде што има голема количина на податоци (слики, видеа, контакти, чат-комуникација, социјални мрежи...), се појави потребата од брз и ефикасен начин на извлекување на информациите од мобилниот уред, а при тоа да се внимава истите да останат автентични и непроменети во понатамошна репродукција пред судските постапки.

Форензичарите за оваа намена почнаа да користат специјализиран софтвер за синхронизација и „back up“ на податоци од мобилните. Овој софтвер на почетокот можеше да врши запишување и читање на податоците кои беа зачувани во мобилните уреди, но како недостаток се појави тоа што не можеше да ги поврати избришаните информации. Овој проблем е решен со развојот на нов софтвер, т.н. „Flasher“ и „Twister“ кутија која работи на принцип на флешување на меморијата на мобилниот уред и враќање на избришани информации, но и кај овој софтвер имаше многу недостатоци, односно вратените податоци не беа автентични.²¹¹

²¹¹ Прирачник за компјутерски криминал / Марко Зврлевски, Спасенка Андонова, Владимир Милошески. - Скопје : OSCE, 2014, 22.

Третата генерација на софтвер за форензичка анализа на мобилни уреди е усовршен и овозможува автоматско пребарување на мобилниот уред и синхронизација со компјутер, враќање на избришани податоци како и отклучување на лозинки. Попознати софтверски апликации за оваа намена се iPhone Analyzer, BitPim, viaForensics Forensics, Cellebrite cloud analyzer, Mobile Internal Acquisition Tool (MIAT), TULP2G, Katana Forensics' Lantern Lite Imager.²¹²

4.3 Идентификација и заплена на дигитални докази од уреди кој поседуваат меморија

Hard disk drive (HDD, хард диск) претставува електромеханички уред кој содржи вртечки дискови и движечки глави за впишување/читање податоци. Дисковите имаат плочи во кои се запишани информациите, и податоците лесно можат да бидат избришани или повторно запишани, при што се зачувува структурата на дискот што ги прави одржливи на подолг временски период. Податоците се складираат на површината на плочата во т.н. сектори и патеки.

Патеките се концентрични кругови, а секторите се сегменти на патеката.

Податоците се складираат во хард дискот во вид на датотеки кои едноставно претставуваат „битови“. Програмите претставуваат датотеки и процесорот ги третира како такви за да може да ги искористи. Повеќето компјутери имаат барем еден хард диск, а има и многу компјутери со повеќе од еден хард диск. За поголемите компјутери, како што се main frame (мејн фрејм), нормално е компјутерите да имаат повеќе хард дискови.

Денес, освен компјутерот како што се CCTV (затворените ТВ системи), вообичаено е и музичките уреди да имаат хард дискови за да можат да сочуваат поголема количина на податоци.²¹³

²¹² Стратегии за заштита од компјутерскиот криминал (Computer Crime Prevention Strategies) Александар Петрушевски, 51.

²¹³ „Меморија и складирање на податоци“ Main frame компјутерите ги користат претежно големи компании или владини институции за извршување суштински апликации, обработка на опсежни податоци (на пример, статистички податоци) и обработка на трансакции, 62.

Solid-state drive (SSD) претставува уред за складирање на податоци којшто користи полупроводничка меморија, т.е. микрочипови кои содржат мобилни делови. Овој уред ги складира постојаните податоци со цел обезбедување пристап до нив на истиот начин како во случај на традиционалниот хард диск. Понекогаш се нарекува и solid-state disk, или електронски диск.

Во споредба со електромеханичките дискови, SSD се помалку чувствителни на физички удари, тивки се, со пократко време на пристап и поголема тајност, но имаат повисока цена. SSD-те употребуваат исти уреди за поврзување како и хард дисковите, па според тоа лесно се заменуваат во повеќето апликации.²¹⁴

CD/DVD/BD²¹⁴ дискови можат да содржат различна количина на податоци и обично се користат за складирање на музика, видео или компјутерски датотеки за употреба на различни уреди. На пример, DVD има исти димензии како и CD, а може да содржи седум пати повеќе податоци од истиот. BD е оптички диск за складирање податоци со капацитет, кој е и до десет пати поголем од оној на DVD.

Random Access Memory (RAM, меморија со произволен пристап) претставува форма на електронско складирање на податоци, иако најчесто се опишува како привремена форма за складирање на податоци коишто ги користат активните програми со цел побрзо да се пристапи до нив.

Процесорот бара податоци од RAM-от. Тие се обработуваат, и како такви се впишуваат во RAM-от. Ова се случува милиони пати во секунда.

Universal Serial Bus (USB) можат да се најдат на повеќето современи компјутери и овозможуваат едноставно додавање голем број на уреди на компјутерот, како што се глушецот, печатачи, надворешни складишта на податоци и мобилни телефони.

²¹⁴ CD – Compact Disc (компакт диск), DVD – Digital Versatile Disc (дигитален повеќенаменски диск), BD – Blu ray Disc (диск со син зрак), 90.

Во моментот ова е најчестиот метод за поврзување на надворешни уреди кон компјутерот. Во пракса постои можност за поврзување на повеќе од 127 уреди со еден компјутер преку користење на УСБ.

Леснотијата со којашто можат да се користат USB уредите, тие се истакнуваат како најчесто употребувани во многу дигитални форензични истраги/вештачења.

Во прилог ќе доставиме табела на статистички податоци за кривични дела и сторители за наведените кривични дела во период од 2017-2019-тата година.

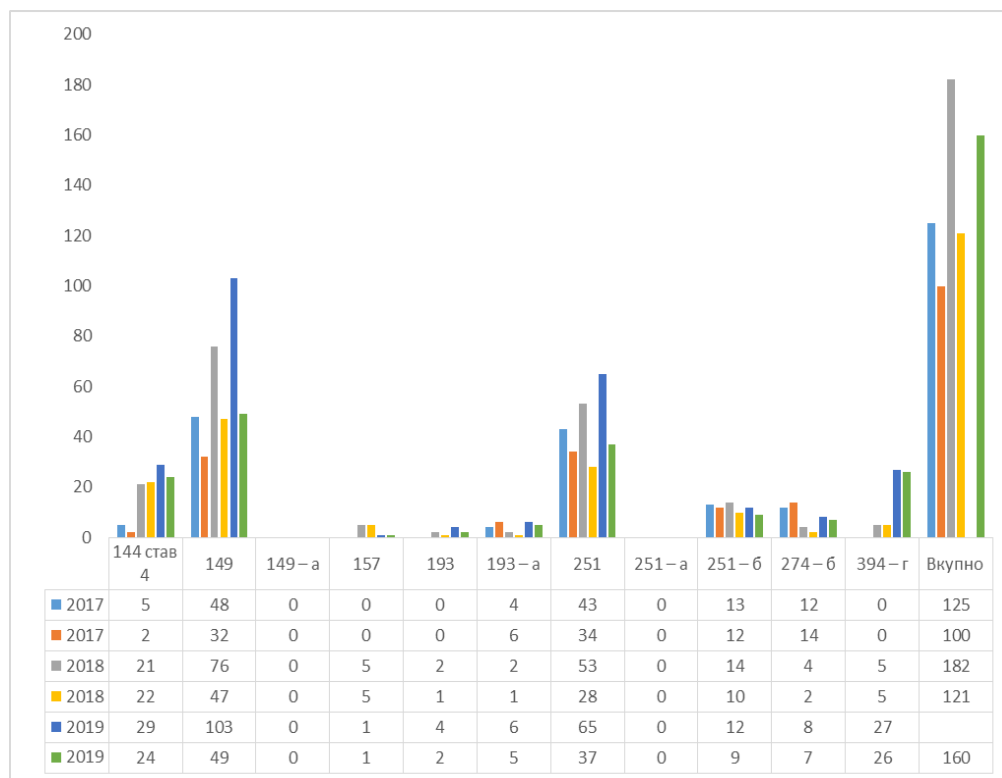
Овие податоци се земени од Министерството за внатрешни работи при СВР Тетово - Оддел за односи со јавност и стратешки прашања - Сектор за односи со јавност и протокол.²¹⁵

Членови од Кривичен законик		2017		2018		2019	
		К.Д	Сторители	К.Д	Сторители	К.Д	Сторители
144 став 4	Загрозување на сигурноста	5	2	21	22	29	24
149	Злоупотреба на лични податоци	48	32	76	47	103	49
149 – а	Повреда на авторско право и сродни права	/	/	/	/	/	/
157	Повреда на правото на дистрибутерот на технички посебен заштитен сателитски сигнал	/	/	5	5	1	1
193	Прикажување на порнографски материјал на	/	/	2	1	4	2

²¹⁵ Министерство за Внатрешни работи на Република Северна Македонија - Оддел за односи со јавност и стратешки прашања – Сектор за односи со јавност и протокол на 15.05.20 на 17:00 часот.

	дете						
193 – а	Производство и дистрибуција на детска порнографија	4	6	2	1	6	5
251	Оштетување и неовластено навлегување во компјутерски систем	43	34	53	28	65	37
251 – а	Правење и внесување на компјутерски вируси	/	/	/	/	/	/
251 – б	Компјутерска измама	13	12	14	10	12	9
274 – б	Изработка и употреба на лажна платежна картичка	12	14	4	2	8	7
394 – г	Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем	/	/	5	5	27	26
Вкупно		125	100	182	121	255	160

Табела бр. 1. Табела за кривични дела и сторители во врска со компјутерски криминал за периодот од 2017-та до 2019-та година



Графички приказ бр. 2. Кривични дела и сторители во врска со компјутерски криминал за периодот од 2017-та до 2019-та година

Заклучок

Под компјутерски систем се подразбира каков било уред, или група на меѓусебно поврзани уреди, од кои еден, или повеќе од нив, вршат автоматска обработка на податоци според одредена програма.

Со овој труд сакаме да докажеме дека граѓаните во нашата држава се идеални жртви за овој вид на криминалитет токму поради тоа што не се запознаени како функционира истиот, и не ги разбираат последиците, односно со истиот се запознаваат откако ќе станат жртви на овој вид криминалитет.

Сакаме да докажеме дека сторителите на овие кривични дела се сè потешки за откривање поради тоа што постои една позитивна врска помеѓу извршителите и новата технологија, а производителите на истата прибираат сè помалку податоци за нивните корисници, односно нудат сè поголема приватност за нивните потрошувачи, за што ќе биде разгледана статистиката од Министерството за внатрешни работи на Република Северна Македонија во временскиот период од 2016-та година до 2019-та година, каде што ќе се види колку пријави имаат поднесено граѓаните до нив, и колку дела од нив се расветлени, односно колку кривични пријави имаат поднесено до надлежните Јавни Обвинителства. Република Македонија не претставува исклучок од земјите кои зголемено се соочуваат со компјутерски криминал. Целта на Република Македонија е да биде дел од глобалната безбедносна мрежа во борба против перењето пари, организираниот криминал, финансирањето на тероризам и влегувањето на „валканите пари“ во економијата.

Нашата земја треба да преземе напори за да се заштити од различните криминални активности како што се кражба на личните податоци, високо-безбедносни тајни, воени планови и измамнички активности, т.е. „крадењето пари“ од кредитните/дебитните картички. Компјутерскиот тероризам и криминалните активности имаат видливо неповолно влијание врз земјата, т.е. врз нејзината економија, безбедноста на граѓаните, јавниот живот и човековите права и слободи.

Поради сите горенаведени причини, овој нов облик на организиран криминал треба да биде спречен од понатамошно ширење не само на нашата територија, туку и во целиот свет.

Компјутерскиот криминал е само општа форма преку која се изразуваат различните форми на криминални активности. Тоа е посебен вид на криминал насочен против компјутерските системи како целина, или еден дел, во различни начини, и со различни средства, со намера за себе или некој друг да се добие некоја корист, или да се предизвика штета на некој друг. Во споредба со традиционалните форми на криминал, компјутерскиот криминал брзо ги менува формите и облиците на манифестација, границите меѓу државите и видот на жртвата. Овие кривични дела се сокриени, често без видлива и блиска просторна врска помеѓу сторителот и жртвата. Најчесто е тешко да се открие, а уште потешко да се докаже. Долго време сторителите остануваат речиси непознати, додека оштетениот не претрпи штета којашто е видлива во компјутерскиот систем. Како што постојат големи можности за злоупотреба на компјутерите и информатичката технологија и се различни формите на можното противправно однесување, така постојат голем број класификации на кривични дела. Компјутерите и информатичката технологија може да послужи да се извршат традиционалните форми на криминал, но, исто така, и сосема нови форми на злоупотреба на компјутери, компјутерски системи и мрежи поврзани со криминал. Традиционалните форми на криминал вклучуваат компјутерска кражба, проневера, измама и фалсификат. Новите современи форми на компјутерски криминал вклучуваат специфични кривични дела што можат да се направат само со употреба на компјутери, компјутерски системи и мрежи. Ова се на пример, хакирањето, создавањето, и дистрибуцијата на вируси. Големите практични можности што се предвидени од страна на информатичката технологија, со себе носат ризик од ширење на масовната употреба на прислушувањето, кражба на деловни тајни, повреда на приватноста, но во последно време и на реалната закана од терористички напади. Компјутерска форензика е доказ од компјутер којшто треба да биде издржан, убедлив и доволен, за судот да може да го прифати.

Во форензичко-информатички постапки без разлика колку и да се внимателни луѓето кои имаат за цел да крадат електронски информации тие оставаат траги од нивните активности. Кога сторителите се обидуваат да го уништат доказот кој е на компјутерот тие позади себе оставаат траги. Во двата случаи може да се докаже дека овие траги може да се пронајдат и да се презентираат пред судот. Компјутерските форензички специјалисти прават повеќе од вклучување на компјутерот, листање на фолдери и пребарување на фајлови. Тие треба да бидат оспособени да извршат комплексни „evidence recovery procedures“, со вештина и експертиза која ќе го држи кредибилитетот на електронските докази пред судот. Употребата на научно изведени и докажани методи кон зачувување, собирање, валидација, идентификација, анализа, толкување, документација и презентација на дигитални докази добиени од дигитални извори со цел да се олесни или продолжи реконструкцијата на криминалните настани, или помагање за да се предвидат неовластените дејствија кои се покажале како неприфатливи за планираните операции, претставуваат операции на дигиталната форензика. Очигледно е дека информатичката технологија придонесува во современото општество безброј поволности, но исто така создала и низа проблеми и ризици кои многу порано не постоеле. Растечката зависност од информатичката технологија, која добива колосални размери, создала услови за настанување на бројни зони на осетливост со потенцијално многу сериозни консеквенци, кои можат да се протегаат поради губиток на контрола над нивната судбина, што укажува на фактот дека општествената заедница во сè поголема мера станува изложена на новиот феномен, ранливост во информатичката ера. Денес, повеќето држави веќе имаат суштински ресурси базирани на информатичката технологија. Оние кои тоа сè уште го немаат, прават сè за на овој план да создадат одредени резултати. Клучните сектори, како телекомуникациите, банкарството и финансиите, транспортот, електрична енергија, нафтата и гас, снабдувањето со вода, сервисите за вонредни ситуации и витални војни и цивилни операции, есенцијални за секојдневно успешно и непречено функционирање на економијата и државните органи, стануваат се позависни од оваа технологија.

Користена литература

1. Ачковски, Ј. Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012.
http://eprints.ugd.edu.mk/10870/1/Skripta%20za%20Sigurnost%20na%20kompiuterski%20osistemi,kompjuterski%20kriminal%20i%20terorizam_revJA_2.pdf,
2. Aleksić, Z., Škulić, M., Kriminalistika, Beograd, 2007, str. 46-63.
3. Australian Institute of Criminology, www.aic.gov.au
4. Bayuk, L. J., Healey, J., Rohmeyer, P., Sachs, H. M., Schmidt, J., Weiss, J., Cyber Security Police Guidebook, Wiley, 2012 <http://www.it-ebooks.info/book/2375>
5. Боцевски, Д., Советување за сајбер криминал – Компјутерски инциденти и истражување на компјутерски криминал во Република Македонија.
6. Petrović R. S., Kompjuterski kriminal, op. cit.
7. Petrović R. S., Kiberterorizam, Vojno delo, god. LIII, br. 2/2001, str. 100-122.
8. Petrović R. S., Neki aspekti nacionalne bezbednosti u informacionom dobu, Nauka, Tehnika, Bezbednost (NTB), Rad po pozivu, UDC: 681.324; 65.012.8, Godina XI, Broj 1, Septembar 2001, str. 7-27.
9. Светлана Николовска, Методика на истражување на компјутерски криминалитет, 2013.
10. Вlado Камбовски - Казнено Право општ дел, Скопје 2011.
11. Вlado Камбовски и Никола Тупанчевски, Казнено Право посебен дел, Скопје 2011.
12. Miliovanovic, Z., Kompjuterski kriminalitet I elektronsko piratstvo, Pravni Zivot, br-8-10/1991.

13. Separovic. Z., Kriminologija I socialna patologija, Zagreb, 1987.
14. Марко Зврлевски, Спасенка Андонова, Владимир Милошевски, Прирачник за компјутерски криминал.
15. Aleksic-Milovanovic- Kriminalistika, Beograd, 1994.
16. Boskovic.M- Kriminalisticka Metodika II-Beograd, 2000.
17. Parker.D, Computer Crime-Criminal Justice Resource Manual-Washington U.S, 1998.
18. Golubev. V, Cyber Crime Statistics in Ukraine, 2004.
19. Предраг Димитриевиќ - Компјутерски Криминал.
20. Милица Дракулиќ - Компјутерски Криминал.
21. Конвенција за компјутерски криминал – Совет на Европа, 2001.
22. Кривичен законик на РСМ.
23. Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computerrelated Crime, <http://europa.eu.int>
24. Cyberstalking, Anatomy of a Predator, www.cyberangels.org
25. Robinson J., Internet as the Scene of Crime, International Computer Crime Conference, Oslo, 2000., www.ccips.org
26. Legal Aspects of Computer-related Crime in the Information Society – COMCRIME, <http://europa.eu.int/ISPO/legal/en/crime/crime.html>.
27. Бакрески, Оливер. „Најсилио оружје досега“, Современа македонска одбрана, бр.9, стр.165. Скопје, 2004.

28. Бункер, Џ. Бункер. „ Не-државни закани и идни војни“,превод Анита Костовска, Нампрес, Скопје, 2009.
29. Георгиева, Л. „Творење на мирот - Мирот, безбедноста и конфликтите по студената војна“, Виладорф, Скопје, 2004.
30. Гинтер, Кајзер. „Кргшинологија - воеед во основите“, Александрија, Скопје, 1996.
31. Гоцевски, Трајан. „Основи на системот на национална безбедност“, Филозофскифакултет, Скопје, 2006.
- 32.Зигел, Д. Х.ван де Бунт, Д.Зоур. „Глобален организиран криминал-трендови и случувања“, превод - Николина Утковска, Магор, Скопје, 2009.
- 33.Тупанчевски, Никола. „Компјутерски криминалитет“, Годишник на правниот факултет, Скопје, 1991.
- 34.Сулејманов, Зоран. (Криминологија).

Интернет извори :

- www.wikipedia.org
- www.internetlivestats.com
- www.internetworldstats.com
- http://eprints.ugd.edu.mk/10870/1/Skripta%20za%20Sigurnost%20na%20kompjuterski%20sistemi%2C%20kompjuterski%20kriminal%20i%20terorizam_revJA_2.pdf
- <http://www.maturskiradovi.net/forum/Thread-kompjuterski-kriminal>
- http://www.rtv.rs/sr_lat/evropa/milionska-kradja-lozinki-u-nemacko_454999.html
- <http://www.britannica.com/topic/Stasi>
- <http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillanceemail>
- http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=0
- <http://techterms.com/definition/malware>
- <http://www.kaspersky.com/internet-security-center/threats/malware-classifications>
- <http://www.informationweek.com/medco-sys-admin-pleads-guilty-to-computersabotage/d/d-id/1059395?>
- <http://lat.rtrs.tv/vijesti/vijest.php?id=135279>
- http://www.camet.hr/posredovanje_u_ijesavanju_racunalmh_incidenata
- <http://www.cybercrime.gov/unlawftd.htm>
- <http://www.brighthub.com/engineering/civil/articles/47197.asph>
- <http://www.telh-faq.com/logic-bomb.shtml>
- <http://www.nûcrosft.com/security/worms/conficker.aspx>
- <http://www.ic3.gov/media/annuaheports.aspx>
- Official Site of European Union, Central Library,