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

FAKULTETI JURIDIK
ПРАВЕН ФАКУЛТЕТ
FACULTY OF LAW

STUDIMET PASDIPLOMIKE - CIKLI I DYTË
DREJTIMI: STUDIME TË SIGURISË

TEZA:

BURIMET E HETIMIT TË KRIMIT KOMPJUTERIK DHE PARANDALIMI I TIJ NË FAZA TË HERSHME

KANDIDATI:
GËZIM ALITI

MENTORI:
PROF. DR. JETON SHASIVARI

Shkurt 2019, Tetovë

Abstract

Even the fact that not all people are victims of cybercrime, they are all at risk today, it's because that cybercrime doesn't stop, cybercrime is a crime that is committed at anytime, anywhere and by anyone. As a crime can, be committed from a child of 12 years old up to a person with almost 67 years old. Also, this crime is transnational so it can happen that the attacker and the victim may not know each other because the attacker can be completely from another continent than the victim is from and this type of crime can be done at any time, so that's for why this type of criminality is so special and very important in the 21st century. Cybercrime variates day by day and it is being professionalized everyday by appearing in such more types and forms than from the first day that existed as a criminality. For committing this type of crime, a person needs at least one device from where he or she can connect to the internet. With the growth of technology, we can see that these days not so many banks are stolen directly with old methods, so with going on the crime scene, with physical attacks, with gunfire etc. so where the life of criminal should be jeopardized, unlike this today without going on the crime scene and without using a weapon, and only by getting a device that can access the internet the criminals can carry out a much heavier steal than ever has happened.

It is apparent that cybercrime poses a serious threat to all electronic operations and works of all modern corporations and organizations, but on the other side cybercrime appears to be a new challenge for organizations dealing with others corporate security. Even the largest organizations in the world have undergone major cyber security compromises, therefore for stopping these interventions it is foreseen that for helping our countries we need as many skilled workers and strongly responding to everyday problems in this area. I believe that all organizations need to understand the threats and the danger of computer crime that they can face every day in life and that every organization should at least have a qualified and appropriate person to try to reduce the number of crimes that can be carried out in that organization, even to try and eliminate in total the computer crime in that place. And the same person should regularly attend to new seminars and courses throughout the world because this kind of criminality is spreading widely and in new forms every day.

Even though we know that today it is impossible for a person or even a state to live and function without the use of computers and the Internet because of modernization around the world, which makes it clear why these tools used in everyday life are also being used for illegal purposes, mainly for a person's benefit, various avengers, various struggles between firms and states, and many other things that are detrimental to all people who use the Internet in the everyday life. Since our reality in recent years has marked many cases of cybercrime and computer abuses worldwide has come to the point that every state must regulate the law of this crime, and also not only to create preventive measures but to establish a legal system of sanctions because of the degree of danger that this criminality has, and also all states together around the world should have conventions and laws that they would respect. Since seeing the cybercrimes degree of danger, Macedonia joined with the rest of the European countries that have a very regulated justice system for this kind of crime with sanctions whether with money or even with prison.

Although Macedonia has this legal system from other countries, from the statistics that I saw for the year 2017 and before we see that approximately 50% of this small number of cases have been solved, although there are a lot of laws for cybercrime now in Macedonia, only three types of cybercrimes have been discovered, and we see that every day in this country cybercrime is committed by someone, and we see that Macedonia is very convenient territory for people who commit the cyber-attacks and cybercrimes, and all this is happening because the lack of the number of experts in this field that this country needs.

So my opinion for this place would be that persons designated for prevention and stopping of the cybercrime in the country should be persons who have knowledge of information technology and people who will discover different forms of cybercrime in this place, and the same people to be trained every day with new updates and new seminars because the hackers are always one step ahead of us and they discover new things every day and finally, persons that are going to be found that they did cybercrime they should be sentenced immediately because if they will be released than this type of crime will blossom from other criminals and new generations in place.

PËRMBAJTJA:

Lista e shkurtimeve

ACORN - Australian Cybercrime Online Reporting Network – Rrjeti për raportim të krimit kibernetik online në Australi

Akount – Llogari

Amazon – Ueb faqe për blerje në internet

Antivirus – Program për kontrollimin dhe zhdukjen e viruseve kompjuterike

Antimalware – Program për kontrollimin dhe zhdukjen e malware

APEC – Organizatë që mundëson tregun e lirë nëpër Azi

AZOP - Agjencioni për sigurimin e të dhënave personale në Kroaci

Bitcoin – Monedhë digjitale

Bot – Shkurtim i fjalës robot

Botnet – Sistem rrjetor i kompjuterëve që komandohet nga një apo më shumë persona për qëllime spiunimi

Brightplanet – Është kompani softuerike që kryen mbledhjen e të dhënave të strukturuara dhe përgatit ato për analiza të ndryshme

Burger King – Zinxhirë lokalesh që merren me shitjen e ushqimit të shpejt

C++ - Program me ndihmën e të cilit krijohen programet tjera

CIA – Është organizatë qeveritare e Shteteve të Bashkuara të Amerikës që mbledh informacione sekrete për vendet tjera të botës

Cracker – një person i cili kryen deshifrimet e programeve të ndryshme

Cyberterrorism – terrorizmi nëpërmjet internetit

DDoS – Shkurtesë nga Distributed Denial of Service që në shqip do të thotë ndalesa e shërbimit nga ndonjë ueb faqe

Ebay – Ueb faqe për blerje në internet

E-mail – Posta elektronike

Ethereum - Monedhë digjitale

ENISA – Agjencia Europiane e Sigurisë së Informacionit dhe rrjeteve

Facebook – Rrjet social

FBI – Agjencion qeveritar në Shtetet e Bashkuara të Amerikës që heton nëse rrezikohet siguria e vendit dhe nëse thehet ndonjë ligj kombëtar

Firewall – Sistem sigurie që monitoron dhe kontrollon trafikun e rrjetit hyrës dhe dalëse në bazë të rregullave të sigurisë

Freenet – Shfletues interneti

FUD – Full Undetectable – Program për ta bërë që një virus të jetë plotësisht i padukshëm për antivirusin

G8 – Grupi i tetëshes

Google – Motor kërkimor, motor për kërkimin e të dhënave

Hacking – Zakonisht i rreferohet ndërhyrjes së paautorizuar në një kompjuter ose rrjet

Haker – Person i cili njeh mjaft mirë përdorimin e kompjuterit dhe përdor atë apo ndonjë paisje tjetër me qëllim që të fitojë qasje të paautorizuar në të dhëna

Hyper link – Lidhje nga një link në një link tjetër

I2p – Shfletues interneti

INHOPE – Është një rrjet telefonik bashkpunues prej 46 linjave telefonike në 40 vende në mbarë botën dhe ka të bëjë me eliminimin e përmbajtjeve me abuzime seksuale të fëmijëve dhe eliminimin e përmbajtjeve ilegale

Instagram - Rrjet social

Interpol – Është organizatë ndërkombëtare që lehtëson bashkpunimin ndërkombëtarë të policisë

IRA – Organizatë terroriste e Irlandës

ITU - Unioni Internacional i Telekomunikimeve

Kaspersky – Kompani që merret me shkatrimin e viruseve kompjuterike

KGB – Agjencion kryesorë për siguri në Bashkimin Sovjetik

Kremlin Kids – Hakera rus që sulmuan Estoninë

Kriptovaluta – monedha digjitale

Malware – softuer i cili është i projektuar posaçërisht për të prishur, dëmtuar ose fituar qasje të autorizuar në një sistem kompjuterik

Meritalk – Portal për lajme të reja në lidhje me teknologjinë informative

MIT – Instituti i teknologjisë në Masaçusets

Nato – Organizata e Traktatit të Atlantikut Verior

Neofil – person i dashuruar në sende të reja

Norton Security - Kompani që merret me shkatrimin e viruseve kompjuterike

OKB – Organizata e kombeve të bashkuara

Onecoin - Monedhë digjitale

Online – Paisje apo ueb i lidhur në internet

P2P – Peer to Peer – program për shpërndarje të programeve

Password – Fjalëkalim

PC – Kompjuter Personal

Pedofil – një i rritur që tërhiqet seksualisht nga fëmijët e vegjël

PENTAGON – Selia e departamentit të mbrojtjes së Shteteve të Bashkuara të Amerikës

Phishing – Kopjim i faqeve të vërteta me qëllim përfitimi

Phreaker – është një person i cili thyen në mënyrë të paligjshme rrjetin telefonik, zakonisht për të bërë thirrje në distancë ose për të përgjuar

Ripple (XRP) - Monedhë digjitale

R.M. – Republika e Maqedonisë

SERVER – është një kompjuter që ofron të dhëna për kompjuterë tjerë

SHBA – Shtetet e Bashkuara të Amerikës

Sistem Operativ – është softueri i sistemit që menaxhon burimet kompjuterike dhe softuerike dhe ofron shërbime të përbashëta për programet kompjuterike

Smartphone – celular i cili mund të kryej më shumë funksione se sa ai normal

Snapchat - Rrjet social

SONY – Kompani për shitje të paisjeve elektronike

Teknologjia Digjitale – Përfshin të gjitha llojet e paisjeve dhe aplikacioneve elektronike që përdorin informacionin në formën e kodit numerik

Tor – shfletues interneti

Twitter - Rrjet social

UEB – World Wide Web – faqe online në internet

Virus Kompjuterik – program që krijohet me qëllim të dëmtimit, spiunimit dhe shkatrrimit të kompjuterit

Washington Post – Portal për lajme

Yahoo – Ueb faqe për lajme dhe për përdorimin e adresës elektronike

HYRJE

Bota në të cilën jetojmë është përplot me njerëz të cilët dita-ditës përdorin paisje elektronike siç janë: kompjuterët, celularët, laptopët, televizorët, e paisje të tjera, të cilat në shumicën e rasteve janë të lidhura me internet. Interneti është sistem rrjetor që kryen dhe mundëson lidhjen e miliarda paisjeve elektronike për të bërë kërkime nga më të ndryshmet duke u bazuar në një spektër të gjërë të informatave dhe burimeve të cilët i zotëron ai. Përdorimi i internetit në raport global që nga viti 2000 e deri në ditët e sotme është në një rritje masive prej 1066% dhe në çdo moment nëpër tërë botën janë mbi 4.2 miliard njerëz online[1]. Sado që të jetë përdorimi i internetit i dobishëm nga njëra anë, ai po aq mund të jetë i dëmshëm nga një këndvështrim tjetër. Pra, duke parë se bëhet rritja e përdoruesve në një numër masiv, duhet ditur se edhe rreziku i krimeve nëpërmjet internetit në rajon global dhe po ashtu edhe në Republikën e Maqedonisë bëhet edhe më i madh. Në ditët e sotme siguria e sistemit informativ mund të rrëzohet në mënyra të ndryshme, nga hakerë të ndryshëm, duke kryer zbulime nga më të ndryshmet, të cilat gati se edhe janë të padukshme apo shumë vështirë zbulohen nga përdorues të thjeshtë të internetit.

Me rritjen e suksesshme të internetit, në fakt me rritjen masovike të përdoruesve të internetit u krijua një themel i fortë për përhapjen e infeksioneve, viruseve dhe malwareve të ndryshëm, të cilët mund të ndikojnë te një numër i madh i sistemeve, pothuajse edhe në miliona sisteme nga më të ndryshmet. Po ashtu, në ditët e sotme është i njohur krijimi i një programi të madh që mban emrin BOTNET, ku kryhet kontrollimi i një rrjeti të madh me kompjuterë të infektuar nga e gjithë bota nga ana e viruseve të krijuara nga hakerë të ndryshëm, duke ardhur te përfitimi i informatave apo edhe të dhënave të ndryshme me qëllime përfitimi apo edhe hakmarrjeve të ndryshme.

Duke pasur parasyshë rëndësinë aktuale të këtij fenomeni se sot çdokush nga ne ka së paku një paisje nëpërmjet së cilës lidhet në internet, duke u bazuar në atë se sot gati çdo person

[1] Statistika të nxjerura nga analiza e fundit që është kryer më 30 Qershor 2018 nga faqja http://www.internetworldstats.com/stats.htm (Qasur më 28/11/2018)

mund të kryej kriminalitet nëpërmjet internetit dhe duke e ditur se çdo ditë kryhen blerje nëpërmjet internetit dhe duke ditur se Republika e Maqedonisë është një shtet i varfër dhe jo shumë i njoftuar në këtë lëmi, kam vendosur që të bëj një kërkim shkencor në lidhje me krimin kibernetik. Do të tregoj si fillon ky krim, kush e kryen atë më së shpeshti dhe si të ruhemi që të mos jemi një nga viktimat e tij dhe ta parandalojmë. Interesant është fakti se kryersi te krimi kompjuterik mund të jetë një fëmijë 12 vjeçar por mund të jetë edhe një plak 60 apo më tepër vjeçar dhe pasojat mund të jenë të mëdhaja dhe të rënda, si në aspektin e vlerave pasurore poashtu edhe në vlerat morale dhe dinjitoze.

Punimi është i ndarë në katër kapituj:

Në kapitullin e parë do të elaborohet kriminaliteti kompjuterik në përgjithësi, do të bëhen disa analiza themelore të përkufizimeve nga autorë të njohur në lidhje me kriminalitetin kompjuterik dhe historinë e tij, do të shihet se cilat janë burimet e kriminalitetit kompjuterik, do të kryhet trajtimi kriminalistik, pra të shihet se si trajtohet ky lloj kriminaliteti në R.M., si trajtohet në Europë dhe si trajtohet në tërë botën. Do të bëhet analiza dhe do të shihen raporte nga më të ndryshmet, nga autorë të njohur dhe specialistë të kësaj lëmie. Në këtë kapitull poashtu do të përshkruhet se në cilat fusha mund të hasim kriminalitet kompjuterik, pra në cilat hapsira duhet të kemi kujdes nga ky lloj krimi e nga cilët persona, dhe për në fund të këtij kapitulli do të shihen tendencat apo qëllimet e këtij lloj kriminaliteti.

Në kapitullin e dytë do të analizohet më gjërësisht kriminaliteti kompjuterik dhe tema të cilën e shkruaj unë do ta përqëndroj më së shumti në këtë kapitull duke u njoftuar se cilët janë mënyrat dhe llojet e kriminalitetit kompjuterik, çfarë janë viruset kompjuterike, si krijohen ato, si kryhen sulmet e vogla dhe sulmet e mëdha të sistemeve kompjuterike, si kryhen vjedhjet e identitetit, cilët materiale apo përmbajtje janë të ndaluara, si bëhen mashtrimet dhe shitjet on-line. Poashtu në këtë kapitull do të përshkruhen ndryshimet teknologjike gjatë 10 viteve të fundit dhe do të shihet se numri i krimeve kompjuterike a është rritur masovikisht apo jo dhe se a është ende në rritje. Më pas do të shkruhet për një aplikacion me emrin BOTNET që njihet edhe si një ndër aplikacionet më të rrezikshme që njeh bota. Në fund të kapitullit të dytë do të flitet për një rrjet të veçantë që mban emrin Deep Web dhe sot njihet si rrjeti më i madh i kriminalitetit

nëpërmjet të cilit kryhet gati se çdo lloj kriminaliteti duke përfshirë edhe vrasjet me pagesë, shitjen e drogës e shumë e shumë krime të tjera për të cilat do të flitet më vonë dhe si për fund të këtij kapitulli do të shkruhet shkurtimisht edhe për kiber terrorizmin, ky lloj krimi ndonjëherë thirret edhe si luftë informative pasi që me anë të këtij krimi sulmohen bankat, ushtritë, qendrat kontrollore të trafikut ajror, etj.

Në kapitullin e tretë do të analizohet parandalimi i kriminalitetit kompjuterik në fazat më të hershme, si duhet ikur nga ky lloj kriminaliteti, do të përshkruhen të gjitha mjetet dhe metodat me anë të cilave mund të kryhet parandalimi i kriminalitetit. Po ashtu do të shihet ky lloj kriminaliteti në dimenzion ndërkombëtar, se si organizatat më të njohura botërore parandalojnë kriminalitetin kompjuterik edhe me ligj, do të shkruhet për atë se cilët janë mekanizmat ndërkombëtar dhe konventat të cilat mbahen për parandalimin dhe gjykimin e kriminalitetit kompjuterik dhe së fundmi do të shkruhen disa nga ligjet me anë të së cilave zotron Republika e Maqedonisë në lidhje me këtë lloj kriminaliteti.

Kapitulli i fundit do ta përqëndrohet tek kriminaliteti kompjuterik në Republikën e Maqedonisë dhe Europë. Sa është përqindja e tij në këtë vend, sa është numri i errët i krimeve kompjuterike, do të shohim se çfarë veçorishë kanë personat të cilët merren me krimin kompjuterik, sa të njoftuar janë qytetarët e Republikës së Maqedonisë për këtë lloj kriminaliteti. Do të shohim se sa prej tyre kanë qenë viktima të krimit kompjuterik, sa është numri i viktimave të këtij lloj krimi në gjithë territorin e Republikës së Maqedonisë, cilët persona shfaqen më së shpeshti si viktima. Këto e disa të dhëna të tjera do të merren nëpërmjet intervistave të shkurtra që do tentoj të kryej me persona nga më të ndryshmit, duke filluar nga një fëmijë e deri tek një plak. Po ashtu do të tentoj që të jenë të gjithë të lëmive të ndryshme, nëpërmjet formularëve me disa pyetje me përgjigje të shkurtra Po ose Jo dhe të njëjtat do të analizohen dhe do të arrihet tek një përfundim.

Për ta përmbyllur këtë punim do të paraqes rezultatet e intervistave të cilat do t'i kryej me persona të ndryshëm të niveleve të ndryshme ku do të shihet se në cilën pjesë më së shumti kanë problem qytetarët e Republikës së Maqedonis. Po ashtu do të shohim se a zgjidhen problemet e viktimave të kriminalitetit kompjuterik, do të shohim se si ligji e mbron një person nga krimi kompjuterik në Republikën e Maqedonisë, sa Republika e Maqedonisë ka raport me Bashkimin

Europian dhe me tërë botën në përgjithësi në sferën e kriminalitetit kompjuterik. Gjithashtu duhet ditur se nuk mjafton vetëm një kuadër ligjor për të kryer parandalimin e kriminalitetit kompjuterik në vend, pra nevojitet edhe zbatimi në praktikë, ku duhet bërë rritja e ndërgjegjes së qytetarëve dhe përmisimi i mekanizmave kundër këtij lloj kriminaliteti.

Metodologjia e hulumtimit

Së pari, kërkimet e kryera janë bazuar në një qasje induktive të temës, pra duke observuar dhe studiuar faktet, do të nxirren rezultate në lidhje me situatën e krimit kibernetik në të drejtën e R. Maqedonisë dhe me qëllim për të përcaktuar nëse shteti i Republikës së Maqedonisë është mjaftueshëm i përgatitur për të luftuar krimin kibernetik dhe sfidat që ai përbën për sigurinë kombëtare.

Së dyti, për realizimin me sukses të këtij punimi do të përdoren metoda të ndryshme për përmbledhjen dhe analizën e të dhënave të paraqitura në këtë punim të magjistraturës. Metodologjia e hulumtimit të këtij punimi do të bazohet në shqyrtime të më shumë librave që kanë të bëjnë me kriminalitetin kompjuterik duke filluar nga fazat më të hershme e deri tek fazat e fundit dhe sanksionet. Po ashtu do të bazohet në raporte dhe artikuj të ndryshëm të marra nga faqe të ndryshme në internet të cilat merren me raportimin e krimeve, të cilat kryhen nëpërmjet internetit, do të shihen shkaqet dhe motivet e këtyre krimeve, nga kush kryhen dhe në cilat vende kryhen këto krime më së shumti.

Së treti, do të përfshihen analizat legjislative dhe jurispodenca duke përfshirë dënimet e duhura që duhet të jepen për këta lloj krimesh, do të përfshihen konsultime dhe mendime nga persona që merren me biznese, viktima, persona familjarë dhe analiza nga raportet e këtij lloji kriminaliteti nga mediat e ndryshme botërore.

Qëllimet e hulumtimit

Qëllimi i këtij punimi është analizimi i krimeve të cilat kryhen nëpërmjet internetit, metodave të cilat janë përdorur, përdoren akoma dhe do të përdoren për të kryer një kriminalitet kompjuterik, si kryhet kriminaliteti kompjuterik, sa krime kompjuterike kryhen brenda një viti apo dekade. Po ashtu qëllimi është të gjindet se kush i kryen këto krime të rënda më së shpeshti, sa para janë në rrezik brenda një vendi apo në raport global për një afat të caktuar, sa para humben (vidhen) dhe sa para arrihen të kthehen tek viktimat. Si qëllim tjetër kryesor është arritja e reduktimit të kriminaliteti kompjuterik me anë të preventivave të nevojshme të ndërmarra nga ana e ekspertëve të IT në kohëra të caktuara dhe me anë të ndëshkimit të kriminelëve nga ana e inspektorëve dhe gjykatave të ndryshme në një vend me dënime më të ashpra të mundshme. Po ashtu si qëllim tjetër i hulumtimit është menaxhimi i ruajtjes së privatësisë të përdoruesit, fitimi i besimit nga ana e përdoruesve se bota e internetit nuk është një botë e mbushur përplot me kriminelë dhe hakerë prej më të ndryshmive, pra kjo arrihet duke hapur organizata të shumta të cilat merren me udhëzimin e njerëzve se si t'iu shmangen këtyre krimeve, duke shpallur artikuj të ndryshëm nëpër media dhe duke funksionuar ligji i një vendi.

KAPITULLI I PARË

KRIMINALITETI KOMPJUTERIK – TRAJTIMI TEORIK

1.1 Historia e kriminalitetit kompjuterik dhe analizat themelore të përkufizimeve të kriminalitetit kompjuterik

Shoqëria jonë moderne ishte në kërkim të shkallës apo zbulimit që do të bënte lidhjen në mes të qytetarëve, bizneseve, institucioneve financiare dhe qeverive të cilat do t'i kalonin kufinjtë politik dhe kulturor. Teknologjia dixhitale është ajo e cila e mundësoi këtë lidhje dhe u dha përdoruesve të saj shumë përfitime nga njëra anë, por njëkohësisht nga ana tjetër teknologjia dixhitale është ajo që siguroi një mjedis të pasur me informacione për të kryer aktivitete kriminale duke filluar nga vandalizmi i identitetit të vjedhur e deri tek vjedhja e informatave të klasifikuara të qeverive.

Si kriminalitet, krimi kompjuterik për herë të parë është shfaqur në vitin 1960 ku edhe u përdor për herë të parë termi hacking[2] për të përshkruar një aktivitet me anë të cilit, modelit të trenit MIT i'a modifikuan funksionimin e tij dhe zbuluan mënyra për të ndryshuar disa funksione, pa rikonstruktimin e tij[3]. Në vitet e 70 - ta kur edhe filloj hackingu të bëhet edhe më evident, pra filloi të shfaqet edhe më shumë, një nga shoqatat e hakerëve e quajtur *phreakers* filloi të merret me sistemet telefonike dhe me anë të disa kodeve dhe sinjaleve të cilët ata përdornin, arritën deri tek zbulimi i thirjeve telefonike me distanca pak më të largëta, pra ishte një zbulim goxha i madh për atë kohë. Në vitet e 80 - ta filluan sendet pak nga pak të ndryshonin pasi që në këto vite ishte koha kur për herë të parë filluan që t'i shitnin kompjuterët njerëzve, pasi që deri atëherë kompjuter kishin vetëm universitet, firmat me biznese të mëdhaja, e tani u mundësua që çdo kompjuter të mund të përdoret për nevoja personale, çfardo qofshin ata dhe pa asnjë surprizë nga kjo erdhi deri tek rritja e numrit të personave të cilët do të merreshin me krime kompjuterike. Derisa disa nga hakerët e atëhershëm dikush tentonte që të gjejë gabimet që kishin atëherë

[2] Term që përdoret për të përshkruar veprimtarinë e modifikimit të produktit ose për të ndryshuar funksionimin e tij normal https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/ (Qasur më 28 Nëntor 2018)

[3] Informata nga histori e përshkruar në lidhje me kriminalitetin kompjuterik https://www.linkedin.com/pulse/20141001193003-152360640-history-of-cyber-crime (Qasur më 28 Nëntor 2018)

sistemet operative, dikush nga ana tjetër filloi të merret me kriminalitet kompjuterik që atëherë duke filluar me pirateri, duke krijuar viruset e para dhe duke kryer ndërhyrje nëpër sisteme ku mund të vjidhnin informata sekrete. Mirëpo nuk u desht shumë deri te përgjigja nga shtetet e atëhershme të cilat sollën një ligj të asaj kohe në lidhje me kriminalitetin kompjuterik i cili mban emrin Federal Computer Fraud and Abuse Act (Mashtrimi federal kompjuterik dhe akti abuzues)[4].

Vitet e 90 – ta ishin vitet ku hakingu filloi të marrë një famë të lartë, ishin vitet kur filluan të paraqiten persona të cilët nuk thirreshin haker por ishin persona të cilët kishin kaluar në një shkallë më të lartë të rrezikshmërisë ishin cracker-ët[5] e asaj kohe, të cilët nëpërmjet kodeve të tyre filluan të qaseshin ku të donin, mirëpo këto vite njihen edhe si vite të rënda për personat të cilët merreshin me kriminalitetin kompjuterik, pasi që shumë persona u burgosen në këto vite dhe në shkëmbim të lirive ato filluan që të spiunojnë njëri-tjetrin.

Në fillimin e viteve të 2000 – filluan që të sulmohen organizatat dhe bizneset pak më të njohura ku të gjitha u sulmuan nëpërmjet DDOS[6] sistemit i cili sistem atëherë u zbulua dhe me anë të përdorimit të tij erdhi tek dëmtimi i Microsoftit, Ebay, Yahoo, Amazon dhe poashtu u sulmua Departamenti i Mbrojtjes dhe Stacioni ndërkombëtarë i hapsirës nga një fëmijë 15 vjeç. Vitet 2010 e lart dimë se tani bota është në vitet e dixhitalizimit, komuniteti i hakerëve është bërë më i sofistikuar e më i komplikuar se kurrë. Këto janë vitet ku mund të gjejmë nga një haker të vetmuar apo një grup hakerësh gati se në çdo kënd në të cilin ka internet. Mirëpo sot këto grupe janë shumë të rrezikshme pasi që ata kanë mundësi të marrin shumë informata apo sekrete shtetërore të cilat më pas munden edhe t'i bëjnë publike, gjë që do të sillte shumë probleme në një vend. Sidoqoftë dimë se qoftë hakerët e mirë apo të këqinjt gati se gjithmonë janë dhe do të jenë një hap përpara ekspertëve të kriminalitetit kompjuterik[7].

Në vitet e fundit njihet edhe transferimi i parave nëpërmjet kriptovalutave si një ndër rreziqet më të mëdhaja që historia njeh, pasi që kjo gjë mundësoi një numër të madh të personave të kryejnë transferime të parave nga një konto në tjetrën pa mos ditur emër, mbiemër, adresë apo

[4] Shiko amandamentin e krijuar në vitin 1986 kundër kriminalitetit kompjuterik https://ilt.eff.org/Computer_Fraud_and_Abuse_Act_(CFAA).html (Qasur më 28 Nëntor 2018)
[5] Një person apo grup personash që bënin dhe bëjnë thyerjen e programeve nëpërmjet kodeve
[6] Sulmi i uebfaqeve nga programi botnetit duke kryer vizita të shumta të ueb faqeve të ndryshme për një kohë të caktuar dhe kjo bën që të vijë deri tek rënia e tyre
[7] Histori e kriminalitetit kompjuterik prej viteve 1970 - 2010 https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/ (Qasur më 28/11/2018)

edhe vetëm një informatë të vetme nga pranuesi, e gjithë kjo u krye nga persona të cilët merren me krime kompjuterike por edhe me krime të lëndëve të tjera dhe me këtë ato arrinin tek një shumë parashë për të cilën nuk duhet përgjigjur shkaku i anonimitetit.

Si definicion fjala krim kibernetik është një aktivitet kriminal i cili mund të kryhet me anë të kompjuterëve (në shumicën e rasteve) dhe të gjithë llojeve tjera të paisjeve teknologjike që kanë qasje në internet[8]. Krimi kibernetik është një kriminalitet digjital pra si kryes mund të jetë çdokush, pa dallim gjinie qoftë mashkull apo femër, pa dallim moshe duke përfshirë edhe një fëmijë të vogël e deri tek një plak i cili ende është në një gjendje normale dhe ka njohuri në këtë lëmi. Krimi kibernetik i referohet një aktivitetit kriminal i cili kryhet me ndihmën e telekomunikimeve në arenën apo fushën e internetit dhe njihet si manifestim i krimit të vjetër nëpërmjet një mediumi të ri. Krimi kibernetik si lloj kriminaliteti dallon prej një kriminaliteti tjetër në katër aspekte edhe atë: shumë lehtë mund të kryhet, nevojiten burime minimale për të arritur deri tek një dëmtim mjaft i madh, është një krim në të cilin kryersi nuk është patjetër të jetë prezent fizikisht, pra si kryerës ai mund të jetë gjithkund dhe së fundmi si krim ligjërisht i dënueshëm, shpesh nuk është i qartë plotësisht[9].

1.2 Burimet e krimit kompjuterik

Ekzistojnë më shumë burime të kriminalitetit kompjuterik por më me rëndësi janë dy:

a) hacking-u dhe

b) vjedhja e identitetit

a) Hacking-u – ekzistojnë më shumë definicione nga mbarë literatura e botës në lidhje me hacking-un mirëpo unë kam zgjedhur një nga ato të cilët mendoj se është më i përafërt me të vërtetën, duke u bazuar në fjalët e specialistëve me përvojë dhe ekspertëve të njohur. Hackingu është një qasje e paligjshme e një rrjeti kompjuterik ose e teknologjisë së informacionit për të pushtuar apo

[8] Definicion i zgjeruar në lidhje me krimin kibernetik nga fjalori i Oxfordit https://en.oxforddictionaries.com/definition/cybercrime (Qasur më 28/11/2018)
[9] Definicion dhe analiza të kriminalitetit kompjuterik në Universitetin e Washington-it https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf (Qasur më 28 Nëntor 2018)

për të keqpërdorur privatësinë e rrjetit duke kryer aktivitete të paligjshme në formë të vjedhjes (si të drejtat autoriale të një personi, duke bërë vjedhjen e identitetit dhe duke shitur atë nëpër markete të zeza), ose duke kryer qasje të paautorizuar për ndonjë lloj emocioni apo për shkaktim të ndonjë dëmi i çfarëdo sfere qoftë ai.[10]

Personi i cili merret me hacking mban emrin hacker. Hakeri është një person i cili gjen dhe shfrytëzon dobësitë e sistemeve kompjuterike dhe rrjeteve për të fituar qasje. Hakerët zakonisht janë programues të aftë kompjuterik me njohuri të larta në sigurinë kompjuterike.[11] Ekzistojnë edhe tipe të hakerëve pasi që ato klasifikohen sipas punës që ata kryejnë dhe sipas aksioneve të cilat ata i marin:

- Ethical Hacker (haker i moralshëm) ose white hat është tipi i parë i hakerëve i cili fiton qasje në sistemin e një kompjuteri me qëllim për t'i rregulluar dobësitë e identifikuara, ky tip i hakerit poashtu mund që të testojë dhe vlersojë cenueshmërinë e një rrjeti, ndryshe ky tip njihet si haker i mirë, pra ndihmon në sigurinë e një personi, kompanie apo organizate shtetërore.
- Cracker (black-hat) është një person i cili fiton qasje të paautorizuar në sistemet dhe rrjetet kompjuterike për përfitime personale ose përfitime për dikënd tjetër, zakonisht qëllimi i këtyre ndërhyrjeve është që të bëjnë vjedhjen e të dhënave korporative, të shkelë të drejtën e privatësisë, të kryej transferimin e fondeve nga një llogari bankare në tjetrën, etj.
- Grey-Hat është një person në mes hakerit etik dhe crackerit. Ai ose ajo thyen sistemet kompjuterike pa autorizim, me qëllim që të identifikojë dobësitë e sistemit dhe t'i tregojë pronarit se ku janë gabimet dhe ku duhet ndryshuar sendet me qëllim që të mos arrihet një ndërhyrje e njejtë në të ardhmen.
- Script kiddies (fëmijët me skripta) janë persona që nuk kanë dijeni dhe njohuri mbi këtë lëmi mirëpo duke përdorur programe të gatshme, vijnë deri në qasje të sistemeve kompjuterike në të cilat më pas shkaktojnë edhe dëmtime me apo pa vetëdije.

[10] Cit. nga Internet Law – Primary Cyber Crime Sources in US Part 9 (Qasur më 9 mars 2017). Shiko http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2595

[11] http://www.guru99.com/what-is-hacking-an-introduction.html Cit. nga definicione të përmbledhura nga ekspertë të krimit kompjuterik (Qasur më 28 Nëntor 2018)

- Hacktivist është një haker i cili përdor intelegjencën e tij për të kryer hacking me qëllim për të dërguar mesazhe sociale, politike, religjioze, etj. Kjo zakonisht kryhet me një metodë duke kryer ndërhyrje në uebfaqe të huaja dhe duke lënë mesazhe nga më të ndryshmet në to.
- dhe së fundmi kemi:
- Phreaker, i cili është një haker që identifikon dhe shfrytëzon dobësitë e telefonave[12].

b) Vjedhja e identitetit si vepër penale është marrja e paligjshme e të dhënave apo informacioneve të ndonjë personi tjetër për qëllime të impersonimit të viktimës në aktivitete kriminale dhe e gjithë kjo për përfitim financiar personal apo për përfitim të ndonjë personi tjetër[13]. Vjedhja e identitetit në kohë të fundit është në rritje mjaft të madhe dhe duke u bazuar në informata të burimeve primare të krimit kompjuterik në SHBA, të cilët njoftojnë se vitin e kaluar institucionet financiare dhe bizneset kanë humbur një shumë marrëmendëse prej 48 miliard dollarë, ndërsa personat si individë kanë humbur dikund tek 5 miliard dollarë brenda një viti. Mënyrat më të shpeshta të vjedhjes së identitetit janë nëpërmjet përdorimit të kredit kartelave, kartat e debitit dhe çekat me anë të cilëve kryhen blerje të paligjshme. Numri i viktimave në vitin e kaluar është vlersuar në 10 miljon njerëz vetëm në SHBA, poashtu ngjajshëm edhe në Europë.[14]

Duke parë këto shifra të humbjeve në dollarë tek institucionet dhe duke parë numrin e madh të viktimave brenda një viti, ne si individë arrijmë të kuptojmë se ky krim është një ndër krimet më serioze për momentin dhe mund të parashtrojmë pyetje se sa i rrezikshëm atëherë është ky krim dhe si të mbrohemi ne që të mos jemi viktimë e këtij lloj kriminaliteti, për këto më detajisht do të shkruhet te kapitulli i tretë, i cili ka të bëjë me parandalimin e kriminalitetit kompjuterik.

[12] Ndarje nga ekspertë të krimit kompjuterik http://www.guru99.com/what-is-hacking-an-introduction.html (Qasur më 29/11/2018)
[13] Definicion i cituar nga Internet Law – Burimet primare të kriminalitetit kompjuterik https://www.upcounsel.com/internet-law (Qasur më 19/12/2018)
[14] Statistika të marrura nga ueb faqja e ligjit të internetit dhe burimet primare të kriminalitetit kompjuterik në SHBA http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2595 (Qasur më 09/03/2017)

1.3 Trajtimi kriminalistik i krimit kompjuterik

Kriminalistika si për format tjera të kriminalitetit ashtu edhe për kriminalitetin kompjuterik ka rëndësi të veçantë për zbardhjen e ndonjë rasti, parandalimin e kriminalitetit dhe luftimin e kriminalitetit në qoftë se krimi ka ndodhur. Funksionimi i kompjuterit në aspektin kriminalistik manifestohet në katër forma themelore edhe atë: kompjuteri si mjet i kryerjes së veprës penale, kompjuteri si objekt i atakimit, kompjuteri si mjet për organizim, realizim, udhëheqje dhe planifikim të veprimeve kriminale dhe së fundmi kompjuteri si mjet me të cilin kryhet parandalimi dhe të provuarit e veprave penale nga ana e policisë.[15]

FBI duke trajtuar dhe hetuar problematikën e veprave penale të kriminalitetit kompjuterik ka konstatuar se egzistojnë tre grupe personash që paraqesin probleme, tek grupi i parë që edhe quhet sipas tyre grupi më i madh marrin pjesë personat të cilët bëjnë ndërhyrje në sistemet kompjuterike vetëm për të parë se a është e mundur dhe e kryejnë këtë pa ndonjë qëllim të caktuar pra nuk shkatërojnë asgjë dhe nuk vjedhin asgjë. Në grupin e dytë hyjnë personat me qëllime të këqija pasi që këto persona bëjnë thyerje në sistemet kompjuterike me qëllim të shkatërimit të sistemit kompjuterik dhe së fundmi në grupin e tretë marrin pjesë persona profesionistë të cilët shfrytëzojnë intelegjencën e tyre për përfitim material qoftë për vete apo dikënd tjetër, duke përdorur mangësitë e sistemeve kompjuterike.[16]

1.4 Fusha kërkimore dhe natyra e krimit kompjuterik

Kriminaliteti kompjuterik si çdo kriminalitet tjetër ka fushat e veta se ku mund të veprojë dhe ku mund që të kërkojmë më së shpeshti atë. Mirëpo për dallim nga krimet e tjera ky lloj kriminaliteti nuk ka kufi dhe është në një rritje në një numër të madh krimesh për kohë të shkurtër. Kriminelët e këtij krimi gjithmonë e shfrytëzojnë shpejtësinë, komoditetin dhe anonimitetin e këtij krimi për të kryer një seri veprimesh kriminele dhe nuk njohin kufi qofshin ato fizik apo virtual. Krimet të cilat kryhen në këtë lloj kriminaliteti paraqesin kërcënime shumë reale

[15] Dr. Sc. Veton G. Vula, "Kriminaliteti kompjuterik", Prishtinë 2010, cit. Fq 52
[16] William S. Sessions Kriminaliteti kompjuterik – trend i cili eskalon, Doracaku 3/91, fq.221

për viktimat në mbarë botën. Megjithëse nuk ka një përkufizim të saktë për krimin kibernetik, zbatimi i ligjit bën një dallim midis dy llojeve kryesore të krimit në internet, edhe atë[17]:

- Krimi kompjuterik i avancuar apo i teknologjisë së lartë – me anë të së cilit krim kryhen sulme të sofistikuara ndaj paisjeve kompjuterike dhe softuerit dhe

- Krimi kompjuterik i aktivizuar – ku shumë krime tradicionale kanë marrë një kthesë të re me ardhjen e internetit, siç janë krimi kundër fëmijëve, krimet financiare, poashtu edhe krimet e terrorizmit.

Në të kaluarën krimi kompjuterik kryhej zakonisht nga individë apo grupe të vogla, ndërsa sot ne shohim se ka rrjete kibernetike komplekse të cilat kanë arritur që të sjellin persona nga e gjithë bota në të njëjtën kohë për të kryer krim kompjuterik nga një shkallë e paparë. Shumë organizata kriminale të cilat janë marrë me krime nga më të ndryshmet janë kthyer tek krimi kompjuterik pasi që arrihet në shumë kohë të shkurtër tek një sasi e madhe parash. Natyrat e krimeve që kryhen sot jo që nuk janë të njohura janë si shembull vjedhjet, mashtrimet, lojrat e fatit që janë ilegale, shitja e shumë sendeve që janë ilegale, e shumë e shumë krime të tjera të cilat janë përhapur shumë dhe sot kryhen nëpërmjet internetit nëpër tërë botën.

[17] Zbatimi i ligjit nga ana e Interpol-it shiko https://www.interpol.int/en/Crime-areas/Cybercrime/Cybercrime (Qasur më 29/11/2018)

KAPITULLI I DYTË

HETIMI I KRIMIT KOMPJUTERIK

2.1 Mënyrat dhe llojet e kriminalitetit kompjuterik

Ekzistojnë shumë mënyra dhe lloje të krimit kibernetik dhe për atë arsye ky lloj kriminaliteti shumë rëndë luftohet. Sot, të gjitha paisjet dixhitale (duke përfshirë kompjuterët, tabletët, smartfonet, etj.) janë të lidhura me internet. Pra, në teori kriminelët mund të sjellin një kaos të madh dhe të bllokojnë gjithë qasjet tona nëpër gjithë botën nëpërmjet internetit dhe shkaku i këtij rreziku të madh që paraqitet nëpër tërë botën, qeveritë kanë filluar që të kapin shumë seriozisht krimin kibernetik dhe luftën ndaj tij. Ekzistojnë disa mënyra dhe lloje të krimit kompjuterik e ato janë: Cyber bulling-u, Spam Email-at, Phishing-u, vjedhjet e identitetit, përmbajtjet fyese të ndaluara, materialet abuzive seksuale të fëmijëve, mashtrimet dhe shitjet on-line, etj. Në vazhdim do të shpjegoj për secilën ngapak se çka janë dhe si shfaqen.

2.1.1 Cyber Bulling (Ngacmimi kibernetik)

Cyber bullingu apo ndryshe i quajtur ngacmimi kibernetik, është ngacmim i cili në shumicën e rasteve bën pjesë tek celularët, kompjuterët dhe tabletat. Ky ngacmim zakonisht ndodh nëpërmjet mesazheve, teksteve të ndryshme apo aplikacioneve online në të cilat njerëzit mund të shohin, participojnë apo shpërndajnë përmbajtjen. Cyber bullingu përfshin dërgimin, postimin apo shpërndarjen negative, të dëmshme dhe false për dikënd tjetër. Mund të përfshijë shpërndarjen e informacionit personal ose privat mbi dikë tjetër që shkakton turpërim ose poshtërim, poashtu duhet cekur se kemi edhe cyberbulling që kalojnë vijën e sjelljeve të paligjshme apo vijën kriminale.

Vendet ku më së shumti mund të gjejmë cyberbullingun janë:

- Në mediat sociale, siç janë Facebook-u, Instagrami, Snapchati, Twitter, etj.

- Në SMS

- Në mesazhet e çastit (viber, whatapp, skype, etj.) dhe

- Email

Cyber bullingu mund të jetë: I vazhdueshëm, i përhershëm dhe shumë pak i dukshëm.

Mbrojtja nga Cyber bullingu – zakonisht me cyber bulling merren fëmijët, pasi që ata kanë më shumë qasje nëpër mediat sociale ku edhe krijojnë bindje nga më të ndryshmet dhe në shumicën e rasteve ngacmojnë personat tjerë nga xhelozia, shpërndajnë foto nudo të shokëve apo shoqeve, krijojnë profile të rrejshme, gënjejnë dhe kryejnë akuzime të rrejshme, prandaj rekomandohet kontrollimi më i shpeshtë nga ana e prindërve te kompjuterët, celularët apo tabletat e fëmijëve të tyre, shkaku i asaj që të mos vijë deri te këta lloj ngacmimesh.

Cyber bullingu është i shfaqur dhe shfaqet në një frekuencë mjaft të lartë ku 21% e fëmijëve nga vitet e 12 e deri 18 i janë nënshtruar këtij lloj krimi kompjuterik dhe nga këto 16% e nxënësve kanë qenë të shkollave të mesme të cilët kanë qenë të ngacmuar 12 muajt e fundit.[18]

Një person mund të jetë i përfshirë në ngacmimin kibernetik në disa mënyra, siç janë: personi mund të jetë i ngacmuar, personi mund të ngacmojë persona të tjerë, apo edhe personi të jetë dëshmitar i ndonjë ngacmimi.

2.1.2 Spam email-at dhe phishing-u (replikat)

Vetë fjala Spam do të thotë bllokim nga gjuha angleze, pra këtu kemi të bëjmë me email-at që bllokohen apo ndalohen. Spam email-at janë ekuivalente me junk email-at (email-at e padëshiruar), dhe janë email-a prezent gati se te çdo email që përdoret sot. Sidoqoftë spam nuk është vetëm i bezdisshëm ashtu siç dikush mendon, ai është edhe i rrezikshëm e sidomos kur është i bashkangjitur me një faqe apo ndonjë blog i cili nuk është origjinal por është replikë, atëherë vjen deri tek vjedhja e të gjitha të dhënave të një personi në mënyrë elektronike. Email-at e bllokuar dërgohen në një numër masovikisht të madh nga ip të ndryshme, nga persona të cilët

[18] Statistika të marrura nga shtojca e krimit shkollor të Amerikës Dhjetor 2016 https://nces.ed.gov/pubs2017/2017015.pdf (Qasur më 01/12/2018)

mbajnë emrin spammer-a[19] apo kriminel kibernetik të cilët për qëllime të ndryshme siç janë: fitimi i parave nga një numër i vogël i personave të cilët do t'ju përgjigjen këtyre emaileve, krijimi i faqeve të rrejshme me emra të njohur të brendeve, pra krijimi i faqeve false për qëllime të përfitimit të fjalëkalimit, kredit kartelave, detajeve nga numri bankar dhe si qëllim i fundit zakonisht është shpërndarja e një kodi me qëllim të keq që të dëmtojë kompjuterin e pranuesit të email-it.[20]

Spam email-at zakonisht dërgohen me programe të ndryshme nga një numër i madh i ip adresave[21] dhe në tekste gjithmonë përmenden fitime nga loteri të ndryshme, përditsime nga ana e bankës nga e cila vjen direkt tek informatat bankare të një personi, etj.

Phishingu – është një kriminalitet kompjuterik në të cilin viktima apo viktimat kontaktohen nëpërmjet emailave, telefonatave, mesazheve të ndryshme nga dikush i cili paraqitet si institucion legjitim për të joshur individët në sigurimin e të dhënave të ndjeshme si informatat personale, detajet e kredit kartelave dhe llogarive bankare, fjalëkalimet, etj. Më pas ky informacion i vjedhur përdoret për të qasur llogari të ndryshme nga e cila mund të vijë apo rezultojë deri tek vjedhja e identitetit të personit apo humbja financiare.[22] Si lloj kriminaliteti kompjuterik është mjaft i përhapur dhe i dëmshëm, rreth më tepër se 100 milionë emaila në ditë lëshohën dhe punohet në drejtim të asaj që sa më shumë informata personale të mblidhen dhe afër 85% e organizatave janë në shenjestër.[23]

Gjithë emailët që kanë për qëllim phishingun kanë karakteristika gati të njejta të cilat janë:

1. **Tepër e mirë për të qenë e vërtetë** – këto llojë emailësh janë përtepër të koncentruar në atë që personi i cili i lexon ato, t'i bie menjëherë në sy, këto lloj emailash zakonisht kanë të

[19] Persona të cilët merren me dërgimin e email-ave të bezdishëm me qëllime përfitimi
[20] Qëllime të cituara nga kompania e mirënjohur e antivirusëve Kaspersky https://usa.kaspersky.com/resource-center/threats/spam-phishing (Qasur më 01/12/2018)
[21] Shkurtim nga fjala Internet Protocol Adress që do të thotë etiketim numerik i caktuar për çdo paisje të lidhur me një rrjet kompjuterik që përdor protokolin e internetit për komunikim. Zakonisht shërbejnë për identifikimin e kompjuterit dhe vendodhjen e tij.
[22] Definicion i cituar nga faqja e cila merret vetëm me raportimin e phishingu-t http://www.phishing.org/what-is-phishing (Qasur më 01/12/2018)
[23] Statistika të marrura nga faqja më e njohur dhe më e besuesme në lidhje me phishingun www.phishing.org

bëjnë me atë se personit të cilit i dërgohet emaili ai është fitues i lotarisë, fitues i një iphone, trashëgimtar i ndonjë çeku bankar, etj, pra duhet patur kujdes nëse shohim kështu raste të emailave, sidomos duhet patur kujdes me hapjen e tyre pasi që me të vërtetë nuk janë emaila real.

2. **Kërkimi urgjencor** – në kohë të fundit kjo është ndër llojet e phishingut më të rrezikshëm dhe është phishing favorit pasi që në këto emaile shkruhet se llogaria e ndonjë personi në çfardo llogarie qoftë (bankare, nga rrjetet sociale, email, etj.) ajo përshkruhet kurse ajo llogari ka skaduar, është suspenduar dhe duhet kryer përditësimin. Duhet ditur se shumica e organizatave nuk kërkojnë përditësimin e llogarive nëpërmjet internetit prandaj duhet kontaktuar direkt tek organizata dhe duhet pyetur nëse është e vërtetë emaili që ka pranuar.
3. **Hyper linqet** – ndodh që linku të mos jetë ashtu siç duket, pra pa mos shtypur një link me miun tonë duhet që vetëm të afrohemi te linku dhe ajo na tregon se ku do të na drejtonte në qoftë se ne shtypnim atë. Në qoftë se URL është më ndryshe se sa linku që ne kërkojmë është mirë që të mos shtypet aspak por duhet shikuar mirë gjithashtu sepse mund që në linkun e futur të ketë vetëm 1 ose 2 shkronja të ndryshme të cilët po nuk i vërejtëm do të na kushtonin shumë si shembull kemi www.bankofamerica.com e shkruajnë si www.bankofarerica.com ku në vend të 'm' është futur shkronja 'r', prandaj duhet vërejtur me kujdes se çka në të vërtet surfojmë.
4. **Shtojcat e panevojshme** – nëse në emailin tonë arrin ndonjë email nga ato të përditshmet apo ndonjë email që vjen për të parën herë tek ne dhe ne shohim se ka ndonjë shtojcë (attachment) që nuk duhet të jetë apo nuk ka lidhje me emailin e shkruar më lart është mirë që të mos hapim atë pasi që shumë shpesh këto shtojca përmbajnë viruse, ransomware, etj. Lloji i vetëm i sigurt i shtojcës që mund të hapet është kur shtojca është një .txt fajll.
5. **Dërguesit e pazakontë** – nëse ndodhë që në emailin tonë arrin ndonjë letër dhe na duket sikur është nga dikush që nuk e njohim apo qoftë edhe nga dikush që e njohim, nëse diçka

duket ndryshe nga herët tjera ose diçka duket e dyshimtë nga letrat e zakonshme që vinë në email, për sigurinë tonë duhet që mos të klikohet mbi to.[24]

2.1.3 Vjedhja e identitetit

Vjedhja e identitetit për momentin është si një ndër problemet më serioze dhe më të përhapura në jetën e përditshme. Ekzistojnë shumë teori për vjedhjen e identitetit dhe gati se përmendet si lloj kriminaliteti në çdo sferë, si krim paraqet veprimin e një personi i cili përdor të dhënat personale të dikujt tjetër në kundërshtim me ligjin me të cilën përveçse paraqet lëndim të privatësisë (si për shembull hapja e profileve të rrejshme nëpër faqe të ndryshme, prezantimi i rrejshëm), po ashtu paraqet edhe akt të dënueshëm me të cilin parashihet edhe dënim me burg.[25]

Kur flitet për vjedhje të identitetit ekzistojnë disa lloje motivesh dhe mënyrash se si mund të arrihet deri te kjo, duke filluar nga moskujdesi i vetë qytetarëve me të dhënat e tyre personale, e më rrallë te mbrojtja joadekuate ose e pamjaftueshme e të dhënave personale nga kreu i koleksioneve që përpunojnë të dhënat personale. Rreziku për keqpërdorimin e të dhënave personale po ashtu mund të jetë i lartë nëse ato i jepen ndonjë personi të panjohur ose ndonjë personi të dyshimtë, apo nëse me vetëdije të plotë publikohen informacione apo të dhëna personale nëpër rrjete sociale, ku edhe mundësia është mjaft e lart për manipulime me të dhënat personale. Si shembuj të ndryshëm për vjedhjen e identitetit kemi edhe email-at e përditshëm të cilët na vinë neve me përmbajtje se kemi trashëguar shuma marrëmendëse nga persona të cilët edhe nuk i njohim, mirëpo ato në të vërtetë kërkojnë të dhënat tona personale siç janë emri, mbiemri, datëlindja, kredit apo debit kartela dhe shumë e shumë të dhëna të tjera me anë të së cilës ato mund të përfitojnë shumë nga ne ose mund të na dëmtojnë shumë neve.

Mënyra më e mirë për t'u mbrojtur nga ky lloj kriminaliteti është që të kemi përgjegjësi për të dhënat tona personale se kujt ia japim ne ato dhe për çfarë arsye i japim ato, duhet vërejtur se

[24] Tiparet e përbashkëta të email-ave nga Phishingu – http://www.phishing.org/what-is-phishing (Qasur më 01/12/2018)

[25] Definicion i cituar nga AZOP (Agjencioni për sigurimin e të dhënave personale në Kroaci) shiko http://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi (Qasur më 01.12.2018)

ku i lënë dhe i japim të dhënat tona personale, pasi që nëse ne publikojmë në ndonjë nga llogaritë e rrjeteve sociale disa të dhëna personale, në ndonjë vend tjetër disa të dhëna të tjera dhe në vendin e tretë të dhëna të tjera personale, pra ne kemi arritur në nivelin më të lartë për të na vjedhur gjithë të dhënat personale, pasi që dikush që neve na ndjek mund që të lidhë të gjitha këto të dhëna dhe të keqpërdor sëbashku kundër neve. Është e rekomanduar që në qoftë se na janë vjedhur të dhënat personale, momentin e parë të mundshëm të reagojmë të njoftojmë policinë e vendit për rastin konkret me të gjithë të dhënat e mundshme që kemi që t'i ndihmojmë edhe ata në gjetjen e personit i cili ka manipuluar me të dhënat tona.

2.1.4 Përmbajtjet fyese të ndaluara

Në botën e internetit që sot surfojmë, ekzistojnë shumë informata dhe të dhëna të ndryshme të cilët kanë përmbajtje nga më të ndryshmet, si ato të dhëna të cilët mund të na ndihmojnë shumë në jetën e përditshme, poashtu kemi edhe të dhëna të cilat janë të ndaluara edhe të shfaqen. Përmbajtjet fyese më së shumti janë të ndaluara për auditoriumin e fëmijëve më të vegjël se 18 vjet, zakonisht kanë përmbajtje të përshkrimeve të aktivitetit seksual midis të rriturve, video nga më të ndryshmet ku tregohet dhuna me ndikim të lartë, xhirime që detajojnë praktikat seksuale fyese, material i cili ofron udhëzime të hollësishme për kryerjen e ndonjë krimi, etj.

Materiali ekstremist apo i ndaluar zakonisht përfshin artikuj, fotografi, fjalime ose video që nxisin urrejtjen dhe dhunën në mes njerëzve, deklarata ose postime të bëra në rrjetet dhe mediat sociale, përmbajtje që nxisin njerëzit që të kryejnë akte terrorizmi, faqet e internetit që krijohen nga organizata terroriste, materiale me anë të së cilëve mund të trajnohen terroristët, përmbajtjet e dyshimta në lidhje me përdorimin ose shitjen e drogës dhe kemikaleve të ndryshme dhe video ose imazhe të sulmeve terroriste.[26]

[26] Ndalime të cituara nga ACORN (Australian Cybercrime Online Reporting Network) që vlejnë në nivel global https://www.acorn.gov.au/learn-about-cybercrime/prohibited-offensive-and-illegal-content (Qasur më 01/12/2018)

2.1.5 Materialet on-line me përmbajte abusive seksuale të fëmijëve

Shumë njerëz e kanë të vështirë që të imagjinojnë imazhet pornografike të fëmijëve dhe prandaj nuk e kuptojnë se çfarë nënkuptohet me ‘’pornografinë e fëmijëve’’. Në shumë vende kjo quhet edhe si material për abuzim seksual të fëmijëve për të përforcuar atë se pas imazheve të pornografisë së fëmijëve ka me të vërtetë abuzim seksual të fëmijëve. Pornografia e fëmijëve ka përkufizime apo definicione të ndryshme ligjore në vende të ndryshme. Minimumi përcakton pornografinë e fëmijëve si një figurë që tregon një person që është fëmijë dhe i angazhuar ose përshkruhet si i përfshirë në aktivitete seksuale. Një nga çështjet që shkakton mosmarrëveshje, mosha e pëlqimit të mardhënieve seksuale që ndryshon nga vendi në vend dhe përveç kësaj legjislacioni ndryshon nëse posedimi i pornografisë së fëmijëve është një krim, nëse një fëmijë duhet të përfshihet dhe nëse imazhet e krijuara përbëjnë pornografinë e fëmijëve. Ekzistojnë disa mënyra të shpërndarjes së materialeve me abuzime seksuale të fëmijëve e ato janë:

Rrethet pedofilike – janë një grup personash që punojnë sëbashku në internet në vende dhe juridiksione të ndryshme me qëllim që të bëhet mbledhja dhe shpërndarja e materialeve me abuzime seksuale të fëmijëve për kënaqësinë e tyre. Ekziston një perceptim i fortë se interneti është faktor kryesor në zhvillimin e këtyre rretheve pedofilike në mbarë botën. Dënimet e fundit nëpër botë kanë mbështetur këtë përceptim dhe shpërndarja e pornografisë së fëmijëve po shkakton një shqetësim të madh për Agjencitë Ndërkombëtare të cilat janë të angazhuara në mbrojtjen e të miturve, ndërsa në anën tjetër këto të ashtuquajturit rrethe pedofilike gjithnjë e më shumë përparojnë duke përdorur mënyrat dhe metodat e fundit të teknologjisë së avancuar siç është kriptimi i të dhënave dhe ka ardhur deri tek ajo që ato gjithnjë e më vështirë zbulohen.

Ueb faqet me materiale të abuzimit seksual të fëmijëve – deri në kohët e fundit nuk kishte shumë ueb faqe të cilat mireshin me shpërndarje të materialit me abuzim seksual të fëmijëve, zakonisht edhe ato që ekzistonin ishin për kënaqësi personale apo edhe nevoja për të kërkuar persona me prirje të njejtë. Sidoqoftë, sot për fat të keq ekziston një numër i madh i ueb faqeve të cilët merren me pornografinë me fëmijë dhe më e keqja e kësaj është se dita-ditës është në rritje të madhe ku llogaritë nëpër këto faqe paguhen me metoda të ndryshme. Zakonisht këto lloj ueb faqesh vendosen në vende ku ligji nuk është shumë i ashpër në lidhje me pornografinë me fëmijë

ose në vende ku ekonomia e shtetit është e dobët. Me përparimin e teknologjisë tani është e mundur që çdokush të ketë llogari bashkë me fjalëkalime nëpër ueb faqe të ndryshme me materiale abuzive seksuale të fëmijëve, ku zakonisht këto llogari shiten me abonime ditore, javore, mujore, ose edhe vjetore. Pagesa e këtyre abonimeve bëhet nëpërmjet kredit kartelave apo kriptovalutave dhe arrihet deri tek llogaria bashkë me fjalëkalimin dhe më pas mund të hihet dhe surfohet tek një ueb faqe e caktuar jo vetëm nga kompjuteri por nga çdo aparat i mundshëm me qasje në internet qoftë celular, tablet, TV, etj. [27]

2.1.6 Mashtrimet dhe shitjet e rrejshme online

Mashtrimi në internet është përdorimi i shërbimeve të internetit dhe softuerëve që kanë qasje në internet për të mashtruar viktimat ose për të përfituar nga ato. Skemat e krimeve nga interneti vjedhin miljona dollarë në çdo vit nga viktimat duke përdorur mënyra nga më të ndryshmet dhe e keqja e kësaj është se kjo vazhdon dita- ditës dëmton internetin me metoda të ndryshme. Disa nga metodat të profilit të lartë janë:

Kompromisi i biznesit nëpërmjet email-it – Ky është një mashtrim i sofistikuar që synon apo si target i ka bizneset që punojnë me furnizues të huaj dhe kompani që rregullisht kryejnë pagesa nëpërmjet transfertave bankare elektronike. Mashtrimet zakonisht kryhen duke kompromentuar llogaritë e ligjshme të kryera nëpërmjet internetit dhe email-it në një biznes të caktuar në të cilin më pas me metoda të ndryshme dhe ndërhyrje kompjuterike ato llogari hack-ohen dhe më pas kryhen transferime të paautorizuara të fondeve nga edhe vjen dëmtimi i një biznesi dhe dëmtimi i firmave apo qoftë edhe dëmtimi i një personi të vetëm që merret me biznes.

Thyerja e të dhënave – Një rrjedhje e të dhënave që lirohet nga lokacion i sigurt në një mjedis të papërmbajtur. Shkeljet apo thyerjet e të dhënave mund të ndodhin si në nivele personale ashtu edhe në nivele të korporatave ku edhe përfshihen informacione shumë të ndjeshme, informacione të mbrojtura dhe informacione konfidenciale që të gjitha mund të

[27] Citate nga artikulli Child Sexual Abuse Material (Child Pornography) - INHOPE http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/child-pornography.aspx (Qasur më 01/12/2018)

kopjohen, transmetohen, shihen, vidhen dhe përdoren nga një individ apo grup individësh të paautorizuar për të kryer një akt të këtillë.

Mohimi i shërbimit (Denial of Service - DOS) – ndërprerje e qasjes së një përdoruesi të autorizuar në një sistem apo rrjet, zakonisht ndërprerjet me qëllime të këqija.

Kompromisi i llogarisë apo email-it – Ngjajshëm si kompromisi i biznesit, vetëmse ky lloj synon apo si target e ka publikun e gjërë apo në përgjithësi, duke mos u bazuar në institucionet financiare, kompanitë e pasurive të patundshme dhe firmat ligjore. Autorët e këtij kompromisi përdorin email-a të kompрometuar për të kryer pagesa në më shumë vende të rrejshme.

Malware – janë softuerë të krijuar me qëllime të këqija që të dëmtojnë ose çaktivizojnë kompjuterët apo sistemet kompjuterike. Ndonjëherë ndodh që të përdoren edhe taktika të frikshme nga autorët e krimit me qëllim të përfitimit të fondeve nga ana e viktimave.

Spoofing "Shakatë" / Phishing-u – të dyja nga këto kanë të bëjnë me falsifikimin e dokumentave elektronike. Zakonisht Spoofing përdoret për shpërndarje të email-it i cili është i falsifikuar për tu shfaqur sikur të ishte dërguar në emër të një personi komplet tjetër, ndërsa phishingu paraqitet si një biznes legjitim i vendosur on-line, me qëllim të marrjes së të dhënave personale si fjalkalimet, kredit kartelat dhe shumë informatave të ndjeshme nga konsumatorët apo përdoruesit e atij biznesi, që më pas të hedh apo të drejton te biznesi i vërtetë nëpërmjet linqeve.

Ransomeware – Është një formë e malware që synon apo si target të saj i ka dobësitë njerëzore dhe dobësitë teknike të organizatave ose rrjeteve individuale në përpjekje për të mohuar disponueshmërinë e të dhënave apo sistemeve. Zakonisht te ky lloj mashtrimi kriminelët bllokojnë llogaritë apo ueb faqet e një personi dhe për këtë ato kërkojnë dëmshpërblime nga ato sigurisht në monedha virtuale siç është bitcoin me qëllim që të mos kuptohet se kush e ka kryer krimin.

Shembuj të shpeshtë të cilët përfshijnë mashtrimet në internet janë mashtrimet e biznesit, mashtrimet me kredit kartela, mashtrime me ankande të ndryshme, mashtrimet me letra nigeriane dhe mos dhënia e mallrave etj.[28]

Mashtrimet e blerjeve që kryhen online – këto mashtrime përfshijnë mashtrues që pretendojnë të jenë shitës të ligjshëm në internet, poashtu paraqiten edhe me një uebfaqe të rrejshme ose edhe paraqiten me reklama të rrejshme për një dyqan elektronik i cili në të vërtetë nuk ekziston.

Derisa shumë shitës online tentojnë që të jenë dhe janë të ligjshëm, për fat të keq hakerët keqpërdorin natyrën anonime që ka interneti, për të vjedhur blerësit që nuk dyshojnë dhe lehtë manipulohen. Hakerët përdorin teknologjitë, mënyrat dhe metodat e fundit për të krijuar ueb faqe të rrejshme të shitjes me pakicë dhe tentojnë që të kopjojnë dhe të duken si ueb faqet që janë të vërteta dhe në të vërtetë merren me shitje me pakicë. Ata përdorin dizajne dhe prapavija shumë të sofistikuara, poashtu përdorin logo dhe numra të vjedhur vetëm që të arrijnë qëllimet e tyre. Dallimi më i madh i uebfaqeve të vërteta dhe këto që janë të rrejshme është tek metodat e pagesës së artikullit, aty gjithmonë ka ndryshime apo dallime që janë të dukshme dhe më ndryshe se sa që janë në shitoret e vërteta.

Mirëpo, rreziku ekziston gjithmonë pasi që ka shumë njerëz të cilët nuk bëjnë shumë blerje por dhe kur e bëjnë atë, atyre u vjen njëjtë dhe atëherë ato lehtë manipulohen dhe përpos se nuk ju vjen artikulli i porositur, ekziston mundësia që edhe kredit kartelat t'ju zbrazet. Zakonisht faqet e rrejshme kanë çmime shumë më të ulëta se sa që janë çmimet normale me qëllim që të bien në sy të publikut.[29]

[28] "Mashtrimet në internet" nga FBI https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (Qasur më 01/12/2018)
[29] Online Shopping Scams – Australian Competition & Consumer Commision https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams (Qasur më 01/12/2018)

2.2 Kronologjia e kriminalitetit kompjuterik

Si çdo lloj kriminaliteti po ashtu edhe kriminaliteti kompjuterik ka kronologjinë e saj. Pra, ekzistojnë disa lloje të krimeve kompjuterike dhe ekzistojnë disa ngjarje të cilët kanë ndodhur prej vitesh dhe janë të rëndësishme, prandaj do të kisha dashur që t'i theksoj në këtë punim. Në nëntemën e mëposhtme do të shkruaj se kur kanë ndodhur sulmet kibernetike më të mëdhaja, ndaj kujt kanë ndodhur dhe konsekuencat që kanë ndodhur.

2.2.1 Llojet e krimeve kompjuterike sipas viteve dhe ndryshimet në motivet e kryersve sipas viteve

Viti 1982 – ishte viti kur disa nga zyrtarët e sigurisë kombëtare të SHBA filluan një nga sulmet e para kibernetike në botë drejt një vendi tjetër i cili ishte Bashkimi Sovjetik. Zyrtarët e SHBA-së nëpërmjet një burimi të KGB-së të quajtur Farewell Ddosier, dëgjuan se Sovjetikët kishin për qëllim blerjen e disa paisjeve kompjuterike përmes një kompanie të përparme për të operuar një gazsjellës. Agjentët e SHBA-së ishin ato të cilët ndryshuan softuerin e tyre i cili më vonë shkaktoi shpërthimin e tubacionit.[30]

Viti 1988 – i ashtuquajturi ''Krimbi Morris'' (Worm Morris) – një nga krimbat e parë të njohur për të ndikuar në infrastrukturën kibernetike të sapolindur në botë, ky krimb u përhap te shumë kompjutera dhe kryesisht në SHBA. Krimbi përdori dobësitë e sistemit të atëhershëm ''unix 1'' dhe mundësoi vetes replikimin e shumëhershëm, pra shtimin e tij në masë të pandalshme dhe kjo solli deri te ngadalsimi deri në pikën që ato të jenë të papërdorshëm, pra 10% nga 88 000 kompjutera që ishin të lidhur me internet në atë kohë. Ky krimb u krijua nga Robert Tapan Morris i cili ishte student i univerzitetit Cornell, i cili tha se ishte duke u përpjekur të shohë se sa i madh është interneti. Mëpas ky person u bë personi i parë në SHBA që u dënua për mashtrim dhe abuzim kompjuterik. Tani personi i njejtë punon si profesor në MIT.[31]

Viti 1994 – ishte viti kur grupa e Anonymous në mënyrë të përsëritshme sulmuan Laboratorinë e forcave ajrore të Romës në New York, duke nënvizuar edhe kërcënimin ndaj

[30] The Farewell Dossier – Gus W. Weiss - CIA https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm (Qasur më 01/12/2018)
[31] Historia e sulmeve kibernetike (The history of cyber attacks) – a timeline – NATO https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm (Qasur më 01/12/2018)

sistemeve ushtarake. Hetuesit e kësaj ngjarje zbuluan se një adoleshent britanik dhe një teknik izraelit kishin përdorur sisteme dhe rrjete telefonike në tetë vende të botës për të mbuluar anonimitetin e sulmeve të tyre në sistemet ushtarake dhe qeveritare.[32]

Viti 1997 – ishte një viti kur Pentagoni i Shteteve të Bashkuara bëri një test apo një ushtrim të luftës informative dhe nga kjo zbuloi se sistemet industriale dhe informative në të gjithë Shtetet e Bashkuara të Amerikës janë të cenueshme ndaj sulmeve kibernetike të ushtruara nga hakerët që përdorin gjithmonë teknologjinë e fundit në dispozicion. Specialistët thanë se sulmet e stimuluara në rrjetet e energjisë dhe komunikimit në disa shtete u arritën me shumë lehtësi.[33]

Viti 2003 – Ishte viti kur hakerët supozohet se të mbështetur nga Kina sulmuan sistemet ushtarake dhe qeveritare të SHBA dhe nuk u ndëshkuan. Këta hakerë sollën deri te shuarja dhe fshierja e aq shumë të dhënave sa që kaluan shumë terabajt. Këta sulme nga zyrtarët e SHBA-së u quajtën Titan Rain.[34]

Viti 2007 – Ishte një ndër vitet më të rënda për shtetin e Estonisë, pasi që gjatë një mosmarrveshje në mes Rusisë dhe Estonisë, hakerët rus nisën sulmet masive ndaj agjencioneve qeveritare, bankave, gazetave dhe organizatave të tjera të njohura estoneze, duke përdorur një rrjet të madh kompjuterësh për të arritur deri tek shuarja apo fikja totale e internetit në gjithë Estoninë. Disa nga analistët e njohur paraqitën këtë akt të Rusisë si një nga rastet e para të luftës kibernetike në gjithë botën.[35]

Nga viti 2010 e deri në ditët e sotme kemi një numër të madh të ndërhyrjeve nga ana e kriminelëve nëpër sisteme apo rrjete kompjuterike si zbulimi i krimbave dhe viruseve të reja, një humbje e madhe prej 170 milionë dollarë në kompaninë e Sony-it në vitin 2011 dhe shumë e shumë ndërhyrje tjera që nuk mund të përfshihen në një punim të tërë por nga e gjithë kjo kuptojmë se gjatë historisë apo kronologjisë së krimit kibernetik shihet qartë se motivet kanë qenë

[32] Information security: Computer Attacks at Department of Defense Pose Increasing Risks – GAO fq.3
[33] Cyberwarfare – CRS Report for Congress viti 2001 fq.4
[34] Artikull nga WashingtonPost me titull ''Hackers attack via Chinese Web Sites'' nga autori Bradley Graham në vitin 2005 http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html (Qasur më 01/12/2018)
[35] Kremlin Kids – We launched The Estonian cyber war https://www.wired.com/2009/03/pro-kremlin-gro/ (Qasur më 01/12/2018)

nga më të ndryshmet dhe së pari kanë qenë si zbulime se çka mund të arrihet me përdorimin e internetit, e më pas si luftë kibernetike ndërmjet shteteve e në vitet e fundit kriminalitetin kompjuterik e shohim më së shumti si kriminalitet i cili dëmton më së shumti ekonominë qoftë të një personi ose më shumë personave e deri në dëmtimin e miliona e miliona organizatave ose firmave nga më të ndryshmet duke u ndjekur më pas edhe tek dëmtimi i të dhënave sekrete të një shteti, pra kriminaliteti kompjuterik në kohë të fundit përdoret si biznes për përfitime materialiste qoftë personale apo për dikënd tjetër.

2.2.2 Statistikat e rritjes së shfrytëzuesve të internetit dhe rritja e krimeve nëpërmjet shfrytëzimit të tij

Duke ditur se përdorimi i internetit nga njerëzit është në një numër jashtëzakonisht të madh, duhet ditur nga ana tjetër se rritet edhe numri i krimeve të cilat kryhen nëpërmjet kompjuterit nga persona që kryejnë atë për përfitime personale, përfitime të dikujt tjetër apo edhe për të treguar sjelljen e tyre egoiste apo kriminale. Krimi kompjuterik është në një rritje të jashtëzakonshme me një numër prej 600 miliard dollarë në vit në rajon global, e cila vlerë është ngritur për 200 miliard dollarë në vetëm 3 vitet e fundit.[36] Shifër e cila pak sa na çon të mendojmë se sa në të vërtetë është ky lloj kriminaliteti i rrezikshëm dhe çfarë në të vërtetë qëndron pas arsyes së rritjes së këtij krimi. Duke ditur se ekzistojnë afër 430 miljon tipe të maluerit, krimi kibernetik përbën një kërcënim të vërtetë dhe të vazhdueshëm ndaj bizneseve, qeverive, dhe institucioneve financiare. Sulmuesit dalëngadalë po zbulojnë të gjitha mënyrat dhe metodat e paisjeve që të mund t'i përdorin ato për të sulmuar të tjerët, ku numri dhe sofistifikimi i sulmeve gjithashtu po rritet.

[36] Statistika të marrura nga artikulli ''Global Cyber Crime Hits 600 billion – Gets Its Own aaS Category'' i Meritalk – artikull i postuar më 08 Mars 2018 që ka për qëllim përmisimin e rezultateve të qeverisjes https://www.meritalk.com/articles/global-cyber-crime-hits-600-billion-gets-its-own-aas-category/ (Qasur më 02/12/2018)

2.3 Botnet-i

2.3.1 Definicioni dhe strukturat

Botneti është një koleksion i përdoruesve të kompjuterëve të lidhur në internet, të cilët janë të infektuar nga një virus me qëllim të keq që quhet malware, i cili virus i lejon krijuesit të bëjë kontrollimin e kompjuterëve nga distanca nëpërmjet të një serveri përmes së cilit mund të komandojë dhe kontrollojë që të kryhen detyra të automatizuara, të kryhet vjedhje e informacionit të viktimës, të kryhet sulm ndaj kompjuterëve tjerë apo ueb faqeve të ndryshme, pra me një fjalë krijuesi spiunon viktimën pa vetëdijen e viktimës për përfitime të veta. Botneti është i dizajnuar në atë mënyrë që krijuesi i saj të mund të komandojë apo kontrollojë me më shumë kompjutera dhe të spiunojë ato në të njejtën kohë[37]. Me ndihmën e metodave të komunikimit siç është IRC, krijuesit e botnetëve mund që të bëjnë infektimin e një numri të madh të kompjuterëve dhe t'i dirigjojnë ato për të kryer aktivitete kriminale.

Faza e krijimit të botnetit varet shumë edhe prej aftësive por edhe prej kërkesave të sulmuesit i cili do të krijoj rrjetin e botnetit. Sulmuesi mund që të krijon vetë kodin, të marrë ndonjë bot të shpërndarë apo të rregullojë ndonjë bot të vjetër. Mirëpo në qoftë se personi nuk din që të krijojë kode atëherë ai e ka një mundësi tjetër e cila është blerja e kodeve në internet, pasi që ekzistojnë shumë forume hakerësh që krijojnë botët i konfigurojnë dhe në fund i shesin ato. Për krijim të bot-ës përdoret programi që është për programim C++, pas krijimit të bot-ës krijuesi duhet që të gjejë metodën për të bërë shpërndarjen e bot-ës, një ndër metodat për shpërndarjen e bot-ës është ngjitja e bot-ës me një nga programet të cilët shkarkohen më së shumti në përditshmëri.

Ekzistojnë programe që bëjnë ngjitjen e programit bashkë me virusin dhe si procedurë e fundit që duhet kryer te kjo metodë është që virusi të bëhet i padukshëm për antivirusin, edhe kjo arrihet përmes një programi tjetër që mban emrin crypter dhe së fundmi bot-i apo virusi bëhet FUD[38]. Shpërndarja e bot-ës kryhet edhe në mënyra të ndryshme siç janë shpërndarja nëpër

[37] Internet society "Botnets" 30 Tetorë 2015 cit. fq 1 apo linku i mëposhtëm https://www.internetsociety.org/wp-content/uploads/2017/07/ISOC-PolicyBrief-Botnets-20151030-nb.pdf (Qasur më 02/12/2018)
[38] Shkurtesë nga Full Undetectable që në shqip do të thotë plotësisht i pazbulueshëm

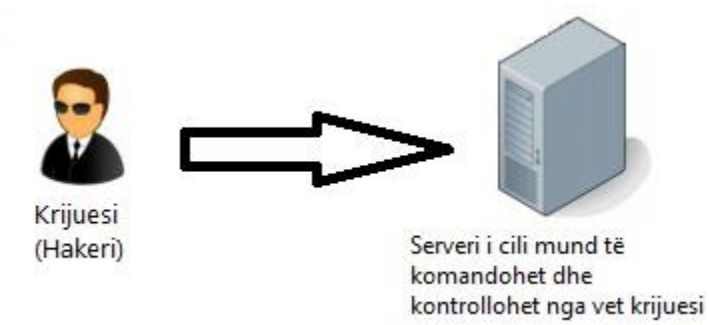
rrjetet sociale (Facebook, Instagram, Twitter, etj), shpërndarja nëpër email, etj. Pasi që sulmuesi e zgjedh qasjen e duhur ai fillon edhe me sulmin e tij[39].

2.3.2 Funksionimi i Botnet-it

Botneti është një aplikacion i cili krijohet dhe futet në përdorim nga një haker siç e sqarova edhe më lart dhe nëpërmjet të disa ilustrimeve do të tregoj mënyrën se si funksionon ai:[40]

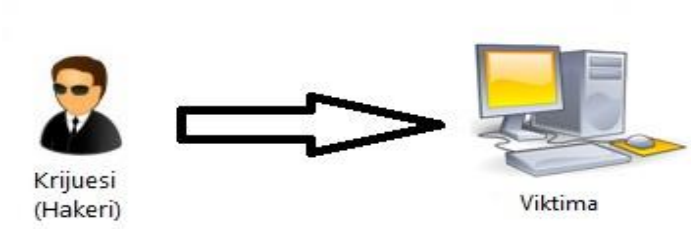
1.Së pari krijuesi (hakeri) e konfiguron bot-in e tij, pra ja jep funksionet që duhet t'i kryej dhe më pas i jep direkcionet se në cilin server të futet ai.

Ilustrimi 1



2. Për të infektuar kompjuterin me bot duhet që të hapet apo lexohet bot-i në kompjuter dhe këtë e kryen hakeri duke infektuar kompjuterin e viktimës.

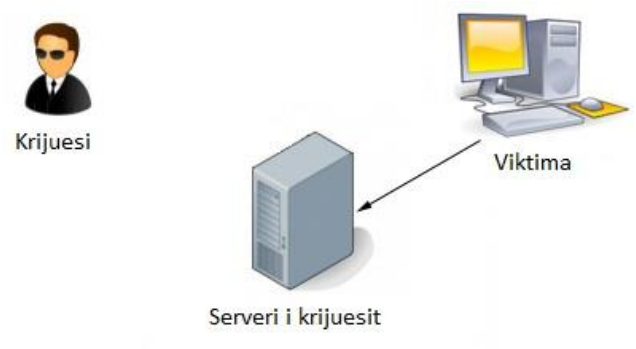
Ilustrimi 2



[39] Tutorial nga një ndër forumet më të njohur të hakerëve hackforums.net https://hackforums.net/showthread.php?tid=4772281&highlight=botnet (Qasur më 02/12/2018)
[40] Ilustrime nga Tyler Hudak i KoreLogic, "An introduction into the world of Botnets" shkarkuar 12 Mars 2017 cit. fq. 6

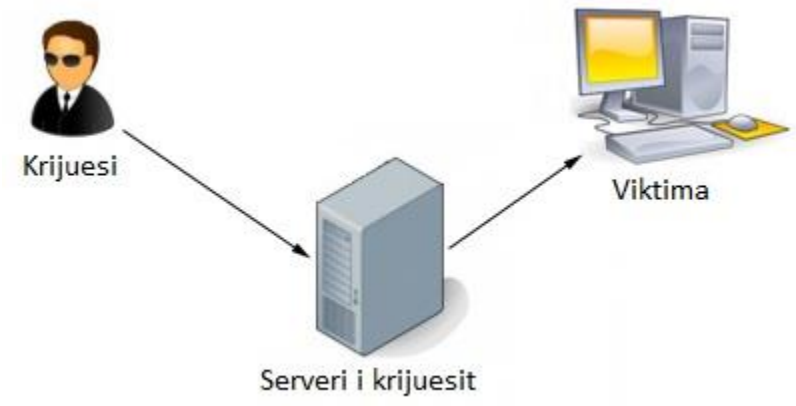
3. Në fazën e tretë kompjuteri i infektuar (kompjuteri i viktimës) përmes bot-ës lidhet në serverin që mund të kontrollohet dhe komandohet nga vetë krijuesi, e kjo mund të kryhet përmes IRC, HTTP dhe protokoleve tjera.

Ilustrimi 3



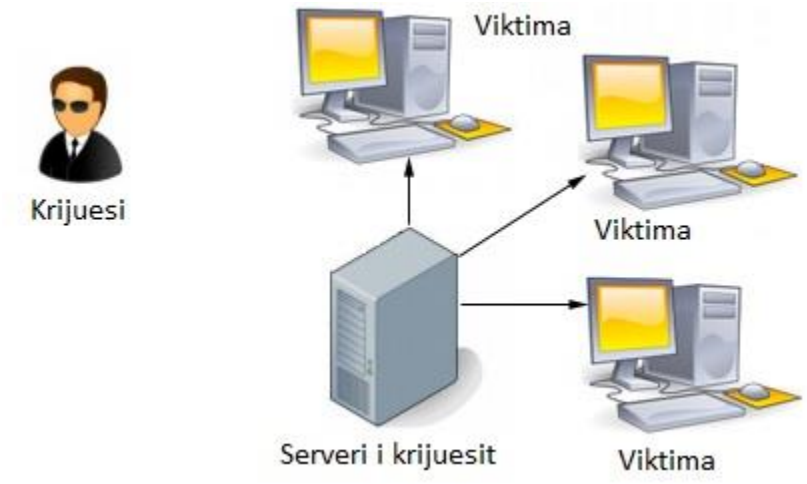
4. Në fazën e katërt pas krijimit të suksesshëm të rrjetit botnet, krijuesi dërgon komandat përmes serverit të tij tek kompjuteri i infektuar i viktimës dhe fillon që të kontrollojë, spiunojë apo keqpërdorë atë.

Ilustrimi 4



Kjo fazë vazhdon të përsëritet derisa krijuesi i botnetit formon një ushtri viktimash, të cilën ai e kontrollon vetëm nga një pikë (serveri i vetë krijuesit).

Ilustrimi 5



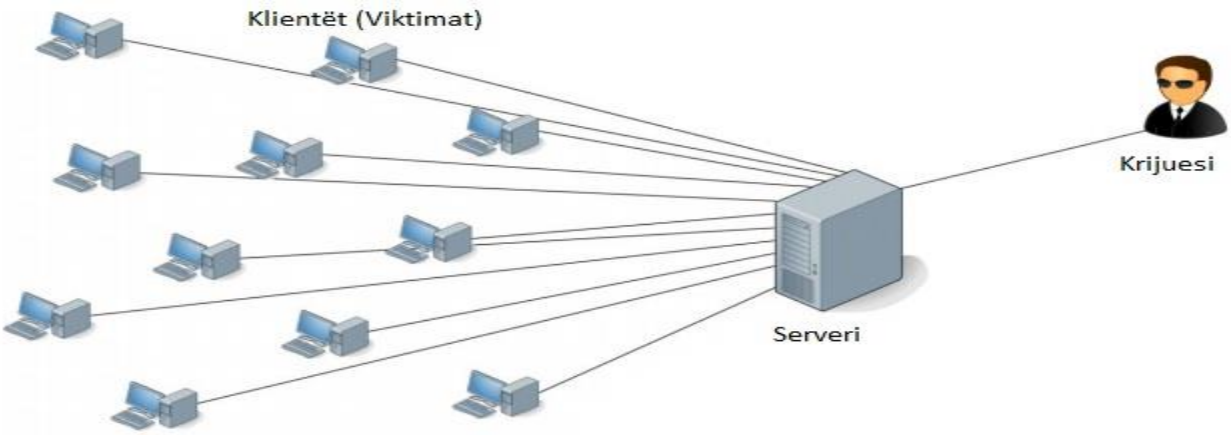
Përveç ilustrimeve të shfaqura në lidhje me krijimin dhe shpërndarjen e botnet-it, ekziston mundësia që tre fazat e para të jenë të njëjta, por fazat tjera të ndryshojnë shkaku i asaj se krijuesi mund t'ua shesë personave të tretë apo të japi me qira serverat e gatshëm, të cilët janë përplot të mbushur me viktima të cilët mund të komandohen edhe nga personat e tretë.

2.3.3 Strukturat e botnetit

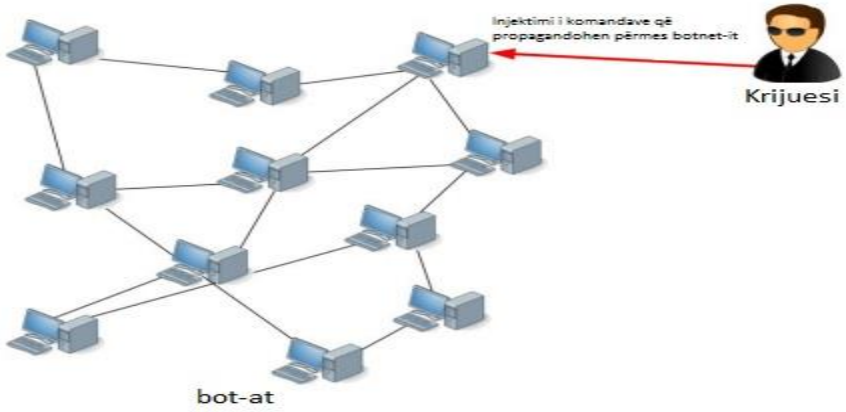
Ekzistojnë tre lloje të strukturave të botnetit, ato janë:

1. **Struktura qendrore** – ky botnet është i ndërtuar në themel të sistemit klasik me shemën klient-server. Në botnetet e këtilla bot-at veprojnë si klientë dhe lidhen në një ose më shumë serverë qendrorë, të cilët servera janë nën komandën dhe kontrollën e bot-krijuesit. Me lidhjen e më shumë bot-ëve në këtë server bot-krijuesi mund që njëherësh të komunikojë dhe t'ju japë komanda të gjithë bot-ëve që janë online në server, të cilët më pas përcjellin urdhërin e krijuesit te klientët.[41] Struktura e këtillë pasi që është në një lidhje direkte mundëson reagim për një kohë të shpejtë dhe një koordinim mjaft të mirë, poashtu mundëson monitorim të thjeshtë të statusit të botnet-it dhe siguron numrin e bot-ave që janë aktive. Në mënyrë ilustrative do të dukej kështu[42]:

[41] ENISA "Botnets" e publikuar më 07 Mars 2011 nga autorët Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder, cit fq. 15 https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence (Qasur më 02/12/2018)
[42] Foto ilustruese nga Enisa "Botnets" fq.15 të përpunuara nga vetë unë në gjuhën shqipe



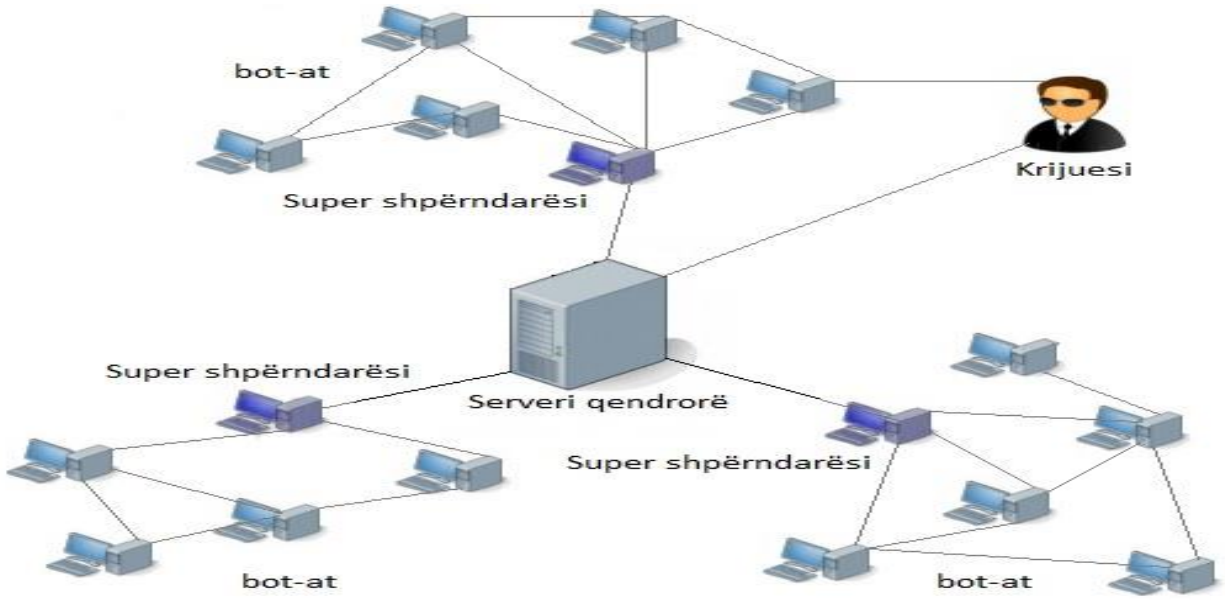
2. **Struktura P2P** – tek ky lloj i botnetit është interesant pasi që secili kompjuter i infektuar me bot njëkohësisht reagon edhe si klient edhe si server dhe kjo domethënë se në këtë lloj strukture nuk ekziston një server qendror real si në strukturën qendrore, por flitet për një strukturë të decenteralizuar. Domethënë që në vend që bot-i të konektohet si klient në server qendror, ai i bashkohet rrjetit duke kontaktuar me kompjuterin e infektuar, por për tu arritur një gjë e tillë duhet që së paku të ketë një kompjuter i cili përdoret për lidhje të botnet-it[43]. Në këtë sistem ka një mangësi pasi që nuk mund të merren informata direkte në lidhje me të gjithë botnetin dhe komandat apo urdhrat mund të jepen vetëm në njërin prej kompjuterave, mirëpo për dallim nga botneti me strukturë qendrore, kjo strukturë e botnetit mjaft rëndë zbulohet por edhe më rëndë prishet. Në mënyrë ilustrative do të dukej kështu[44]:



[43] ENISA "Botnets" e publikuar më 07 Mars 2011 nga autorët Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder, cit fq. 18 https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence (Qasur më 02/12/2018)

[44] Foto ilustruese nga Enisa "Botnets" fq.18 të përpunuara në gjuhën shqipe nga vetë unë

3. **Struktura hibride** – kjo strukturë në fakt është kombinimi i strukturës qendrore me atë p2p. Deri tek kjo strukturë ka ardhur me qëllim që të mbulohen të gjithë gabimet e strukturës qendrore dhe asaj p2p. Në ilustrimin në vazhdim do të shihet qartë se si kjo strukturë funksionon, do të shohim se kemi më shumë lidhje p2p dhe të gjitha ata lidhje të bashkuara në një server qendror. Krijuesi i bot-ës mundet që të urdhërojë apo të dërgojë komandat e tij përmes serverit qendror por edhe nëpërmjet njërit prej kompjuterëve të infektuar që më pas shërben si server i kompjuterëve tjerë[45].



[45] Foto ilustruese nga Anita Laktašić "Hyrje në Botnet"
http://security.foi.hr/wiki/index.php/Botneti_i_napredni_oblici_malwarea_-_analiza_zeus_/_spyeye_sourcea#Definicija_botneta

Krahasimi i strukturave

Në bazë të karakteristikave më të rëndësishme të tre strukturave të botnetit, është bërë një krahasim nga Instituti për Internet dhe Siguri në vitin 2009 në Gjermani dhe rezultatet janë të shfaqura në mënyrë tabelare si vijon:

Tabela nr 1

Tabela e krahasimit të strukturave të botnetit nga Instituti për Internet dhe Siguri

	Serveri qendrorë	**Serveri P2P**	**Serveri hibrid**
Detektimi	I lehtë	I rëndë	Mesatar
Elasticiteti	I vogël	Tepër i lartë	Goxha i lartë
Gjendja latente	E ulët	Goxha e lartë	Mesatare
Gjetshmëria	Goxha e rëndë	Shumë e rëndë	E rëndë
Pajtueshmëria	E lehtë	Mesatare	E lartë
Përvoja	Shumë e madhe	Mesatare	S'ka përvojë

2.3.4 Sulmi DDoS

a) Sulmi DDoS (Distributed Denial of Service) – është sulm mjaft i organizuar nga qindra apo mijëra kompjutera të infektuar përnjëherë, të cilët për qëllim kanë mbingarkimin e ueb serverit, rrjetit apo ndonjë pjese tjetër të infrastrukturës dhe në këtë mënyrë pamundësohet hyrja e përdoruesve apo klientëve tjerë në po të njëjtin vend që sulmohet. Shembull sulmi DDoS direkt në link pamundëson qasjen në internet nga klientët tjerë, ndërsa sulmi DDoS në server sjell deri tek "rënimi" i një ueb faqes[46]. Sulmi DDoS është shfaqur në fillim të këtij mileniumi dhe nga viti në vit shfaqen edhe më shumë, janë shumë më voluminoz dhe më intenziv. Shumë rëndë parandalohen, shumë lirë mund të gjenden në tregun e zi dhe mund të kenë pasoja afatgjate dhe shkatërruese.

Sulmi DDoS zakonisht përdoret për të dërguar sistemin në gjendje jostabile, që më vonë të

[46] Definicioni dhe mbrojtja nga Ddos – artikull i shkruar nga specialist të IT për siguri në Sërbi shiko linkun http://www.it-klinika.rs/blog/sta-su-ddos-napadi-i-kako-se-odbraniti (Qasur më 03/12/2018)

përdor ndonjë dobësi të sistemit dhe në fund të hijë në të, pra si sulm është mjaf sulm serioz. Nga ky lloj i sulmit mund të jenë të kërcënuar të gjithë personat që kanë ueb faqe, institucionet shtetërore, kompanitë, por edhe individët. Motivet për këtë lloj sulmi zakonisht janë aktivistë politik, fetarë apo nacionalist, ka edhe prej atyre hakerave të cilët bëjnë prova të ndryshme, apo edhe kryejnë sulmin DDoS për argëtim. Sulmi DDoS për hakerin i cili sulmon është mjaft i lirë dhe mund që të kushtojë prej 10 deri në 1000$ për një ditë dhe mjaft lehtë mund të arrihet deri tek këto botnet-a, mirëpo në anën tjetër për kompanitë dhe për sigurimet të cilët miren me këto lloj sulmesh mund që të kushtojnë me një shumë mesatare deri në 22000$ për një minutë[47].

2.3.5 Kundërveprimet e nevojshme në lidhje me Botnet-in

Botnetët paraqesin një sfidë të madhe në komunitetin e internetit pasi që sulmuesit përdorin mjetet më të mira të mundshme, që bën edhe më të rëndë luftën kundër botnetëve dhe zbulimin e krijuesve të tyre. Për këtë gjë ekzistojnë disa mënyra me të cilat mund që të mbrohemi para se të jemi të infektuar me një nga virusët apo bot-at, të cilët mund të na sjellin shumë dëme materiale dhe financiare. Një nga mënyrat primare preventive është që së pari duhet që të shohim gjendjen e antivirusit, nëse ne si individë kemi një antivirus apo antimalware të instaluar në kompjuterin tonë dhe më pas duhet që të veprojmë. Nëse nuk kemi një antivirus apo antimalware të installuar duhet që në momentin e parë të mundshëm të shkarkojmë atë nga uebfaqe serioze dhe oficiale e jo nga kompanitë e dyta, treta, etj. Ndërsa nëse kemi antivirus të installuar duhet që zakonisht të shohim se nëse është i përditësuar, a është valid, a ka një licencë valide dhe a është antivirus i paguar apo është falas.

Mënyrë tjetër e rekomanduar nga microsoft është vendosja e passwordëve (fjalëkalimeve) të komplikuar dhe mbajtja e tyre sa më sekret, pra sa më pak persona të dinë për fjalëkalimin tuaj aq më i vogël është rreziku nga kriminaliteti, poashtu nuk duhet që asnjëherë të bëjmë fikjen e firewall-it në kompjuterin tonë dhe së fundmi duhet që t'i kontrollojmë usb e ndryshme që fusim në kompjuterët tonë, pasi siç dimë edhe usb mund të sjellin infektime nga më të ndryshmet tek

[47] The Ponemon institute study "Cyber security on the offense" publikuar Nëntor 2012, cit. Fq. 2 apo shiko https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf (Qasur më 03/12/2018)

kompjuterët tanë[48]. Nëse ka ardhur deri tek ajo që kompjuteri është infektuar nga një bot duhet që sa më parë të intervenojmë duke kryer fshirjen e files apo skedarit, duke desinfektu ato me antivirus apo antimalware. Në qoftë se asnjëra nga këto nuk ndihmon dhe ne shohim se ende kemi probleme dhe simptoma në kompjuterin tonë (të cilat mund të jenë si ngadalsim i dukshëm i kompjuterit tonë, përdorimi i memorjes dhe diskut me maksimum fuqi në mënyrë të pandalshme, hapja e reklamave të ndryshme pa shtypur ndonjë sustë, ndezja e kamerës kohë pas kohe, etj[49]) atëherë ne duhet që sëpari të konsultohemi me ndonjë specialist të IT-së dhe më pas të kryejmë edhe një formatim të kompjuterit tonë (nëse specialisti e sheh të nevojshme këtë) sa më parë që të mundemi pasi që çdo vonesë mund të sjellë pasoja edhe më të rënda dhe nga më të ndryshmet[50].

2.4 Deep web – si rrjet i veçantë

2.4.1 Definicioni dhe mënyra e qasjes në Deep Web

Deep web që në përkthim në gjuhën shqipe i vjen ueb i thellë është përshkrim i paqartë i internetit që është i pa arritshëm për motorët kërkimorë siç janë Google, Yahoo dhe Bing. Gjatë surfimit të internetit zakonisht deep web-in e kemi përpara neve por ne mund që mos dimë asgjë për atë. Mënyra e vetme që një përdorues i internetit të ketë qasje në këtë pjesë është duke e shkarkuar shfletuesin Tor, I2P ose Freenet. Këto surfues përdoren shkaku i asaj që të mbulohet ip adresa e cila është unike për çdo aparaturë e cila kyçet në internet me qëllim që të mos dihet se kush është kyçur për shkaqe sigurie si nga personat tjerë po ashtu edhe nga shërbimet sekrete dhe policia.

Duke u bazuar në studimet e kryera dhe të shfaqura në internet nga Universiteti i Kalifornisë në vitin 2001 kur edhe për herë të parë u përdor fjala deep web u pa se deep web-i ka një përmbajtje përafërsisht prej 7.5 petabytes, ku sot thuhet se përafërsisht sot ka material prej

[48] Artikull nga Microsoft-i "How to better protect your Pc from botnets and malware" https://www.microsoft.com/en-us/safety/pc-security/botnet.aspx (Qasur më 03/12/2018)
[49] Artikull elektronik i publikuar on-line nga Microsoft-i "How to detect malware symptoms" https://www.microsoft.com/en-us/safety/pc-security/malware-symptoms.aspx (Qasur më 03/12/2018)
[50] Artikull elektronik i publikuar on-line nga Microsoft-i "Antivirus Protection and how to avoid viruses" https://www.microsoft.com/en-us/safety/pc-security/antivirus.aspx (Qasur më 03/12/2018)

7,9 zettabytes[51]dhe duke ditur se google ka vetëm 8 miliardë faqe shihet se vetëm 4% e internetit është e dukshme për publikun dhe një pjesë e madhe prej 96% e internetit është e fshehur në një errësirë e cila nuk është në dukje për publikun[52]. Pra, me fjalë të tjera interneti është si një akull apo ajsberg në mes të oqeanit ku mund të shihet vetëm pjesa e sipërme që mund të jetë një pjesë mjaft e vogël dhe pjesa më e madhe është ajo pjesë e cila nuk është e dukshme me sy pra është e fshehur nën oqean.

Zakonisht faqet e deep web-it mbarojnë me .onion dhe nuk janë të lehta dhe të ngjajshme si ueb faqet të cilat surfojmë ne çdo ditë dhe kërkojmë ato në google. Shumicën e rasteve janë me shkronja dhe numra dhe janë të pakuptimta kur shkruhen, gjë që bën edhe më të rëndë gjetjen e këtyre faqeve dhe zbulimin e tyre nga ana e shtetit. Si qëllim kryesor i deep webit është privatësia e klientëve të tij edhe atë nga hyrja e deri në dalje të surfimit të faqeve të tij. Përmbajtjet të cilët i kanë faqet e deep uebit janë përmbajtje mjaft të këqija për auditoriumin e sidomos për fëmijët apo adoleshentët që janë në moshat ndër 18 vjeçare.

2.4.2 Rreziku dhe shit-blerjet e mundëshme në Deep Web

Blerja e librave të cilët janë të ndaluara për t'u lexuar, blerja e kredit kartelave të vjedhura, letërnjoftimeve të rrejshme, pasaportave të falsifikuara, blerja dhe dorëzimi deri në shtëpi i secilës lloj droge me vetëm një klikim të miut në afat prej disa ditëve, blerja e armëve nga më të ndryshmet, porositja e vrasjeve me pagesë, bisedat e ndryshme dhe shkëmbimi i informacioneve sekret në mes gazetarëve nga shtetet më të cenzuruara, porositja e përdhunimeve të ndryshme të cilat kryhen on-line dhe me pagesë, larja e parave dhe shumë e shumë krime nga më të ndryshmet dhe më të rëndat kryhen në deep ueb.

Në deep ueb po ashtu ekziston rreziku i madh që një klient apo person amater që të jetë viktimë e dikujt pasi që me anë të viruseve të ndryshme mund që t'ju sulmojë dikush tjetër dhe pa vetëdije të jepni të gjithë passwordet e mundshme nga të dhënat dhe informatat personale. Të

[51] Zettabyte është e barabartë me 1 miljon petabyte e cila është e barabartë me 1 miljon gigabyte
[52] Bergman, Michael K (August 2001) "The Deep Web: Surfacing Hidden Value" Zhurnal i publikuar online https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104 (Qasur më 03/12/2018)

gjitha këto shit-blerje të mundëshme që përmenda më lart dhe shumë e shumë krime të tjera kryhen në deep ueb, gjë që na çon të mendojmë se sa e rrezikshme dhe sa mirë e komplikuar dhe sa rëndë për tu zbuluar është kjo strukturë e deep uebit. Kuptohet se për tu kryer të gjitha këto shit-blerje duhet përdorur para, mirëpo me dërgimin e parave ndërmjet personave me emra të vërtetë dhe kredit kartela të vërteta do të kuptohej shumë lehtë nga ana e policisë se kush merret me kësisoj krimesh, prandaj kjo solli deri tek formimi i disa valutave të reja elektronike të cilat mund të krijohen edhe pa asnjë të dhënë personale reale apo të dhënë të saktë. Disa nga këto valuta janë Bitcoin, Onecoin, Ripple (XRP), Ethereum, e shumë e shumë valuta të tjera të cilat dita e ditës formohen.

Ndër më të njohurat dhe me më shumë vlerë është bitcoin e cila valutë mund të dërgohet edhe pranohet pa asnjë të dhënë se kush e ka dërguar apo kush e ka pranuar pasi që përdoren dërgues dhe pranues të kryptuar, pra me më shumë se 30 shkronja, gjë që bën zbulimin e dërguesit apo pranuesit të parave dhe zbulimin e organizimit të krimit shumë më rëndë. Valuta e bitcoin është shfaqur për herë të parë në vitin 2008 dhe për herë të parë është përdorur në vitin 2009 dhe është valuta elektronike e parë e shfaqur ndonjëherë, është mjaft e ndryshueshme dhe dita-ditës është në një rritje të hatashme, ku në fillim ishte afër 0.2 dollarë për vetëm 1 bitcoin e tani vlerën e ka afër 3750 dollarë[53] e dikund në shtator të vitit 2017 bitcoin pati vlerën prej 20000 dollarë.

2.4.3 Diferenca e Deep Web-it me motorët tjerë kërkimor

Gjithçka apo secila informatë e dhënë që është e ndaluar në google dhe motorët tjerë kërkimor në internet mund të gjendet vetëm në deep ueb. Të gjithë motorët kërkimor si google, yahoo apo bing nga më të njohurat e shumë motorë tjerë më pak të njohur, kanë gati të dhënat e njëjta si lajme, muzika, video të ndryshme, rrjetet sociale të gjitha këto i indeksojnë linqet dhe na lejojnë që shikojmë rezultatet e kërkimeve tona, ndërsa për dallim nga këta motorë kërkimorë Deep uebi nëpërmjet BrightPlanet-it[54] e cila pas kërkimit të ndonjë sendi në internet faqe bën nxjerrjen e gjithë përmbajtjes e cila bazohet në tekst nga secila faqe e rezultateve dhe më pas

[53] Vlera e bitcoin e kontrolluar më 19/12/2018 në faqen e kryptovalutave https://www.coindesk.com/price/bitcoin
[54] Super motor kërkimorë apo faqe e deep uebit që përdoret për informata nga më të ndryshmet

bëhet përgatitja e përmbajtjes për disa lloje të analizave, varësisht nga kërkesat e përdoruesve të fundit apo klientit të fundit që ka qasur atë kompjuter.

Google dhe motorët tjerë kërkimorë janë mjaft mirë të organizuara dhe avansuara për gjetjen e ueb faqeve të cilat janë në sipërfaqe, për përgjigje të pyetjeve të lehta si shembull deri sa orë punon një shitore le të themi Burger King, apo sa cm është 1 metër e kështu me radhë, mirëpo kur vjen deri tek ajo që një person apo kompani të bëjë pyetjen se kush e shet produktin tim online nëpër botë si replikë? Cilët janë pacientët që testojnë drogën time dhe çfarë mendimi kanë ata për këtë lloj droge? Sa është çmimi i aksioneve të një kompanie? Cili hulumtim i ri i kancerit që është publikuar muajin e kaluar dhe çka thonë njerëzit për këtë hulumtim? Atëherë vjen deri tek ajo që duhet marrë përgjigjet nga Deep uebi pasi që metodën e kërkimit dhe informatat të cilët posedon deep uebi arrijnë që tu përgjigjet gati gjitha pyetjeve të mundshme.

Ja edhe disa shembuj ku vërtetohet se deep uebi dallon dukshëm nga të gjithë motorët tjerë kërkimorë:

- Gazetat – Në vend që të kërkojmë uebfaqen e gazetës me emrin e saj, grupi i gazetave te raporti burimor i deep uebi-t përfshin çdo gazetë në SHBA dhe në pak sekonda deep ueb apo më saktë Brightplanet sjell përmbajtjet apo të gjitha temat, duke përfshirë edhe ato më specifike nga çdo gazetë në SHBA dhe, përveç kësaj, gazetat renditen sipas shtetit që kërkimi jonë të përshtatet sipas nevojave tona.

- Ligji – Brenda këtij grupi ka disa kategori. Një nga këto kategori janë gjykatat. Ky grup përfshin burime që na lejojnë të kërkojmë vendimet e gjykatave te të gjitha nivelet e degës gjyqësore, shtetërore, lokale dhe federale dhe të gjitha këto në një çast do të shfaqen para ekranit tonë.

Financat dhe Marketet – që përdoruesit mos të merren me blerjen e thashethemeve, shitjen e lajmeve ato mund të gjejnë edhe thashethemet edhe lajmet shumë më shpejt se sa mund t'i shohin në Lajme, Ueb faqe të financave, bordin e financave dhe blloqet tjera specifike të industrisë.[55]

[55] Citate nga ueb faqe e deep web-it http://www.brightplanet.com (Qasur më 03/12/2018)

2.5 Kiber terrorizmi

2.5.1 Definicioni dhe tipet e kiber terrorizmit

Përfshirja e krimeve të terrorizmit që kryhen në mënyrë elektronike kundër individëve, bizneseve, organizatave dhe kundër vetë qeverisë paraqet kiber terrorizmin. Shumica e informatave nga jetët tona sot është e përfshirë në internet, duke filluar nga të gjithë të dhënat e mundëshme që shkruajm në CV-të tona, llogaritë bankare, dosjet tona mjekësore dhe shumë e shumë sende tjera. Me një lehtësi të madhe dhe nga mosdija ne japim të gjithë këto të dhëna për vetëm pak çaste nëpër shumë ueb faqe jo të sigurta, gjë që bie shumë lehtë tek terrorizmi kibernetik. Duhet menduar prej te vetja jonë se sa nga të dhënat tona sot janë të shfaqura në internet, kush na mbron të gjithë këta të dhëna të cilët ne kemi shkruar në internet, çfarë na mbron nga vjedhja e këtyre informatave të cilët ne kemi shfaqur on-line dhe shumë e shumë pyetje të tjera të cilët mund të jenë si një preventivë nga mbrotja e të qenurit të hakuar dhe nga mbrotja e kiber terrorizmit.

Një terrorizëm kibernetik mund të ndodhë mbi një internet publik, mbi një server privat, apo edhe mund të ndodhë nëpërmjet rrjeteve të siguruara të qeverisë. Ekzistojnë shumë mënyra dhe mjete të ndryshme me anë të së cilëve një kriminel mund të frikësojë dhe dhunojë një person tjetër. Shumë më lirë dhe më mirë i del një krimineli që të blej vetëm një kompjuter se sa që të blejë armë apo bomba dhe të rrezikojë veten në raport direkt, gjë që solli tek interesimi shumë i madh i kriminelëve nga e gjithë bota, pasi që krimi mund të kryhet edhe pa mos qenë në vend ngjarje, mund të kryhet nga çdokush pa marrë parasyshë moshën dhe gjininë, pa marrë parasyshë shtetin se ku ndodhet ai ose ajo mund që të kryej një krim mjaft të rëndë dhe mund të jetë anonim gjatë gjithë kohës.

Ekzistojnë tre tipe të aftësive për të kryer terrorizëm kibernetik, e ato janë:

- Tipi i thjeshtë dhe i pa strukturuar – që përfshin aftësinë për të kryer një ndërhyrje kundër një sistemi individual, duke përdorur mjete të gatshme të krijuara nga dikush tjetër, ku organizata mund të posedojë pak informata nga targeti, mund të komandojë dhe kontrollojë ose të mësojë diçka nga kjo ndërhyrje e palejuar apo ndryshe e quajtur hacking.

- Struktura e avancuar – përfshin aftësinë për të kryer sulme më të sofistikuara ndaj sistemeve dhe rrjeteve të shumëfishta, e ndoshta edhe me mundësi për të modifikuar ose krijuar mjete themelore të piraterisë. Te ky rast organizata posedon një analizë elementare të objektivave, poashtu posedon komandën dhe kontrollin dhe aftësinë e të mësuarit.

- Kompleksi i kordinuar – Aftësia për një sulm të koordinuar që mund të shkaktojë përçarje masive kundër mbrojtjeve të integruara dhe heterogjene duke përfshirë edhe kryptografinë. Këtu organizata ka aftësi për të krijuar mjete të sofistikuara të piraterisë, të kryej analizë, kontroll dhe komandim dhe ka aftësi të lartë të organizimit.[56]

Për të qenë edhe më i qartë se çka në fakt është terrorizmi kibernetik do të përfshijë edhe disa shembuj që ndodhin në jetën e përditshme.

Qeveritë e njërit shtet mund që të angazhojnë dhe përdorin hakerë për të spiunuar komunikimet e zbulimit të shtetit tjetër për të mësuar se ku ndodhen trupat ose për të fituar një avantazh taktik në luftë, gjë që fut këtë lloj krimi në kategorinë e krimeve më të rrezikshme në historinë e njerëzimit.

Terroristët vendor mund të hyjnë në servera privat të një korporate, me qëllim që të mësojnë sekrete tregtare, apo për të vjedhur informacionin bankar, ose për të marrë të dhënat private të punonjësve të asaj korporate.

Rrjetet globale terroriste mund të rrëzojnë dhe prishin një ueb faqe të madhe me qëllim që të krijojnë një telash apo shqetësim publik, ose përpiqen që të ndalojnë trafikun në një faqe që publikon tekste me të cilën ata nuk pajtohen.

Terroristët ndërkombëtarë mund të përpiqen për të hyrë dhe për të çaktivizuar sinjalin që mund të fluturojë dron dhe sinjalin që mund të kontrollojë teknologjinë e ushtrisë së një shteti.[57]

---

[56] Cyberterrorism – Dorothy E. Denning (Libër i shkruar më 23 Maj 2000) apo shiko https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Qasur më 03/12/2018)

[57] Disa shembuj të cituara nga Akademia Study (akademi elektronike) https://study.com/academy/lesson/what-is-cyber-terrorism-definition-cases-examples.html (Qasur më 03/12/2018)

2.5.2 Sabotazhi kompjuterik

Sabotazhi kompjuterik është tip i kriminalitetit kompjuterik dhe paraqet bartjen, shkatërimin, fshierjen, ndryshimin, dëmtimin, fshehjen ose keqpërdorimin e të dhënave ose programeve kompjuterike, poashtu paraqet shkatërrimin ose dëmtimin e kompjuterave ose paisjeve të tjera që merren me përpunimin elektronik dhe transferimin e të dhënave me qëllim të çaktivizimit ose pengimit të përpunimit dhe dërgimit të të dhënave që kanë vlerë të veçantë për organet shtetërore, shërbimet publike, institucionet, ndërmarjet e ndryshme dhe subjektet tjera.[58]

Dallimi në mes të sabotazhit kompjuterik dhe përdorimit të paautorizuar të kompjuterit ose rrjeteve kompjuterike është tek dëmtimi i arritur pas krimit. Pra nëse informatat apo të dhënat i takojnë organeve shtetërore, shërbimit publik ose ndonjë subjekti tjetër ligjor atëherë flitet për sabotazh kompjuterik, e ndërsa nëse është kryer përdorim i paautorizuar i kompjuterit ku vepra penale konsiderohet të jetë kryer ndaj një objekti privat atëherë flitet për krim më të lehtë pra për përdorim të paautorizuar.

Sabotazhi kompjuterik poashtu ka një lidhje të ngushtë edhe me terrorizmin kibernetik, me përmisimin e teknologjive informative formohet një numër i madh i njerëzve të cilët i përdorin ato me qëllime dhe në mënyra të ndryshme duke arritur edhe në shkallën e terrorizmit. Kur flasim për terrorizmin kibernetik sot teknologjitë informative janë shumë në favor të tyre pasi që ata shumë lehtë mund të vijnë deri tek një informacion që atyre u nevojitet dhe me marrjen e atij informacioni ato realizojnë qëllimet e tyre. Ajo çka e bën edhe më të komplikuar situatën është se terroristët mund të angazhojnë apo punësojnë njerëz me intelegjencë të lartë me qëllim që të kryejnë ndonjë sabotazh kompjuterik apo ndonjë spiunim të nivelit të lartë dhe më pas atë të keqpërdorin për të fituar qëllimet e veta. Si shembull i sabotazhit kompjuterik mund të përmendim organizatën terroriste IRA e cila në vitin 1997 tronditi publikun anglez duke thënë se ato përveç bombave, vrasjeve dhe formave të tjera të krimit që kanë përdorur ato do të fillojnë edhe me sulme elektronike drejt sistemeve kompjuterike të bizneseve angleze dhe qeverisë angleze.

[58] Definicion i cituar nga kodi penal i Sërbisë neni 299 http://paragraf.rs/propisi/krivicni_zakonik.html (Qasur më 03/12/2018)

Me rritjen e rrezikut nga spiunazhat dhe sabotazhet kompjuterike filluan edhe shtetet nga e gjithë bota t'i kushtojnë më shumë vëmendje kësaj dukurie dhe të luftojnë atë. Si shembull Pentagoni në vitin 2011 vendosi që nëse dikush nga shtetet tjera i kryen spiunazh apo sabotazh kompjuterike SHBA-ve ajo do të konsideronte atë si shpallje lufte dhe për këtë do të dërgonte të gjithë ushtrinë amerikane për të zgjidhur çështjen.[59]

[59] Zhurnali elektronik i Wall Street me titull "Cyber Combat: Act of War" i publikuar më 31/05/2011 https://www.wsj.com/articles/SB10001424052702304563104576355623135782718 (Qasur më 03/12/2018)

KAPITULLI I TRETË

PARANDALIMI DHE LUFTIMI I KRIMIT KOMPJUTERIK

3.1 Dimensionet ndërkombëtarë te krimi kompjuterik

Ende nuk ka ose nuk ekziston ndonjë përkufizim i përbashkët për krimin kibernetik. Krimi kibernetik i referohet aktiviteteve ilegale të ndërmjetësuara që shpesh ndodhin në rrjetet elektronike globale.[60] Krimi kibernetik është "krim ndërkombëtar" ose "krim transnacional" pra nuk ekzistojnë kufijtë kibernetik ndërmjet vendeve. Rrjetet ndërkombëtare shpesh e sfidojnë efektivitetin e ligjit vendor dhe ndërkombëtar poashtu e sfidojnë edhe zbatimin e ligjit. Për shkak se ligjet ekzistuese në shumë vende të botës nuk shkruajn për krimin kibernetik, kriminelët gjithnjë e më shumë kryejnë krime në internet pasi që kanë përparësi nga dënimet ligjore dhe kanë përparësi poashtu në zbulimin e tyre, pra shumë rëndë zbulohen.

Pavarësisht se një vend është i zhvilluar ose jo, qeveritë dhe industritë kanë realizuar kërcënime kolosale të krimit kibernetik në sigurinë ekonomike, politike dhe në interesat publike. Megjithatë kompleksiteti në llojet dhe format e krimit kompjuterik rrit vështirësitë për tu luftuar si krim. Pra, lufta kundër krimit kibernetik bën thirje për bashkpunim ndërkombëtar. Shumë organizata dhe qeveri të ndryshme kanë bërë përpjekje të përbashkëta për vendosjen e legjislacionit dhe zbatimin e ligjit si në nivel rajonal, poashtu edhe në atë ndërkombëtar.

Siguria e një vendi si dhe ajo ndërkombëtare janë të kërcënuara nga kriminaliteti kompjuterik shkaku i asaj se si kriminalitet është transnacional dhe nuk ekziston një shtet i vetëm i cili do të ndalonte kriminalitetin kompjuterik në një vend apo rajon global, prandaj duhet dhe është e domosdoshme që shumica e shteteve të bashkëpunojnë mes veti dhe sëbashku të mbrohen nga kriminaliteti kompjuterik në rajon global. Kriminaliteti kompjuterik ka një spektër mjaft të gjërë në rajon global shkaku se kryhet ku do në botë dhe në shumë mënyra. Duke u

[60] "An International Perspective on Fighting Cybercrime" – Pjesë e shënimeve tek Shkencat Kompjuterike Volumi 2665 tek tema "Intelligence and Security Informatics" faqe 379-384

bazuar në statistikat e Dr Michael Mcguire[61] shohim se profiti i kriminalitetit kompjuterik për vitin 2018 do të arrijë një shifër mjaft të frikshme në para, sipas tij dikund tek 1.5 trilion dollarë.

3.2 Konventat dhe bashkëpunimet ndërkombëtare kundër krimit kibernetik

Tradicionalisht krimi dhe dënimi janë kryesisht lokal, rajonal apo ndërkombëtar. Sot shumë sende që ne përballemi janë të lidhura me karakterin transnacional të krimit kibernetik, prandaj është e rëndësishme që instrumentet ligjore të jenë të gatshme për t'i shërbyer përpjekjeve kundër krimit.

Ekzistojnë disa përgjigje internacionale dhe legjislative në lidhje me kriminalitetin kompjuterik dhe ato janë:

G8 – është një grup që përbëhet nga tetë shtete të industrializuara dhe ato janë: Amerika, Britania, Franca, Italia, Japonia, Gjermania dhe Kanada. Në vitin 1997, G8 lëshoi një komunikatë të ministrave që përfshinë një plan veprimi dhe disa parime për të luftuar krimin kibernetik dhe për t'i mbrojtur të dhënat dhe sistemet nga ndërhyrjet dhe dëmtimet e paautorizuara. G8 gjithashtu i urdhëroi që gjithë personelët e zbatimit të ligjit të jenë të trajnuar dhe pajisur për ta trajtuar krimin kibernetik dhe poashtu të gjitha vendet anëtare të kenë nga një pikë kontakti që do të punonte 24 orë në ditë dhe 7 ditë në javë, me qëllim që të ndalojë kriminalitetin ndërkombëtarë.[62]

Kombet e Bashkuara – Në vitin 1990 asambleja e përgjithshme e OKB miratoi një rezolutë që merrej me legjislacionin e krimit kompjuterik. Në vitin 2000, OKB miratoi një rezolutë mbi luftimin e keqpërdorimit kriminal të teknologjisë së informacionit. Në vitin 2002, OKB miratoi rezolutën e dytë mbi luftimin e keqpërdorimit kriminal të teknologjisë së informacionit.[63]

ITU – si një agjencion brenda Kombeve të Bashkuara, luan një rol udhëheqës në standartizimin dhe zhvillimin e çështjeve të telekomunikacionit dhe sigurisë kibernetike. ITU

[61] Profesor në Univerzitetin e Surrey-it, Britani

[62] "An International Perspective on Fighting Cybercrime" – Pjesë e shënimeve tek Shkencat Kompjuterike Volumi 2665 tek tema "Intelligence and Security Informatics" faqe 379-384

[63] "Regional and International Trends in Information Society Issues" – 08 – 12 Mars 2010 nga Dr. Marco Gercke, Drejtorë i institutit të kërkimeve në lëndën e krimit kibernetik fq. 27

poashtu ishte agjenda udhëheqëse e Samitit Botëror mbi Shoqërinë e informacionit. Në vitin 2003 u shpallën deklaratat e Parimeve të Gjenevës dhe Plani i Veprimit të Gjenevës, i cili thekson rëndësinë e masave në luftën kundër kriminalitetit kompjuterik.

Këshilli i Europës – është një organizatë ndërkombëtare që fokusohet në zhvillimin e të drejtave të njeriut dhe demokracisë në 47 shtetet e saj Europiane.

Në vitin 2001, Konventa për krimin kibernetik, ishte konventa e parë ndërkombëtare që synonte tek dënimet penale në internet, kjo Konventë u hartua nga Këshilli i Europës, SHBA, Kanada dhe Japonia dhe u nënshkrua nga shtetet anëtare të këtij këshilli. Por vetëm 25 vende u ratifikua më vonë. Kjo konventë synon sigurimin bazorë të një kuadri ligjorë efektiv për luftimin e krimit kibernetik përmes harmonizimit të kualifikimit të veprave penale në fushën e krimit kibernetik, sigurimin e ligjeve që fuqizojnë zbatimin e ligjit dhe mundësimin e bashkpunimit ndërkombëtarë.

Në vitin 2005, Kina nënshkruajti një pakt për Planin e Veprimit në Londër në lidhje me spam-in dhe kjo ishte një përpjekje ndërkombëtare për të frenuar problemin e krimit kompjuterik.

Poashtu në vitin 2006 u mbajt Samiti ndërkombëtarë i quajtur “Deklarata e Pekingut” në lidhje me anti spam-in.

Grupi punues i APEC-ut në lidhje me telekomunikacionin u pajtua me një plan veprimi për vitet 2010-2015, i cili përfshinte nxitjen e një mjedisi të sigurtë dhe të besueshëm të TIK-ut.

Në Janar të vitit 2011, Shtetet e Bashkuara të Amerikës dhe Kina për herë të parë në krye të nivelit shtetërorë u pajtuan që të punojnë sëbashku në baza dypalëshe në lidhje me çështjet e sigurisë kibernetike.

3.3 Lufta kundër rrezikut kibernetik dhe parandalimi i tij në faza të hershme

Siç dimë si çdo vit me radhë edhe sot krimi kibernetik është një kërcënim i vazhdueshëm. Shumica e personave nëpër botë kur dëgjojnë për krimin kibernetik, mendimet e tyre shkojnë direkt te hakerët e ndryshëm të cilët mund t’ua vjedhin të gjitha të dhënat personale poashtu edhe ato financiare. Mirëpo nuk është edhe aq e thjeshtë pasi që krimi kibernetik dita-ditës po

zhvillohet dhe po forcohet në të gjitha aspektet me kërcënime të reja që shfaqen çdo vit me rradhë. Shumë persona kur dëgjojnë se analistët në çfar rangu vëndojnë kriminalitetin kompjuterik në krahasim me kriminalitetet tjera duan që të mos e përdorin asnjëherë më internetin, gjë që nuk do të ishte në rregull, por në vend të kësaj si ide e mirë do të ishte që njerëzit nëpër botë që merren me internetin të njoftohen me kriminalitetin kompjuterik, të dinë cilët hapa do ishin të parë që do të ndërmerreshin në shpëtimin dhe mbrojtjen e të dhënave personale.

Marrja e disa masave në kohë, qoftë edhe nëse ka ndodhur kriminaliteti kompjuterik personat duhet të dijnë se kujt t'i drejtohen, pra të jenë të njoftuar me këto hapa që duhet të ndërmerren. Normal, çdokush do që të gjejë metodën apo mënyrën për ta ndalur këtë lloj kriminaliteti apo kësisoj lloj ndërhyrjesh nëpër kompjuterët e tyre personal, mirëpo e keqja e kësaj qëndron pas asaj se ky lloj kriminaliteti nuk mund të ndalet, sepse dita pas ditës zhvillohen dhe formohen programe dhe mënyra të reja nga hakerët për të ardhur deri te ndërhyrjet dhe marrja e të dhënave, e deri sa kompjuterët tanë personal janë të kyçur me internetin atëherë gjithmonë do të ekzistojë një rrezik për të na ndodhur ndonjë ndërhyrje.

Megjithatë, edhe pse nuk mund ta ndalojmë një ndërhyrje në kompjuterin tonë ne mundemi që të marrim masat paraprake që të mos vijë deri te një ndërhyrje nga jashtë. Sipas kompanisë Norton Security që është një kompani mjaft serioze me një traditë 25 vjeçare dhe mbi 1700 të punësuar ekzistojnë disa këshilla që të ruajmë veten nga kërcënimet dhe krimet kibernetike dhe kryejnë parandalimin e tij e ato janë:

- Të kemi të instaluar një antivirus të mirë dhe të licencuar dhe atë të përditësojmë
- Gjatë krijimit të fjalëkalimeve nëpër llogaritë tona qoftë email apo rrjetet sociale duhet që të krijojmë fjalëkalime sa më të komplikuara, duke përdorur shkronja, numra dhe simbole
- Duhet të shohim nëse kemi softuerin kompjuterik të përditësuar
- Duhet të menaxhojmë cilësitë e rrjeteve sociale, të shohim se cilat persona i kemi miq, a i njohim shoqërinë tonë në rrjetet sociale, çfarë raportesh ne kemi me to dhe çfarë të dhënash ne shkëmbejmë gjatë bisedimeve, pasi që nëse ne nuk i mbyllim të dhënat tona që të mund të shohim vetëm ne dhe shokët që kemi ne ato të dhëna mund t'i shohë çdokush dhe me ndihmën e tyre mund që të na resetojnë fjalëkalimin tonë që me automatizëm do të thotë se kemi ndërhyrje ilegale në llogarinë tonë

- Fshehja e ip së rrjetit të shtëpisë do të ishte poashtu ideja e mirë pasi që nëse personat që kryejnë krime kibernetike fitojnë ip e internetit tonë që kemi në shtëpi ato mund të na sjellin probleme nga ma të ndryshmet, e për këtë parashihet që të merren të ashtuquajturit VPN (virtual private network) që në shqip do të thotë rrjeti privat virtual, me anë të së cilës do të mshefej ip e ruterit të shtëpisë, e kjo do të bënte mjaft rëndë që hakerët të vijnë deri te të dhënat tona personale
- Në qoftë se jemi prindër duhet që të flasim me fëmijët tanë se çka nuk duhet të kryejnë dhe çka munden të kryejnë pa mos u bë restrikcione apo ndalesa nga më të ndryshmet, përkundrazi çdo problem që do të kishin fëmijët tanë duhet që të na tregonin dhe bashkë t'i ndërmarrim masat që duhet të ndërmerren
- Nëse ne kemi një biznes apo jemi antar në ndonjë faqe elektronike e cila ka qenë e atakuar apo hackuar duhet që sa më shpejt të ndërrojmë fjalëkalimin tonë tek ajo faqe dhe të shohim në qoftë se nuk është e domosdoshme të jemi antar të asaj faqe duhet që edhe të tërhiqemi.[64]

Zakonisht parandalimi i kriminalitetit duhet të bëhet në mënyrë të drejtpërdrejt, pra nga vetë ne apo nga kontrolla e prindërve duke përdorur këshilla të vogla teknike, mundemi që tu shmangemi shumë sulmeve të ndryshme. Në përgjithësi të gjithë kriminelët e botës së internetit tentojnë që të vijnë deri tek paratë sa më shpejt dhe sa më lehtë të jetë e mundur. Sa më vështirë që ne të bëjmë punën e tyre, aq më shumë kemi shansa që të na kalojnë pa mos na dëmtuar dhe të vazhdojnë punën e tyre te personat ku rrugët e tyre janë shumë më të lehta për të vepruar.

[64] Citate nga kompania Norton Security në lidhje me luftën kundër kriminalitetit kompjuterik në faza të hershme https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html (Qasur më 03/12/2018)

KAPITULLI I KATËRT

KRIMI KOMPJUTERIK NË REPUBLIKËN E MAQEDONISË

4.1 Veçoritë sociale dhe individuale të personave që merren me kriminalitetin kompjuterik në botë dhe në Maqedoni

Siç dimë personat të cilët merren me kriminalitet kompjuterik apo të ashtuquajturit hakera janë persona mjaft intelegjent dhe kanë koeficent të intelegjentës mjaft të lartë dhe poashtu konsumojnë kuriozitetin. Shumica e hakerëve janë neofilë, pra stimulohen nga vlerat dhe risitë intelektuale të reja që ofrohen dita- ditës nëpër botë. Në shumicën e rasteve janë persona individualë, nuk e kanë shumë dëshirë punën në grupe edhe pse ekzistojnë shumë grupe. Profesioni të cilën kryejnë hakerët është mjaft i rëndë se në shumicën e kohës duhet qëndruar ulur dhe koncentruar, edhe pse duhet qëndruar ulur gjatë gjithë kohës shumica e hakerëve janë të dobët në peshë, e ato që janë në peshë të lartë thuhet se ata kanë kaluar në fazën e ekstremizmit. Kanë aftësi të mëdha për të absorbuar, shumë informacione dhe njohuri për një kohë të shkurtër dhe në sy u bien detaje të njerëzve që askujt tjetër nuk do t'i interesonin dhe më vonë ato detaje i përpunojnë dhe arrijnë në përfundime.

Një person me intelegjencë mesatare mund të jetë një haker i shkëlqyeshëm, ndërsa një person gjeni që është kreativ dhe nuk ka një linjë në të cilën ai do të kufizohej, apo ai nuk do të provonte që të arrijë në atë pikë, asnjëherë nuk do të arrijë atë nivel. Hakerët mendojnë se hackingu është formë e përdorimit të njohurive për të arritur te njohuri të reja dhe shumë më të mëdhaja nga këto që kanë. Për nga stereotipet, hakerët njihen si persona që nuk kanë vetëm një anë të botës por ato përpiqen që të kyçen në çdo temë të ndryshme që bisedohet në publik. Sa haker më i mirë të jetë aq në më shumë tema mund që të kyçet dhe të bisedojë pa patur ndonjë problem të vogël. Zakonisht frikësohen nga kontrollat policore dhe kontaktet me persona autoritativ. Edhe pse janë mjaft perfekt në aspektin intelektual, në jetët reale të tyre dinë që të jenë një kaos i vërtetë, pra kodi i programit do të jetë mjaft mirë i shkruar mirpo në jetën reale do të ketë mbeturina nga gjithë anët e tavolinës ku qëndron kompjuteri. Shumicën e hakerëve nëpër botë nuk e tërheqin paratë sa që e tërheqin sfidat dhe mjetet e reja.

4.2 Numri i të dënuarve dhe llojet e kriminalitetit kompjuterik që dënohen me ligj në Republikën e Maqedonisë nga viti 1996 e deri më sot

Si çdo lloj kriminaliteti edhe kriminaliteti kompjuterik është krim i cili dënohet në Republikën e Maqedonisë. Edhe pse nuk ka shumë raste të zbuluara nga kriminaliteti kompjuterik Republika e Maqedonisë ka mjaft mirë të rregulluar me ligj kriminalitetin kompjuterik. Për ndalimin e kriminalitetit kompjuterik në vend është përfshirë ky kuadër ligjor:

4.2.1 Veprat penale të kriminalitetit kompjuterik të parapara në Kodin Penal nga viti 1996

Me miratimin e kodit penal në vitin 1996 në Republikën e Maqedonisë janë paraparë për së pari herë edhe inkriminimet klasike për kriminalitetin kompjuterik, por edhe pse shumë pak shkruhet për llojin e tillë të kriminalitetit në këtë kohë, aty ka të paraqitura dispozita për mundësinë e ekzekutimit me kompjuter, nëse është sulmuar një kompjuter ose një sistem rrjetor. Në këtë kohë te Kodi Penal i Republikës së Maqedonisë, sistematikisht janë të përshkruara elementet e inkriminimeve të kriminalitetit kompjuterik të ndara në tre grupe kryesore, e ato janë[65]:

- **Veprat penale kundër lirive dhe të drejtave të individit dhe qytetarit –** ku bëjnë pjesë:

1. Shkelja e privatësisë apo sekretit të letrave apo dërgesave tjera – Neni 147
2. Keqpërdorimi i të dhënave personale – Neni 149
3. Dëgjimi i paautorizuar telefonik dhe regjistrimi i audios – Neni 151
4. Shkelja e të drejtave autoriale dhe të drejtave tjera të lidhura me të – Neni 157

- **Veprat penale kundër lirisë dhe moralit seksual**

1. Shfaqja e materialeve pornografike të fëmijëve – Neni 193

- **Veprat penale kundër pronës**

1. Ndërhyrja në një sistem kompjuterik – Neni 251

[65] "Gazeta zyrtare e Republikës së Maqedonisë", numër 37/96

Poashtu duhet cekur se në vitin 1999 me ndryshimet dhe shtimet e ndryshme që u bënë në Kodin Penal të Republikës së Maqedonisë, sa i përket kriminalitetit kompjuterik nuk kemi ndryshime.[66]

4.2.2 Veprat penale të kriminalitetit kompjuterik të parapara në Kodin Penal nga viti 2004

Ndryshimet dhe plotësimet në Kodin Penal të Republikës së Maqedonisë nga viti 2004 janë të rëndësishme dhe kanë bërë të ndryshojë përmbajtjen duke plotësuar inkriminimet dhe duke krijuar inkriminime të reja në:[67]

- **Kapitullin e XV – Veprat penale kundër lirive dhe të drejtave të njeriut dhe qytetarit**

1. Rreziku ndaj sigurisë – neni 144 paragrafi 4
2. Shkelja e konfidencialitetit të letrave ose dërgesave tjera – neni 147
3. Keqpërdorimi i të dhënave personale – neni 149
4. Ndalimi i qasjes së një sistemi informativ publik – neni 149 – a
5. Regjistrimi i paautorizuar i përgjimeve dhe regjistrimi i zërit – neni 151
6. Inçizimi i paautorizuar – neni 152
7. Shkelja e të drejtave autoriale dhe të drejtave lidhur me ato – neni 157

- **Kapitullin e XVIII – Veprat penale kundër nderit dhe reputacionit**

1. Shpifja – neni 172
2. Fyerja – neni 173
3. Prezentimi i rasteve personale dhe familjare – neni 174
4. Hudhja e mashtrimit për një krim të caktuar – neni 175
5. Mosndëshkimi i veprave penale nga neni 172 deri 175 dhe
6. Parashtrimi i vërejtjes gjyqësore ose lirimi nga dënimi për krimet e referuara nga neni 172 deri nenin 175.

- **Kapitullin e XIX – Veprat penale kundër lirisë seksuale dhe moralit seksual**

1. Shfaqja e materialeve pornografike të fëmijëve – neni 193

- **Kapitullin e XXIII – Veprat penale kundër pronës**

1. Dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik – neni 251

[66] "Metodologjia e hulumtimit të krimit kompjuterik" nga Svetlana Nikoloska – Univerziteti St. Kliment Ohridski departamenti i sigurimit dhe kontrollës financiare, Dhjetorë 2013
[67] "Gazeta zyrtare e Republikës së Maqedonisë",numër 19/04

2. Krijimi dhe importimi i viruseve kompjuterike – neni 251 – a
3. Mashtrimet kompjuterike – neni 251 – b

- **Kapitullin e XXV – Veprat penale kundër financave publike, qarkullimeve pagesore dhe ekonomike**

1. Përdorimi i paautorizuar i shpikjes apo softuerit të huaj – neni 286

- **Kapitulli XXXII – Veprat penale kundër trafikut ligjor**

1. Falsifikatat kompjuterike – neni 379 – a

Ndryshimet dhe plotësimet e Kodit Penal të vitit 2004 prezantuan përgjegjësinë për personat juridik, edhe pse krimet kryheshin nga personat fizikë por në emër dhe llogari të personave juridik.[68]

4.2.3 Veprat penale të kriminalitetit kompjuterik të parapara në Kodin Penal nga viti 2008

Ligji i Kodit Penal të Republikës së Maqedonisë zbaton rekomandimet e Konventës për kriminalitetin kompjuterik ashtu që së pari i definon emërimet të cilat përdoren për inkriminimet e veprave penale të reja dhe plotësimin e veprave penale të cilat ekzistojnë.[69]

Këtë vit te gazeta zyrtare të emëruara janë edhe termet "Viktimë", "Pornografia me fëmijë", "Sistemi kompjuterik" dhe "Të dhënat kompjuterike".[70]

- Me termin viktimë sipas gazetës zyrtare nënkuptojmë gjithësecilin person, i cili ka pësuar dëm, duke përfshirë dëmtimin fizik dhe psiqik, pësimin emotiv, humbjen materiale apo lëndim tjetër që rrezikon lirinë dhe të drejtat themelore të tij si pasojë e një krimi të kryer.
- Me fëmijë si viktimë e veprës penale nënkuptohet personi i mitur deri në moshën tetëmbëdhjetë vjeç/e. Me pornografi fëmijërore nënkuptohet materiali pornografik i cili në mënyrë vizuele shfaq veprime të dukshme seksuale me personin e mitur, me personin i cili duket si i tillë, ose fotografi reale të cilat shfaqin veprime të dukshme seksuale me të.

[68] "Metodologjia e hulumtimit të krimit kompjuterik" nga Svetlana Nikoloska – Univerziteti St. Kliment Ohridski departamenti i sigurimit dhe kontrollës financiare, Dhjetorë 2013 fq. 72
[69] "Metodologjia e hulumtimit të krimit kompjuterik" nga Svetlana Nikoloska – Univerziteti St. Kliment Ohridski departamenti i sigurimit dhe kontrollës financiare, Dhjetorë 2013 fq 73
[70] "Neni 122 paragrafi 21,22 dhe 23", nga gazeta zyrtare e Republikës së Maqedonisë 07/2008

- Me sistem kompjuterik nënkuptohet çdo instalim apo grup i instalimeve të lidhura ndërmjet tyre prej të cilave njëri apo më shumë prej tyre bëjnë përpunim automatik të të dhënave sipas një programi të caktuar.
- Me të dhëna kompjuterike nënkuptohet prezantimi i fakteve, informatave ose koncepteve në formë të përshtatshme për t'u përpunuar përmes sistemit kompjuterik, duke e përfshirë edhe programin e përshtatshëm që sistemin kompjuterik ta vë në funksion.

Në këtë vit janë kryer edhe disa ndryshime te Kapitulli XV – Krimet kundër lirisë dhe të drejtave të individit dhe qytetarit, në nenin 157 "Shkelja e të drejtës autoriale dhe të drejtat e përafërta" dhe u futën tre inkriminime të reja si: "Cenimi i të drejtës së distributorit të sinjalit satelitor të mbrojtur teknikisht në mënyrë të veçantë" - 157-a, "Pirateria ndaj veprës audiovizuele" - 157-b dhe "Pirateria ndaj fonogramit" - 157-v.

4.2.4 Veprat penale të kriminalitetit kompjuterik të parapara në Kodin Penal nga viti 2009 e deri më sot

Kodi penal, Kodi i procedurës penale, Ligji i komunikimeve elektronike, Ligji për ndjekjen e komunikimeve, Ligji i tregtisë elektronike, Ligji i qeverisjes elektronike, Ligji i finansimit të parave, Ligji i të dhënave elektronike dhe nënshkrimi elektronik dhe Deklarata për një internet më të sigurt dhe si vepra penale që janë të parapara tek kriminaliteti kompjuterik në Republikën e Maqedonisë në Kodin Penal janë këta nene:

Neni 144 artikulli 4 – Rrezikimi i shoqërisë

Neni 147 artikulli 1 dhe 2 – Shkelja dhe zbulimi i letrave apo postave elektronike dhe sendeve tjera

Neni 149 artikulli 2 – Abuzimi i të dhënave personale

Neni 149 a – Parandalimi i qasjes në sistem informimi publik

Neni 157 artikulli 1 dhe 2 – Shkelja e të drejtave autoriale dhe të drejtave lidhur me të

Neni 157 a – Shkelja e të drejtës distributoriale për një sinjal teknik satelitor me mbrojtje të posaçme

Neni 157 b – Pirateria e punës audiovizuele

Neni 157 v – Pirateria e fonogramit

Neni 193 – Shfaqja e materialeve pornografike të një fëmije

Neni 193 a – Prodhimi dhe shpërndarja e pornografive me fëmijë

Neni 193 b – Mashtrimi me mardhënie seksuale me person të gjinisë së kundërt që nuk ka kaluar 14 vjet

Neni 251 – Dëmtimi ose hyrja e paautorizuar në një sistem kompjuterik

Neni 251 a – Krijimi dhe shpërndarja e viruseve kompjuterike

Neni 251 b – Mashtrimet kompjuterike

Neni 271 – Krijimi, blerja ose huazimi i mjeteve për falsifikim

Neni 274 b – Prodhimi dhe përdorimi i kredit kartelave të rrejshme ose falsifikuara.

Siç shohim për kriminalitetin kompjuterik ekzistojnë dikund tek 16 nene nga Kodi Penal i Republikës së Maqedonisë dhe kuadri ligjor i saj që rregullojnë veprat penale në vend për këtë lloje kriminaliteti. Duke u bazuar në këto ligje nga instituti apo enti shtetëror i statistikës në Republikën e Maqedonisë në vitin 2017 kemi këto statistika:

Duke u bazuar në Kodin Penal të Republikës së Maqedonisë, neni 251 vepra penale dëmtim dhe hyrje e paautorizuar në sistemin kompjuterik, gjithsej janë 124 persona që kanë kryer këtë vepër penale nga i cili numër 69 personave u është lëshuar dënimi, 6 personave u është refuzuar dënimi dhe 49 persona që kanë kryer veprën penale në fjalë nuk janë identifikuar. Personi i parë që është dënuar në Republikën e Maqedonisë është në vitin 1997[71].

Sipas nenit 251 b vepra penale mashtrimet kompjuterike, janë identifikuar dhe dënuar 3 persona.

[71] Golemoto çekmexhe, Lufta kundër kriminalitetit kompjuterik – Intervistë nga Renata Mateska me Marian Risteski (Inspektor i kriminalitetit kompjuterik) fq.1 Makedonsko Sonce numër 501 botuar më 06.02.2004

Sipas nenit 271 vepra penale krijimi, blerja ose huazimi i mjeteve për falsifikim, janë identifikuar dhe dënuar 3 persona. Nga e gjithë kjo shohim se gjithsej vetëm 3 lloje të veprave penale për kriminalitet kompjuterik janë zbuluar edhe atë nga gjithsej 130 persona të dënuar, 75 janë identifikuar dhe 55 nuk janë gjetur, pra i bie 57,69 % e rasteve është identifikuar nga ky numër i vogël i veprave penale të kriminalitetit kompjuterik të zbuluara.

4.3 Numri i viktimave dhe fitimet nga kriminalitetit kompjuterik në Republikën e Maqedonisë dhe në botë

Nëpër tërë botën nga paraqitja e të gjitha llojeve të krimeve që kryhen, 35% e tyre janë krime kompjuterike dhe afër 80% e krimeve kompjuterike që kryhen as që paraqiten, pra ngelen si një numër i errët.[72] Ky numër na bën që të mendojmë se sikur të ishin paraqitur edhe këto 80% e krimeve kompjuterike që kryhen nëpër botë do të thotë se afër gjysma e krimeve që kryhet është krim kompjuterik. Duke u bazuar në numrat e viktimave që dita - ditës shtohen nga ky lloj kriminaliteti shihet shumë qartë se mungojnë shumë ekspertë të kësaj lënde si në Maqedoni poashtu edhe në tërë botën.

Siç përshkruajta më lart nga statistikat e organit kompetent për kriminalitetin kompjuterik vërejtëm se shumë pak persona janë të dënuar nga ky lloj kriminaliteti, numri i viktimave nuk dihet shkaku i asaj se është një kriminalitet i ri për Republikën e Maqedonisë, pra edhe nëse ka tek enti shtetëror i statistikave nuk ishte i shkruar, jo që viktima nuk ka. Po ashtu nga statistikat e entit shtetëror shihet qartë se afër 50% e rasteve ende nuk është zbuluar, kjo na tregon qartë se numri i errët është gati se gjysma e krimeve kompjuterike që kryhen në vend nga rastet që janë të zbuluara, e mos të flasim për rastet që edhe nuk janë të paraqitura, pra shohim se kriminaliteti kompjuterik në vend ka një territor mjaft të volitshëm shkaku i mungesës së ekspertëve të kësaj lëmije dhe shkaku i mosdijenis së shumicës së popullit rreth kësaj teme në vend. Ndërsa në botë nga statistikat e analizuara në vitin 2017 shihet qartë se Kina është shteti me më shumë viktima në

[72] Statistika të bazuara nga artikulli i advokatit maqedonas Jordan Apostolski i publikuar më 06.08.2015 shiko https://www.akademik.mk/kompjuterski-kriminal-domashna-pravna-ramka-i-megunarodni-dogovori-advokat-jordan-apostolski/ (Qasur më 05/12/2018)

botë dhe me një humbje prej 66 miljon dollarë nga kriminaliteti kompjuterik duke pasuar Brazilin si vendi i dytë me humbje prej 22,5 milion dollarë dhe Shtetet e Bashkuara në vendin e tretë me 19,4 milion dollarë, e më pas radhiten India, Mexico, Franca, Britania e madhe, Italia, Suedia, Gjermania e kështu me radhë të cilat vende kanë humbje deri në 7 milion dollarë për një vit.[73]

Në vitin 2018 kriminaliteti kompjuterik pritet që të sjellë profite prej 1.5 trilion dollarë kriminelëve, duke ndarë në marketet ilegal që janë online kanë profituar diku te 860 miliard dollarë, shkëmbimet sekrete dhe vjedhjet e ip kanë profituar dikund tek 500 miliard dollarë, shkëmbimet e informatave dikund tek 160 miliard dollarë, krimet dhe luftat kibernetike 1.6 miliard dollarë dhe Ransomware dikund tek 1 miliard dollarë.[74] Nga këto informata shohim se kriminaliteti kompjuterik jo që është i rrezikshëm por ai është transferuar në një biznes mjaft të rëndësishëm që udhëhiqet nga kriminelë mjaft të rrezikshëm. Ndërsa, në Maqedoni nuk dihen profitet nga ky lloj kriminaliteti shkaku i asaj se shumë pak raste janë të paraqitura dhe shumë pak raste të zbuluara, mirpo edhe pse shumë pak raste kemi të zbuluara profitet nga ky kriminalitet në Republikën e Maqedonisë janë të shumta dhe besoj se këto të dhëna do të shfaqen në vitet në vijim shkaku i saj se Republika e Maqedonisë është një ndër shtetet më pak të përgatiitura për këtë lloj kriminaliteti.

[73] Statistika nga portali global mjaft i njohur https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/ (Qasur më 18/12/2018)
[74] Informatë nga The SSL Store kompani për lajme të enkriptimit, lajme të industrisë dhe lajme për sigurinë kibernetike shiko https://www.thesslstore.com/blog/2018-cybercrime-statistics/

PËRFUNDIMET DHE REKOMANDIMET

Megjithëse jo të gjithë njerëzit janë viktima të krimit kompjuterik, ata sot të gjithë janë në rrezik, shkaku i saj se krimi kibernetik nuk ka të ndalur është një krim që kryhet në çdo kohë, në çdo vend dhe nga çdokush. Si lloj krimi mund të kryhet nga persona prej 12 vjet e deri gati se në 67 vjet dhe poashtu mund të jetë edhe transnacional pra kryesi dhe viktima mund që të mos njihen dhe shihen shkaku i asaj se kryesi mund të jetë dhe veproi nga një kontinent krejtësisht tjetër nga ai i viktimës dhe duhet cekur se mund të kryhet në çdo moment pra nuk ka një kohë të caktuar pra dhe kjo gjë bën këtë lloj kriminaliteti që të jetë një ndër më të komplikuarit nga kjo shohim se si lloj kriminaliteti është një ndër kriminalitetet më me rëndësi në shekullin 21. Kriminaliteti kompjuterik dita e ditës ndryshon shumë dhe poashtu shumë profesionalizohet duke u shfaqur dhe formuar në shumë më shumë vende dhe në shumë më shumë lloje se sa nga dita e parë që ekziston si kriminalitet. Si mjet për tu kryer ky lloj kriminaliteti një personit i duhet internet dhe sëpaku një paisje për të qasur internetin. Me rritjen e teknologjisë shofim se në ditët e sodit shumë pak vidhen bankat me metodat e vjetra pra me shkuarje në vendngjarje, me sulme fizike, me të shtëna me arrmë etj, pra ku duhet rrezikuar jeta e vetë kriminelit, ndryshe nga mëparë sot pa mos shkuar në vendngjarje dhe pa përdorimin e një arme por duke marrë pranë vetës së tyre një paisje nga ku do të kishin qasje në internet do të mund të kryenin një vjedhje shumë më të rëndë se sa që ndonjëherë është kryer.

Është e dukshme se krimi kompjuterik paraqet kërcënim mjaft serioz për të gjitha operacionet elektronike të të gjitha korporatave dhe organizatave moderne, por në anën tjetër krimi kompjuterik poashtu paraqitet edhe si një sfidë e re e për organizatat dhe firmat të cilat merren me sigurinë e korporatave tjera. Edhe organizatat më të mëdhaja në botë kanë pësuar kompromise të mëdha të sigurisë kibernetike, prandaj për parandalimin e këtyre ndërhyrjeve parashihet që sa më shumë punëtorë të kualifikuar të ndihmojnë vendet tona dhe fuqishëm të reagohet ndaj problemeve të përditshme nga kjo lëmi. Besoj se të gjithë organizatat duhet të

kuptojnë kërcënimet dhe rrezikun e krimit kompjuterik me të cilin mund të ballafaqohen çdo ditë në jetën e përditshme dhe se duhet çdo organizatë sëpaku të ketë një person të kualifikuar dhe të përshtatshëm që të provojë të zvoglojë numrin e krimeve që mund të kryhen në atë organizatë po qoftë edhe të eliminojë në total krimin kompjuterik në atë vend dhe ai person duhet që rregullisht të ndjekë seminare dhe kurse të reja të mbajtura nëpër gjithë botën shkaku se ky lloj kriminaliteti pëhapet shumë dhe në forma të reja çdo ditë.

Edhe pse dimë se sot është e pamundur që një person apo qoftë edhe një shtet të jetoj dhe funksionojë pa përdorimin e kompjuterit dhe internetit shkaku i modernizimit nëpër tërë botën, gjë që na bën të qartë se përse edhe këto mjete që përdoren në jetën e përditshme po përdoren edhe për qëllime ilegale, kryesisht për përfitime të një personi, hakmarrje të ndryshme, luftra të ndryshme në mes firmave dhe shteteve, e shumë e shumë sende të tjera që janë në dëm të të gjithë personave që përdorin internetin në përditshmëri. Meqenëse realiteti ynë në vitet e fundit ka shënuar shumë raste të kriminalitetit kompjuterik dhe të abuzimeve kompjuterike nëpër gjithë botën erdhi deri tek ajo që çdo shtet duhet të rregulloj ligjin për këtë kriminalitet, por edhe të formojë një sistem sanksionesh ligjore e jo vetëm masa parandaluese shkaku i shkallës së rrezikshmërisë së këtij lloji kriminaliteti, por edhe gjitha shtetet bashkë të kenë konventa dhe ligje të përbashkëta të cilat do t'i respektonin në mbarë botën.

Duke parë shkallën e rrezikshmërisë së kriminalitetit kompjuterik edhe shteti ynë, Republika e Maqedonisë u bashkangjit me shumicën e shteteve tjera europiane që në sistemin e tyre të drejtësisë parashohin forma dhe lloje të ndryshme të krimit kompjuterik të cilat i dënojnë me sanksione të ashpra penale, qoftë me para apo edhe me burg. Edhe pse Maqedonia ka këtë sistem ligjor nga statistikat e para për vitin 2017 dhe më parë shohim se dikund 50% e rasteve është zbardhur nga ky numër i vogël i veprave penale të zbuluara, edhe pse ekzistojnë më shumë ligje dikund vetëm 3 lloje të veprave penale janë zbuluar dhe shifet qartë se dita-ditës në Republikën e Maqedonisë kryhet kriminalitet kompjuterik çdo ditë dhe si territor është mjaft i volitshëm për personat që merren me kriminalitet kompjuterik shkaku i asaj se mungon një numër i madh ekspertësh në këtë lëmi.

Pra, mendimi im do të ishte që personat e caktuar për parandalimin dhe ndalimin e kriminalitetit në vend duhet që të jenë persona të cilët kanë njohuri për teknologjinë informative

dhe persona të cilët do të zbulojnë forma të ndryshme të kriminalitetit në vend, të njejtët persona të trajnohen çdo ditë me përditësime të reja shkaku i asaj se hakerat janë gjithmonë një hap para, pasi që merren me zbulime të reja çdo ditë dhe së fundmi personat që zbulohen të marrin dënimin e dënuar shkaku i asaj se nëse nuk dënohen si që është e paraparë ky lloj kriminaliteti do të jetë i pëlqyer edhe nga personat tjerë dhe gjeneratat e reja dhe do të rritet numri në një shkallë mjaft të lartë. Duke marrë parasyshë karakteristikat e krimit kibernetik shohim se ky lloj kriminaliteti dallon qartë nga krimet tjera pasi si armë të këtij kriminaliteti krimineli ka paisjen me të cilën mund t'i qaset internetit dhe mund të shfaqë rrezik në çdo kënd të botës, pra shkalla e rrezikshmërisë nga ky lloj kriminaliteti është mjaft i lartë.

BIBLIOGRAFIA

LIBRA DHE PUBLIKIME TË SHFRYTËZUARA DHE TË CITUARA

1. An evaluation Framework for National Security Strategies nga agjencioni për siguri në Europë ENISA, 2014
2. An introduction into the world of Botnets, Tyler Hudak 2015
3. Computer Crime ‘’A growing and serious problem’’ volumi 6 nga autori Bequai 1977
4. Fjalori i Oxford J.A. Simpson, 1982
5. Global Cybercrime nga Aaron Shull, 2014 Canada
6. Kiberterrorizmi nga Doroty E. Denning, 2000
7. Kriminalistika nga Dr. Skender Begeja, Tiranë 2007
8. Kriminaliteti kompjuterik nga Mirjana Drakulic, Beograd viti 2009
9. Kriminaliteti kompjuterik, Dr. Sc. Veton Vula, Prishtinë 2010
10. Lufta kundër kriminalitetit kompjuterik “Големото Чекмеџе” nga Makedonsko Sonce 501/06.02.2004
11. Metodika e kërkimit të kriminalitetit kompjuterik nga Svetlana Nikoloska, Dhjetorë 2013
12. Perspektiva internacionale e luftimit të krimit kibernetik, Volumi 2665 nga profesorët e univerzitetit të Tucson në SHBA Richard Miranda, Daniel D. Zeng, Chris Demchak, Jenny Schroeder, Hsinchun Chen, 2003
13. Regional and International Trends in Information Society Issues, Dr. Marco Gercke, Mars 2010

14. Siguria Informative: Sulmet kompjuterike në departamentin e mbrojtjes shkaktojnë rritje të rrezikut Department of Defense Pose Increasing Risks – GAO fq.3 (Information security: Computer Attacks at Department of Defense Pose Increasing Risks – GAO fq.3), AIMD 1996
15. Sigurimi i sistemit kompjuterik - skriptë nga Jugoslav Ackoski, Shkup 2012
16. Strategjia e sigurisë kibernetike të Unionit Europian, Bruksell 2013
17. Studimi i institutit The Ponemon ''Cyber security on the offense'', 2012

BURIME JURIDIKE, PLANE STRATEGJI DHE RAPORTE

1. Amandamenti nga Akademia elektronike Study, nga Pr. Erin Krcatovich profesor i politikave shkencore, 2018
2. Botnet nga Internet Society, 30/10/2015
3. Doracaku BOTNET nga agjencia e sigurisë në internet ENISA, 2011
4. Doracaku i kriminalitetit kompjuterik nga William S. Sessions
5. Doracaku për krimin kompjuterik në Republikën e Maqedonisë nga OSCE, Shkup 2014
6. Gazeta Zyrtare – Sluzben Vesnik, 2010
7. Kodi penal i Republikës së Maqedonisë me përmisime, 2005
8. Kodi Penal i Republikës së Sërbisë me përmisime, 2016
9. Kushtetuta e Republikës së Maqedonisë, Shkup 1991
10. Manual për kriminalitetin kompjuterik nga OSCE, Januar 2014
11. Raporti nga Cyberwarfare – CRS Report for Congress, 2001
12. Shtojca e krimit shkollorë të Amerikës, Dhjetor 2016
13. Zhurnal elektronik i Wall street Cyber Combat: Act of War, 2011

14.Zhurnal elektronik nga Michael K. Bergman The Deep Web, Volumi 7, 2001

Burimet nga Interneti

1. http://actionfraud.police.uk
2. http://azop.hr;
3. http://coe.int/en
4. http://courses.cs.washington.edu;
5. http://en.oxforddictionaries.com;
6. http://hackforums.net;
7. http://ilt.eff.org;
8. http://iwf.org.uk
9. http://nces.ed.gov;
10. http://nw3c.org/
11. http://oun.org
12. http://paragraf.rs;
13. http://quod.lib.umich.edu;
14. http://security.foi.hr;
15. http://security.radware.com;
16. http://study.com;
17. http://us.norton.com
18. http://usa.kaspersky.com;
19. http://web.archive.org;
20. http://www.acorn.gov.au;
21. http://www.akademik.mk/

22.http://www.brightplanet.com;

23.http://www.cia.gov;

24.http://www.enisa.europa.eu;

25.http://www.fbi.gov;

26.http://www.floridatechonline.com;

27.http://www.guru99.com;

28.http://www.ibls.com;

29.http://www.inhope.org;

30.http://www.internetsociety.org;

31.http://www.internetworldstats.com;

32.http://www.interpol.int

33.http://www.it-klinika.rs;

34.http://www.linkedin.com;

35.http://www.meritalk.com;

36.http://www.microsoft.com;

37.http://www.nato.int;

38.http://www.phishing.org;

39.http://www.scamwatch.gov.au;

40.http://www.statista.com/

41.http://www.tripwire.com;

42.http://www.thesslstore.com/

43.http://www.upcounsel.com/internet-law

44.http://www.washingtonpost.com;

45.http://www.wired.com;

46.http://www.wsj.com;