Univerza v Mariboru

Fakulteta za varnostne vede

MAGISTRSKO DELO

Neformalna ekonomija in kibernetska kriminaliteta

Februar, 2015

Matej Škufca

Mentor: red. prof. dr. Bojan Dobovšek

Kazalo

Kazalo grafov

Kazalo tabel

Povzetek

V magistrski nalogi smo povzeli dve raziskavi, in sicer Neformalno ekonomijo in kibernetsko kriminaliteto na Kitajskem ter Poročilo Symantec glede neformalne ekonomije v kibernetskem svetu. Ugotovili smo, da je kibernetska kriminaliteta ustvarila neverjetno zrelo in samostojno neformalno ekonomijo, ki je sestavljena iz štirih delov, ki se medsebojno povezujejo in dopolnjujejo. Cene in ponudbe se prilagajajo glede na povpraševanje in kvaliteto dobrine ali storitve. Kupec se lahko na podlagi vzorcev odloči, ali mu storitev oziroma dobrina ustreza ali ne. Najpogosteje se trguje z informacijami o kreditnih karticah ter s finančnimi računi.

Neformalna ekonomija se na svetovnem spletu največkrat nahaja na spletnih forumih ter na IRC-strežnikih. Delovati mora na javnih mestih, saj lahko samo tako privablja nove člane ter potencialne kupce. Ker pa je na ta način tudi na očeh organov pregona, mora večkrat spreminjati lokacije ter biti pazljiva pri sprejemanju novih članov. Glavni motiv članov kibernetske kriminalitete je dobiček, gre za ljudi različnih znanj in poklicev. Nekateri sodelujejo zgolj zaradi dodatnega zaslužka, medtem ko je za druge to način preživetja, to je seveda odvisno od splošnega stanja v državi ter od zaposlitvenih možnosti.

Plačila za dobrine in storitve na »podzemnih« strežnikih se najpogosteje opravijo po elektronski poti. Načinov plačila je več, najpogosteje pa je uporabljeno plačevanje s pomočjo spletnih valut, ki so na voljo po celem svetu, plačila so nepovratna, takojšnja, stroške transakcije pa nosi prodajalec. Drugi najpogostejši način plačila na »podzemnih« strežnikih pa je menjava dobrin ali storitev.

Osredotočili smo se tudi na zakonodajo. Povzeli smo Zakon o zaposlovanju in delu na črno ter Konvencijo o kibernetski kriminaliteti, ki je bila sprejeta konec leta 2001. Bistvo konvencije je poenotenje zakonodaje med državami podpisnicami ter ustanovitev mednarodne mreže, ki omogoča sodelovanje in pomoč med državami. Mednarodna mreža mora delovati neprekinjeno, saj se storilci kaznivih dejanj kibernetske kriminalitete ne držijo ustaljenih delovnih urnikov, ampak delujejo ob kateremkoli času na katerem koli mestu.

Na koncu smo še povzeli sklepne misli ter odgovorili na hipoteze, ki smo si jih postavili na začetku.

Ključne besede: neformalna ekonomija, kibernetska kriminaliteta, podzemna ekonomija, IRC-strežniki, forumi, goljufije.

Summary – Informal economy and cyber crime

In the master's thesis we summarized two researches – Informal economy and cyber crime in China and the Symantec report on informal economy in cyber space. We found that cyber crime established an unbelievably mature and independent informal crime, consisting of four parts that interconnect and complement each other. Prices and offers are adapting according to the demand and quality of the product or service. The customer can based on samples decide, whether the service or product suits him or not. It is mostly being traded with credit cards and financial accounts.

Informal economy on the web is mostly taking place on web forums and IRC servers. It has to operate in public places, since it this way invites new members and potential customers. Because it is always in front of the eyes of the authorities, it needs to frequently change its location and be careful in accepting new members. The main motive of the members of cyber crime is profit; these are people with different knowledge and occupations. Some participate only because of additional profit, but for some of them this is a way of living; depends on the general welfare of the county and employment possibilities.

Payments for products and services on underground servers mostly take place over the internet. There are more payment types, but most frequently they pay with the help of online currencies, available over the whole world; the payments cannot be returned, are immediate and the costs are paid by the seller. The second most popular payment type on underground servers is trading of products or services.

We also focused on the legislation. We summarized the Prevention of Undeclared Work and Employment Act and the Cybercrime convention of 2001. The essence of the convention is the unification of the legislation among signatory states and the establishment of an international network that enables cooperation and help among the countries. The international network has to operate continuously, since cybercrime offenders are never hanging on to routine work schedules, but are operating at any time, at any place.

Finally we summarized concluding thoughts and verified the hypotheses, set at the beginning.

Keywords: informal economy, cyber crime, underground economy, IRC servers, forums, fraud.

1 Uvod

Živimo v hitro spreminjajočem se svetu. V zadnjih dveh desetletjih je prišlo do ogromnih sprememb v razvoju svetovnega spleta. V začetku je bilo število uporabnikov majhno, vendar se je ta številka z leti zelo hitro večala. Zdaj si ne predstavljamo več življenja brez svetovnega spleta, saj z njegovo pomočjo komuniciramo, trgujemo in si izmenjujemo podatke. Svetovni splet ponuja ogromno priložnosti in ugodnosti, vendar na žalost ne samo poštenim ljudem. Kibernetskemu prostoru so se prilagodili storilci kaznivih dejanj, ki znanja informacijske tehnologije uporabljajo v kriminalne namene (Dobovšek in Drobnak, 2009).

Na svetovnem spletu obstaja sofisticirana in samoučinkovita digitalna »podzemna« ekonomija, kjer so podatki nedovoljen proizvod. Ukradene zasebne in finančne informacije imajo tržno vrednost. Ne prodaja se samo številk kreditnih kartic, tudi informacije, kot so naslov, telefonska številka, matična številka, datum rojstva, se znajdejo na tržišču. Vse to poganja zelo razširjen sistem kriminalnih dejavnosti, kot so spletno ribarjenje, oskrbovanje s kriminalnimi potrebščinami, vdiranje v podatkovne baze, s pomočjo posameznikov, ki so zelo tehnično usposobljeni na svojem področju. Tovrstna ekonomija se je v zadnjih letih razvila do popolnosti, njena tržna vrednost še ni točno znana, ocenjena je na približno 1 bilijon ameriških dolarjev. Goljufije s plačilnimi karticami so primer, kjer se zamegli meja med spletnimi in običajnimi goljufijami. Podatki plačilnih kartic, še posebej kreditnih kartic so idealen proizvod kriminalnega sveta, saj se jih brez težav lahko pošlje preko meja. Organizirani kriminal izkorišča prednost globalizacije, se premika iz države v državo ter tudi na druge celine, z namenom dvigovanja denarja iz zlorabljenih plačilnih kartic ter hkrati z namenom zabrisanja sledi, od kod izvira denar (Europol, 2011).

Pričakovali bi, da je sodelovanje s kibernetsko neformalno tržnico zelo drago, vendar ni tako. Večina orodij in podatkov, ki jih kibernetski kriminalec potrebuje za svoje delovanje, je dokaj poceni. Najem botneta, ki se šteje kot luksuzno orodje, stane približno 225 dolarjev, medtem ko pa na primer program za beleženje tipk stane zgolj 20 dolarjev. Ker se na trgu lahko kupi orodja, ki skoraj avtomatično delujejo, niti ni potrebnega veliko tehničnega znanja za nelegalno pridobivanje podatkov. Še nekaj let nazaj je bila večina kibernetskega kriminala osredotočena na osebne računalnike z naloženim sistemom Windows, vendar danes to več ne drži. Hekerji so se začeli osredotočati tudi na pametne telefone in tablične računalnike, ki imajo

ponavadi slabšo zaščito pred virusi in škodljivo programsko opremo kot osebni računalniki. Razlog za takšno zanimanje pa se skriva v tem, da vedno več posameznikov in organizacij opravlja finančne transakcije ravno preko telefonov in tablic (Bram, 2013).

Kibernetska kriminaliteta se zaradi značilnosti kibernetskega prostora, kot so občutek anonimnosti, mednarodni vidik, lokacijska in časovna neodvisnost, širi z neverjetno hitrostjo in zajema iz dneva v dan nove prostore in niše, le malo od teh pa je odkritih in procesiranih. Težje odkrivanje in pojavljanje novih oblik računalniške kriminalitete le to uvršča med najnevarnejše in družbi najbolj škodljive pojavne oblike sodobnega kriminala. Storilcem kaznivih dejanj na svetovnem spletu je v veliko pomoč neformalna ekonomija. Le ta se pojavlja povsod po svetu kot antipod formalni ekonomiji, čeprav je vidna le delno in poteka vzporedno s tokom družbenega in gospodarskega življenja evropskih mest.

Neformalna ekonomija zagotavlja škodljivo programsko opremo in druga orodja za storitev kaznivih dejanj na spletu, posoja botnete za izvrševanje napadov, razvija škodljivo programsko opremo in antiforenzično tehnologijo s katero se zabrišejo sledi, pošilja nezaželeno pošto na nešteto število naslovov. Neformalna ekonomija tudi ponuja trg ukradenih predmetov, kar na svetovnem spletu največkrat pomeni, da ponujajo številke kreditnih kartic ali bančne podatke ter druge osebne podatke, ki se jih ponavadi uporablja pri kraji identitete. Povedano na kratko, neformalna ekonomija ponuja ekonomsko okolje, za delovanje kibernetskega kriminala (Seger, 2012).

Definicija kibernetskega kriminala mora biti dovolj široka, da lahko zajame vsa različna kriminalna dejanja, ki so povezana s kibernetsko kriminaliteto. Najbolj uporabljena definicija se glasi: Kibernetska kriminaliteta je nelegalno dejanje, izvedeno z uporabo ali pomočjo informacijsko komunikacijskih tehnologij (Dobovšek in Drobnak, 2009).

Na svetovnem spletu obstaja ogromno različnih vrst kaznivih dejanj in goljufij. Ker pa je ta tema zelo obširna se bomo v magistrski nalogi omejili in analizirali naslednje vrste kibernetskega kriminala: goljufije s kreditnimi karticami, prevzeme bančnih računov, spletne prevare, goljufije na spletnih dražbah, investicijske goljufije, goljufije pri spletni prodaja farmacevtskih izdelkov ter na kršenje avtorskih pravic.

1.1 Cilji magistrskega dela

Poskušali bomo razložiti, kaj sploh je kibernetski kriminal, kakšni so njegovi začetki. Opisali bomo najpogostejše vrste kibernetskega kriminala. Pregledali bomo, na kakšen način se s to problematiko soočajo organi pregona v Sloveniji in svetu ter analizirali primere. Iz literature bomo poskušali čim bolje definirati delovanje neformalne ekonomije, ki podpira kibernetski kriminal. Poskušali bomo ugotoviti, kako daleč sežejo njihove povezave ter na kakšen način se začetniki povežejo z neformalno ekonomijo.

1.1.1 Predpostavke magistrskega dela

V okviru magistrske naloge smo si postavili tri hipoteze, ki jih bomo s podrobno analizo tematike zavrnili ali sprejeli.

Prva hipoteza:

Neformalna ekonomija prehaja v kibernetski svet.

Druga hipoteza:

Organi pregona so dobro izobraženi in usposobljeni za pregon tovrstne kriminalitete.

Tretja hipoteza:

V bolj razvitih državah sveta je stopnja kibernetskega kriminala višja kot v manj razvitih državah.

1.2 Uporabljene metode

Za pisanje magistrskega dela smo uporabili *metodo zbiranja pisnih virov* in *metodo analize pisnih virov* (strokovne literature, zakonodaje itd.). V empiričnem delu naloge pa smo uporabili *študijo primera*.

2 Opredelitev pojmov

V magistrskem delu bomo predstavili ter se ukvarjali predvsem s pojmoma neformalna ekonomija in kibernetska kriminaliteta.

2.1 Neformalna ekonomija

Ekonomijo lahko razdelimo v dva sektorja, formalnega in neformalnega. Raziskave kažejo, da neformalna ekonomija v državah v razvoju obsega od 20 % pa kar do 70 % bruto domačega proizvoda, in še vedno raste. V urbanih okoljih, kjer živi polovica svetovnega prebivalstva, pa neformalna ekonomija zaposluje med 40 % in 60 % ljudi. Državno, regionalno ali mestno gospodarstvo nikoli ne more biti popolnoma formalno ali popolnoma neformalno. Obstajajo segmenti, ki so bolj formalni kot neformalni, na drugi strani pa nekateri postajajo bolj neformalni. V zahodnih državah je formalna ekonomija dominantna oblika gospodarstva.

Izraz neformalni sektor se lahko nanaša na ulične prodajalce v Bogoti, voznike rikš v Kalkuti, zbiralce smeti v Kairu, izdelovalce oblačil v Manili in delavce z elektroniko v Kuala Lumpurju. Izraz neformalna ekonomija torej zavzema izjemno široko področje, mnogi strokovnjaki so si enotni, da je to področje preprosto preveč raznoliko, da bi ga lahko poimenovali s samo enim izrazom (Shapland in Ponsaers, 2010).

Neformalna ekonomija ni zabeležena v nobenih uradnih gospodarskih dokumentih. Označujejo jo tudi imena, kot so črna ekonomija, skrita ekonomija, senčna ekonomija, vzporedna ekonomija, podzemna ekonomija in podobno. Najbolj pogosto uporabljena definicija se glasi: »Neformalna ekonomija je del gospodarske aktivnosti, ki bi morala biti, pa ni zapisana v državnih podatkih.« Pojavlja se tako v državah v razvoju, kot tudi v zelo razvitih državah. Neformalno ekonomijo je težko prepoznati in še težje izmeriti (Danopoulos in Žnidarič, 2007).

Neformalna ekonomija je del ekonomije, ki je nereguliran in nelegalen. Lahko je videna kot siva ekonomija, to pomeni, da gre za neprijavljeno dejavnost, ki pa bi bila ob plačevanju davkov popolnoma legalna. Črna ekonomija pa ne more biti legalizirana, saj gre za dejavnost, ki je prepovedana z zakonodajo (npr. prodaja prepovedanih drog). Vse države, najsi bodo tiste v razvoju ali razvite, se borijo proti neformalni ekonomiji s sprejemanjem ustreznih ukrepov, katerih cilj je povečati prihodke s strani davkov.

V projektu učinkovitega boja proti neformalni ekonomiji so povzeli delo T. Spariusa, ki je predstavil tri tipologije neformalne ekonomije.

Ilegalna ekonomija: Ta tip ekonomije ponavadi vključuje zelo široko paleto dejavnosti, kot so: tihotapljenje, izdelava in distribucija prepovedanih drog, prostitucija, igre na srečo, ponarejanje, izsiljevanje, ugrabitve, kraje itd.

Neprijavljena dejavnost: Se nanaša na skupino dejavnosti, ki so v bistvu legalna, vendar iz različnih razlogov skrita pred upravnimi in davčnimi organi. Torej glede na to, da je dejavnost neprijavljena, se lahko ravno tako šteje za nezakonito dejavnost, ki pa ni prepovedana. Za neprijavljanje dejavnosti obstaja več razlogov. Največkrat gre za izogibanje plačevanja davkov, socialnih prispevkov ter za izmikanje neprilagodljivim predpisom o zaposlitvi.

Dejavnost na domu: Ponavadi gre za delo na domu, kot je npr. priprava hrane, čiščenje, pospravljanje, varstvo otrok. Te dejavnosti tudi niso prepovedane, vendar so neprijavljene, kar pomeni, da dohodek ni prikazan v nobeni evidenci, posledično pa država ostane brez davkov (Andrić in Mijović, 2010).

Dobovšek meni, da škoda, ki jo povzroča neformalna ekonomija obsega kar 50 odstotkov bruto domačega proizvoda. Poleg že omenjenih sive in črne ekonomije, omenja tudi belo ekonomijo. Bela ekonomija je del neformalne ekonomije, za katero stojijo politične in gospodarske elite, ki se okoriščajo na račun lukenj v sistemu. Po njegovem mnenju, je v boju proti beli ekonomiji ključno sodelovanje policije in tožilstva ter davčnih in drugih domačih in mednarodnih nadzornih mehanizmov (Žurnal24.si, 2014).

Schneider in Buehn sta v članku, kaj so glavni razlogi zakaj pride do »senčne« ekonomije v razvitih državah OECD, zapisala naslednje razloge:

- Višina davčne obremenitve: Višina skupne obdavčitve ima velik vpliv pri tem, ali se posameznik odloči oziroma ne odloči sodelovati v neformalni ekonomiji. Večja kot je razlika med stroški dela ter dejanskim zaslužkom, večja je verjetnost, da se bodo posamezniki poskušali izogniti plačilu davkov. Višina davčne obremenitve je eden od najpomembnejših razlogov za obstoj neformalne ekonomije.
- Kvaliteta institucij: Kvaliteta javnega sektorja je naslednji ključni faktor za razvoj neformalne ekonomije. Še posebej pomembni so učinkovitost, davčna zakonodaja ter ostali zakoni s strani države. Prej našteto je verjetno še bolj pomembno od višine davčne obremenitve. Torej, sistem z visoko koruptivno politiko se sooča z večjo neformalno aktivnostjo. Na drugi strani pa sistem,

kjer vlada pravna država in kjer so človekove pravice zaščitene, spodbuja formalno delo.

- Zakonodaja: Zakonodaja, ki postavlja ovire pri trgovanju, je tudi eden od razlogov, ki poveča udejstvovanje pri neformalni ekonomiji. Države, ki imajo strožjo zakonodajo, se tudi v večji meri soočajo z neformalno ekonomijo.
- Storitve javnega sektorja: Povečanje neformalne ekonomije pomeni manj prihodkov za državo s strani davkov, kar vodi v zmanjšanje kvalitete delovanja javnega sektorja. To nadalje vodi v višanje davčne stopnje za podjetja in posameznike, da bi se izboljšalo delovanje javnega sektorja. Vendar ima vse to samo še večji negativni učinek, saj se na ta način stopnja neformalne ekonomije samo še poveča. Države, ki pridobijo največ denarja z najmanjšo davčno stopnjo, ki imajo manj strogo zakonodajo, nizko stopnjo koruptivnosti in učinkovit pravni sistem, bi morale imeti najmanjšo stopnjo neformalne ekonomije.
- Zavedanje o plačevanju davkov: Učinkovitost javnega sektorja ima tudi indirektni učinek na stopnjo neformalne ekonomije. Če je javni sektor učinkovit, je večje tudi zavedanje o plačevanju davkov, oziroma bolj kot je javni sektor učinkovit, državljani in podjetja raje sodelujejo pri plačevanju davkov, saj so v končni fazi z javnimi storitvami tudi poplačani in imajo od tega korist. Seveda to deluje tudi obratno. Slabše kot je delovanje javnega sektorja, nižja je tudi pripravljenost plačevanja davkov.
- Odvračanje: Kljub visoki osredotočenosti organov pregona na odvračanje in zastraševanje od neformalne ekonomije, je presenetljivo zelo malo empiričnih študij, ki bi raziskale ali to odvračanje sploh ima pozitivne učinke. Razlog tiči v tem, da podatki o poslovanju in številu revizij niso dostopni na mednarodni ravni, celo za države OECD[1] je take podatke težko pridobiti. Nekaj malega empiričnih raziskav iz tega področja pa je ugotovilo, da višina globe in kazen ne delujejo tako zastrašujoče, da bi posameznika odvrnile od sodelovanja v neformalni ekonomiji, bolj kot to je odvračajoče zaznavanje posameznika, kolikšna je verjetnost, da bo le-ta odkrit in kaznovan.

[1] OECD – Organisation for Economic Co-operation and Development oziroma prevedeno Organizacija za gospodarsko sodelovanje in razvoj. Je mednarodna gospodarska organizacija razvitih držav.

2.2 Kibernetska kriminaliteta

O nevarnostih uporabe kibernetskega prostora[2] se je začelo govoriti, ko so se pojavile tehnologije, ki so omogočale komuniciranje in opravljanje vsakodnevnih nalog. Omogočeno je bilo nakupovanje, plačevanje blaga in storitev, pošiljanje datotek, prenašanje podatkov ter ostale prednosti, ki jih ponuja svetovni splet. Naši podatki in gesla, ki smo jih uporabljali pri teh storitvah, pa so postala zelo zanimiva za morebitne napadalce. V primeru kraje podatkov posledice niso zabavne, lahko pride tudi do izgube večje količine denarja. V izogib vsem tem težavam se je začelo vzpostavljati sisteme informacijske varnosti. Ves čas sledijo razvoju kibernetskega prostora tudi nove oblike kriminalitete. Do večine zlorab pride zaradi neznanja ali brezbrižnosti ljudi, ki uporabljajo računalnike, ki so povezani v internet, saj z informacijskimi sredstvi ravnajo nevestno. Količina sredstev namenjenih kibernetskemu kriminalu se stalno povečuje, saj je finančna korist kibernetske kriminalitete ogromna. Gospodarska kriza pa samo še pripomore k večanju kibernetskega kriminala, saj se kriminalnim združbam pridružuje vedno več izobraženih ljudi, ki ne dobijo ustrezne zaposlitve in poštenega plačila na trgu dela. Pri informacijski varnosti je pomembno, da se najde ustrezno stopnjo varnosti in zaščite. Prevelika stopnja varnosti in zaščite povzroči v organizaciji veliko težav, saj je oteženo hitro dostopanje do želenih informacij. Če pa je informacijska varnost prenizka, pa se močno poveča verjetnost nepooblaščenega dostopa. Ker je Slovenija majhna in si ne more privoščiti lastnega oddelka za pregon kibernetskega kriminala, je potrebno, da sodeluje in se povezuje z državami, ki imajo na tem področju več izkušenj ter sredstev. Prav tako je mednarodno sodelovanje zelo pomembno, saj je izmenjava informacij ključna pri preiskovanju kibernetske kriminalitete, ker ta ne pozna meja. Kibernetsko kriminaliteto pojmujemo kot kaznivo uporabo računalniškega omrežja ali drugega sistema na internetu, napade ali zlorabe sistemov in omrežij za izvedbo kaznivih dejanj in zlorabe, storjene z uporabo novih tehnologij, ali nova kazniva dejanja, ki se na novo razvijajo v kibernetskem prostoru. Kibernetsko kriminaliteto pojmujemo kot kriminaliteto, ki jo sestavljajo kazniva dejanja, pri katerih se informacijska tehnologija (računalnik, tablica, mobilnik) pojavlja kot orodje ali kot predmet napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje računalništva ali informatike. Izraz kibernetska kriminaliteta se nanaša na dejanja, ki so storjena s pomočjo elektronske

[2] Kibernetski prostor je elektronski medij za izmenjavanje informacij v računalniških in drugih (mobilnih, spletnih) omrežjih, ki omogočajo možnost stalne povezanosti in komunikacijo.

opreme za obdelavo podatkov in ki povzročijo neželene posledice (Bernik in Prislan, 2012).

Da lahko definicija kibernetske kriminalitete zajame vso raznolikost kriminalnih dejanj v povezavi z informacijsko komunikacijskimi tehnologijami, mora biti dovolj široka. Obravnava kaznivega dejanja pa mora biti z vidika kazensko procesnega prava enaka, ne glede na to, kje je bilo dejanje storjeno, v virtualnem ali resničnem svetu. Najpogosteje uporabljena definicija se glasi: »Kibernetska kriminaliteta je nelegalno dejanje izvedeno z uporabo ali s pomočjo informacijsko komunikacijskih tehnologij.« Definicija Urada Združenih narodov za droge in kriminal pa se glasi: »Kibernetska kriminaliteta je delovanje, ki vključuje uporabo digitalne tehnologije pri izvedbi kršitve, je usmerjeno na področje informacijskih in komunikacijskih tehnologij ali vključuje uporabo računalnikov v povezavi z drugimi kaznivimi dejanji.«

Pri obravnavi tematike o kibernetski kriminaliteti se pojavljajo naslednji pojmi: računalniška kriminaliteta; kriminaliteta, povezana z računalnikom, ter kibernetska kriminaliteta.

O računalniški kriminaliteti govorimo v primerih, pri katerih je uporaba računalnika bistvena za izvedbo kaznivega dejanja.

O kriminaliteti, povezani z računalnikom, govorimo v primerih, pri katerih ima računalnik določeno vlogo pri izvedbi kaznivega dejanja, ki pa ni ključna, računalnik je lahko uporabljen zgolj kot pripomoček.

Termin kibernetska kriminaliteta pa se uporablja za kazniva dejanja, storjena s pomočjo in v okviru interneta (Dimc in Dobovšek, 2012).

Leta 2001 je Svet Evrope sprejel prvi mednarodni pravni akt, ki sodobno kibernetsko kriminaliteto obravnava z vidika priporočil, ki naj jih podpisnice upoštevajo pri oblikovanju in reformi svojega notranjega prava. Konvencija se nanaša predvsem na spremembe v kazenskem materialnem in procesnem pravu ter na spremembe in dopolnitve predpisov, ki urejajo telekomunikacije. Določa tudi splošen okvir mednarodnega sodelovanja preiskovalcev, saj kibernetska kriminaliteta pogosto presega meje nacionalnih jurisdikcij (Svet Evrope, 2001).

2.2.1 Kategorizacija kibernetske kriminalitete

Natančna kategorizacija kibernetske kriminalitete je zelo problematična, saj se informacijske tehnologije izredno hitro razvijajo, s tem pa tudi pojav kibernetske

kriminalitete. Dr. Dobovšek in mag. Dimc v njuni knjigi povzemata kategorizacijo po Taylorju, ki kategorizira kibernetsko kriminaliteto glede na vlogo, ki jo igra računalnik pri kaznivem dejanju: računalnik kot tarča kaznivega dejanja, računalnik kot orodje kaznivega dejanja, računalnik kot pomoč pri kaznivem dejanju ter kazniva dejanja, povezana s široko uporabo računalnikov. Poudariti je treba, da se ta kategorizacija nanaša na vse informacijsko komunikacijske elektronske naprave (npr. mobilne naprave in tablice), saj so prevzele enake funkcionalnosti kot računalniki (Dobovšek in Dimc, 2012).

- **Računalnik kot tarča kaznivega dejanja**

Cilj tovrstnih kaznivih dejanj je onemogočiti normalno delovanje računalnika, računalniškega ali informacijskega sistema.

Primeri: vdor v sistem; onemogočenje storitev (DoS[3] in DDoS[4] napadi); uničenje ali sprememba podatkov.

- **Računalnik kot orodje kriminalnega dejanja**

V tem primeru se računalnik uporabi z namenom, da se doseže nek sekundarni kriminalni namen. Računalnik je torej zgolj orodje, s pomočjo katerega storilec počne kazniva dejanja.

Primeri: kraja (podatkov in informacij); kraja storitev (kraja digitalnega signala); prevare (nigerijsko pismo 419); grožnje, nadlegovanje in zalezovanje.

- **Računalnik kot pomoč pri kriminalnem dejanju**

Pri teh kaznivih dejanjih računalnik ne igra primarne vloge, temveč je zgolj pripomoček za olajšanje ali izboljšanje učinkovitosti kriminalnih dejanj.

Primeri: pranje denarja; otroška pornografija; uporaba računalnika pri navezovanju stikov s potencialno žrtvijo (pedofili, posiljevalci, morilci).

- **Kriminalna dejanja, povezana s široko uporabo računalnikov**

[3] DoS (*Denial Of Service*) ali zavrnitev storitve je proces, ki so ga razvili hekerji okoli leta 2000. DoS se izvaja tako, da heker pošlje tarči veliko količino podatkov določenega protokola ter s tem upočasni ali onemogoči tarčo.
[4] DDoS (*Distributed Denial of Service*) ali porazdeljena zavrnitev storitve. Princip delovanja je isti kot pri DoS, le da tukaj napadalec uporablja večje število podračunalnikov ali zombijev.

Široka uporaba računalnikov je vplivala na razvoj, dostopnost in celo sprejemljivost nekaterih oblik kriminalitete, saj nas informacijsko komunikacijske tehnologije spremljajo na vsakem koraku in so postale običajen del našega življenja.

Primeri: kraja intelektualne lastnine (piratstvo), ponarejanje (uporaba grafičnih programov), kraja identitete.

Kibernetska kriminalna dejanja le redko spadajo v samo enega od navedenih tipov, ampak gre ponavadi za kombinacijo dveh ali več dejanj.

2.2.2 Vrste kibernetske kriminalitete

Goljufije s plačilnimi karticami (Payment Card Fraud): Ključni faktor pri vzdrževanju ekonomske stabilnosti Evropske unije je zagotoviti varno negotovinsko poslovanje. V letu 2011 je bilo v Evropski uniji izdanih več kot 726 milijonov plačilnih kartic. Vsota vseh transakcij s plačilnimi karticami pa je presegla 3000 milijard evrov. Europol v svojem poročilu sporoča, da organizirane kriminalne skupine uspešno koristijo prednosti svetovnega spleta, med katerimi je največja prednost globalnost le tega. Informacije o kreditnih karticah in številke bančnih računov so najbolj zaželeni podatki na strežnikih neformalne ekonomije. V letu 2011 je bilo 60 % vseh goljufij pri plačilih povzročenih s plačilnimi karticami, kar znese približno 900 milijonov evrov, storjenih na način, da plačilna kartica ni bila prisotna. To pomeni, da je bil predmet ali storitev plačana preko spleta. Preiskovalci goljufij, ki jih podpira Europol, menijo, da se z uporabo notranjih informacij in z uporabo zlonamerne programske opreme najpogosteje pride do podatkov, potrebnih za goljufije s plačilnimi karticami. V večini primerov je število ukradenih podatkov ogromno, saj gre za nekaj sto tisoč pa vse do več milijon podatkov, kar omogoča kriminalnim skupinam, da te podatke prodajajo na spletu (Europol, 2012).

Spletni napadi in prevzemi bančnih računov (Online Banking Attacks and Account Takeover): Spletni prevzemi bančnih računov so neke vrste kraja identitete. Do prevzema bančnega računa pride, ko namesto lastnika do računa dostopa nekdo drug, ki prevzame nadzor nad obstoječim računom. Do večine prevzemov računov ponavadi pride z uporabo škodljive programske opreme, vendar pa storilci uporabljajo tudi socialni inženiring[5], s pomočjo katerega poskušajo spodbuditi žrtev, da razkrije

[5] Socialni inženiring pomeni uporabljanje vpliva in prepričevanja z namenom zavajanja ljudi, da verjamejo, da je socialni inženir nekdo, ki to ni, ali z manipulacijo. Posledica tega je, da

kakšno informacijo glede svojega bančnega računa. S pomočjo teh informacij lahko goljufi v kratkem času dostopajo do bančnih računov in z njih poberejo denar. V raziskavi Javelin so ugotovili, da so izgube zaradi prevzemov bančnih računov presegle 4,9 milijarde dolarjev v letu 2012, kar je kar 69 odstotkov več kot leto prej. Prevzemi računov so možni na več načinov, vendar se goljufi najpogosteje poslužujejo uporabe ribarjenja[6] in nezaželene pošte, s pomočjo katerih prevzamejo nadzor. Pogosto se uporablja tudi programe za beleženje tipk (keyloggers), ki nadzirajo in zabeležijo vsak pritisk na tipko ter na ta način pridobijo podatke, med katerimi so tudi podatki o bančnih računih. Program pošlje vse pridobljene podatke goljufu, ki s tem pridobi dostop do računov (Castell, 2013).

Goljufije, storjene s pomočjo sredstev za množično obveščanje (Mass marketing fraud): Tovrstni izraz se uporablja za goljufije, ki za svoje delovanje uporabljajo sredstva množičnega obveščanja. Svetovni splet, telefon, e-pošta, televizija, radio ter tudi osebni kontakt so načini, s pomočjo katerih goljufi kontaktirajo morebitne žrtve iz celega sveta ter poskušajo od njih pridobiti denar ali vredne predmete. Za goljufije, storjene s pomočjo sredstev za množično obveščanje, se uporablja več različnih izrazov, kot so recimo kreditne goljufije (advance-fee fraud), nigerijske prevare »419« (419 fraud), internetne prevare (internet fraud) in podobno. Izrazov za tovrstne goljufije je vedno več, vendar kljub temu da ima neka goljufija drugačen izraz, je v osnovi zelo podobna ostalim, saj so metode delovanja ter načini komuniciranja z morebitno žrtvijo zelo podobni.

Goljufi, ki se ukvarjajo z goljufijami, ki so storjene s pomočjo sredstev za množično obveščanje, delujejo in iščejo morebitne žrtve po vsem svetu. Zavedajo se ter izkoriščajo razlike med državnimi zakonodajami, ki na različne načine predpisujejo ter omejujejo tovrstne goljufije. Posledica vsega tega je, da so goljufije, storjene s pomočjo sredstev za množično obveščanje, postale velik problem v več državah po svetu.

Mednarodna skupina za boj proti goljufijami storjenimi s pomočjo sredstev za množično obveščanje (IMMFWG[7]) je pripravila oceno tveganja, ki vladam in javnosti po svetu predstavi samo naravo in razširjenost pojava. Mednarodna skupina, ki je bila

---

lahko socialni inženir izkoristi ljudi tako, da od njih pridobi informacije z ali brez uporabe tehnologije.

[6] Ribarjenje (phishing) je v računalništvu nezakonit način zavajanja uporabnikov, namenjenega pridobivanju tujih občutljivih osebnih podatkov. Pri takšnem zavajanju poskuša oseba, ki to izvaja, pridobiti podatke, npr. številke kreditnih kartic, gesla, podatke o računih ali druge osebne podatke tako, da pod pretvezo prepriča žrtev o potrebi po posredovanju teh podatkov. Prevare »phishing« uporabniki običajno prejmejo z neželeno e-pošto ali kot pojavna okna.

[7] IMMFWG – International Mass-Marketing Fraud Working Group.

ustanovljena leta 2007, je sestavljena iz organov kazenskega pregona, nadzornih organov in agencij za zaščito potrošnikov iz več držav, med katerimi so Avstralija, Belgija, Kanada, Nizozemska, Nigerija, Velika Britanija in ZDA ter Europol. Cilj te mednarodne skupine je olajšati mednarodno izmenjavo informacij in zaupnih podatkov, uskladiti čezmejno delovanje s končnim ciljem, odkritja ter prijetja storilcev goljufij. Zelo pomembno pa je tudi izboljšati javno zavedanje o nevarnostih goljufij, ki se jih stori s pomočjo sredstev za množično obveščanje (International Mass-Marketing Fraud Working Group, 2010).

Goljufije na spletnih dražbah (Confidence Fraud Including Auction Fraud): Spletne dražbe so zelo dober način, kako povezati prodajalce s kupci. Največja težava pri spletnih dražbah je, da kupec samega izdelka ne vidi v popolnosti. Spletni goljufi lahko na dražbah napačno predstavijo izdelek, z manipuliranjem pri dvigu cen kupec na koncu plača bistveno več, kot bi plačal brez manipulacije, prodani izdelek je lahko v resnici ponarejen, obstaja pa tudi možnost, da plačanega izdelka sploh ne prejme.

Goljufije na spletnih dražbah so ena najbolj pogostih goljufij na svetovnem spletu. Center za zbiranje prijav na spletu (Internet Crime Complaint Center) je v svojem poročilu izjavil, da je skoraj vsaka četrta pritožba povezana z goljufijami na spletnih dražbah. Vsak, ki sodeluje na spletnih dražbah, je lahko potencialna žrtev, vendar je tveganje večje, če je prodajalec iz tujine, saj se zakonodaja spreminja od države do države. Poleg vsega pa je možnost, da nekdo postane žrtev na spletni dražbi večja, če ni seznanjen z izdelkom, ki ga hoče kupiti, saj je lahko izdelek ponarejen ali pa slabše kvalitete.

Goljufi na spletnih dražbah se največkrat poslužujejo spodaj naštetih metod goljufije:

- Napačna predstavitev izdelka (misrepresentation) – prodajalec namenoma zavaja kupca glede prave vrednosti izdelka. Informacije o izdelku ali storitvi so napačne, priložene so lahko tudi slike, ki ne predstavljajo dejanskega stanja. Prodajani izdelek je lahko tudi ponarejen, najpogosteje se prodajajo ponarejeni CD-ji in DVD-ji ter ponaredki modnih oblačil.
- Nedostava plačanega izdelka (nondelivery) – gre za eno najbolj pogostih goljufij na spletnih dražbah. Kupec plača določen izdelek, vendar ga kljub plačilu ne prejme. V primeru, da kupec plača s kreditno ali debetno kartico obstaja možnost dodatne zlorabe, saj prodajalec pridobi informacije o kartici.

- Triangulacija (triangulation) – v tem primeru goljuf kupi izdelek preko spelta, za nakup pa uporabi ime osebe, kateri so ukradli identiteto in ukradene številke kreditnih kartic. Nato proda izdelek nič hudega sluteči žrtvi na spletni dražbi. Ko je nakup opravljen, kupec prejme izdelek, vendar se kmalu znajde sredi preiskave glede ukradenega izdelka. Organi pregona izdelek odvzamejo, tako da kupec ostane brez denarja in brez izdelka, za katerega je plačal. Škodo pa utrpi tudi lastnik spletne prodajalne, saj je na ta način oškodovan njegov ugled, kar pomeni manjši obisk strani ter posledično manjši zaslužek.
- Dodatni stroški (hidden charges) – spletni trgovec po zaključku dražbe razkrije dodatne stroške, ki jih bo moral plačati kupec. Ti stroški močno povečajo ceno, ki je bila ob koncu dražbe.
- Golufije pri ponudbah (bidding schemes) – goljuf si ustvari več identitet in na spletni dražbi odda več ponudb, ki dvignejo ceno izdelka ter prestrašijo morebitne kupce. Zadnji trenutek, ko se dražba zaključuje, umakne najvišje ponudbe ter na ta način dobi izdelek po mnogo nižji ceni, kot bi bila sicer. Obstaja pa tudi obraten način goljufije, kjer goljuf ter včasih še njegovi prijatelji dvigujejo ceno izdelka, ki jo goljuf prodaja. Na ta način je izdelek prodan za višjo vsoto, kot bi bil brez goljufije.
- Druga priložnost (second-chance schemes) – v tem primeru goljuf ponudi ostalim, ki so izgubili na dražbi želeni predmet po znižani ceni. Kupci dobijo navodilo, da goljufu nakažejo denar. Ko goljuf denar prejme, ga ne slišijo nikoli več (Jones, 2012).

Investicijske in borzne goljufije (Investment Fraud Including Stock Market Manipulation): Večina goljufij na svetovnem spletu izvira še iz časov, ko svetovnega spleta sploh še ni bilo. Prej so goljufi pošiljali navadno pošto ali pa hodili od vrat do vrat in na ta način poskušali najti in ogoljufati morebitno žrtev. Svetovni splet je samo še povečal možnosti goljufom za uspeh. Na primer lepo oblikovana spletna stran lahko ustvari iluzijo velikega in uglednega podjetja, še posebej če vsebuje tudi povezave do legitimnih strani.

Štiri najpogostejše investicijske in borzne goljufije na svetovnem spletu so:

- Piramidne igre (Ponzi Scheme) – gre za igro v obliki piramide, kjer se denar novih vlagateljev uporabi za plačilo prejšnjim vlagateljem. Vsaka piramidna igra enkrat propade, in sicer ko je vsota dolga do prejšnjih vlagateljev višja od vsote vložka novih vlagateljev.

- Goljufije z delnicami (Pump and Dump) – pri tej goljufiji manjše število goljufov opravi nakup delnic nekega podjetja, nato pa s pomočjo svetovnega spleta obvestijo morebitne investitorje, da so s pomočjo notranjih informacij ugotovili, da bo vlaganje v delnice podjetja prineslo velik donos. Delnice na ta način začnejo pridobivati na vrednosti in ko dosežejo vrh, goljufi svoj delež prodajo, kar pomeni, da vrednost delnic doživi velik padec. Pri vsem tem imajo goljufi dobiček, ostali pa ostanejo z delnicami, ki imajo mnogo manjšo vrednost.
- Investicije v tujino (Off Shore Investing) – pri tovrstnih ponudbah je potrebno biti pozoren in skeptičen. V primeru goljufije bodo organi pregona težko odkrili in kaznovali goljufe v tujini.
- Glavna banka (Prime bank) – to je izraz za približno petdeset najboljših bank sveta. Te banke odlikuje velika zanesljivost in varnost. Tega izraza se poslužujejo goljufi, ki na ta način delujejo bolj prepričljivo. Potencialne vlagatelje zavedejo z investicijskim programom banke, ki naj bi zagotovil velik donos ob majhnem tveganju. Ker pa v resnici ti programi ne obstajajo, izgubijo vlagatelji ves vložek (Investopedia, 2014).

Prodaja ponarejenih zdravil in medicinskih pripomočkov na svetovnem spletu (Counterfeit Pharmaceuticals):

Ponarejena zdravila in medicinski pripomočki predstavljajo kriminalen trg, vreden več milijonov dolarjev. Ponarejeni izdelki so lahko sestavljeni iz pravilnih ali nepravilnih sestavin, lahko so brez aktivnih sestavin oziroma jih je v njih premalo, ponarejena pa je lahko tudi sama embalaža. Kriminalne združbe izkoriščajo možnosti, ki jih ponuja svetovni splet, z namenom prodaje ponarejenih zdravil in medicinskih pripomočkov ter ustvarjanja visokih dobičkov ob majhnem tveganju in nizkih stroških.

Glavna dva načina prodaje ponarejenih zdravil in medicinskih pripomočkov na svetovnem spletu sta:

- Prodaja preko spletnih lekarn, ki prodajajo neustrezna, nesprejeta ali ponarejena zdravila in medicinske pripomočke. Plačilo za izdelke se izvede preko svetovnega spleta, denar pa se nakaže v banko, ki se nahaja v tujini.
- Masovno oglaševanje oziroma pošiljanje nezaželene pošte z namenom dosega čim večjega števila potencialnih kupcev. Glede na Commtouch raziskavo iz

leta 2010 je kar 81 % vse nezaželene pošte povezane s prodajo ponarejenih zdravil in medicinskih pripomočkov (Seger, 2012).

Kršenje avtorskih in podobnih pravic: Avtorska dela so individualne intelektualne stvaritve s področja književnosti, znanosti in umetnosti, ki so na kakršenkoli način izražene, na primer: govorjena dela, pisana dela, fotografska dela, avdiovizualna dela, likovna dela, kartografska dela itd. Kot avtorsko delo niso varovane ideje, načela in odkritja, prav tako niso varovana uradna besedila z zakonodajnega, upravnega in sodnega področja ter ljudske in književne umetniške stvaritve. Avtor je fizična oseba, ki je delo ustvarila. Avtorska pravica pripada avtorju na podlagi same stvaritve dela, zato ni potreben noben postopek, da bi bilo avtorskopravno varovano. Ko avtor na primer napiše roman, je njegovo delo že varovano in ima na njem avtorsko pravico. Avtorska pravica traja za časa avtorjevega življenja in 70 let po njegovi smrti. Urad RS za intelektualno lastnino je pristojen za pripravo zakonodaje s področja avtorskega prava, za izdajo dovoljenj kolektivnim organizacijam za opravljanje njihove dejavnosti ter za nadzor nad njihovim zakonitim delovanjem (Urad RS za intelektualno lastnino, 2014).

Tehnološki napredek in široko razširjena uporaba interneta predstavljata velik izziv pri varovanju avtorskih in podobnih pravic, še posebej zaradi razlogov, navedenih v nadaljevanju:

- Avtorsko zaščiteno vsebino se brez večjih težav kopira in prenaša v digitalni obliki po celem svetu s pomočjo interneta.
- Internet sam po sebi ne loči med dovoljenim in nedovoljenim prometom.
- Ne obstaja univerzalen globalni zakon, ki bi varoval avtorske pravice (kar je v neki državi dovoljeno, je lahko v drugi kaznivo in obratno).
- Število kršiteljev je lahko zelo veliko, njihova identiteta je težko določljiva, poleg tega pa se lahko nahajajo na ozemlju, ki je zunaj dosega organov pregona.

To je čas raziskovanja. Države po vsem svetu skupinsko in posamično raziskujejo in preizkušajo nove možnosti, kako izboljšati boj proti kršenju avtorskih in podobnih pravic. Obstaja velik mednarodni interes po uskladitvi zakonov o digitalnih avtorskih pravicah. Prezgodaj je, da bi lahko rekli, kakšen je pravilni pristop pri boju proti kršenju avtorskih pravic. Potrebnih je še veliko raziskav in posvetovanja, da se bo našel pravi način (Internet Society, 2011).

3 Neformalna ekonomija in kibernetska kriminaliteta

V tem poglavju se bomo seznanili s samo zakonodajo, ki poskuša slediti izredno hitremu razvoju informacijsko komunikacijske tehnologije. Poiskali bomo čim več definicij in poskušali ugotoviti, kakšen vpliv ima neformalna ekonomija v povezavi s kibernetsko kriminaliteto ter kakšne so razsežnosti teh dveh pojavov. Analizirali bomo delovanje neformalne ekonomije in kibernetske kriminalitete in poskušali ugotoviti, ali obstajajo kakšne povezave z drugimi kriminalnimi dejanji.

3.1 Zakonodaja

3.1.1 Zakon o preprečevanju dela in zaposlovanja na črno (ZPDZC-1)

Državni zbor RS je na seji dne 23. aprila 2014 objavil Zakon o preprečevanju dela in zaposlovanja na črno (ZPDZC-1). Zakon je pričel veljati 20. 5. 2014, uporabljati pa se je začel 90. dan po njegovi uveljavitvi, to je 18. 8. 2014, z izjemo členov, ki se nanašajo na osebno dopolnilno delo, ki se pričnejo uporabljati 1. 1. 2015 (Uradni list RS, 2014).

Zakon med drugim navaja dejavnosti in dela, ki niso delo ali zaposlovanje na črno, opredeljuje pojem sosedska in sorodstvena pomoč humanitarno delo, karitativno delo, delo za invalidske organizacije, prostovoljno ter dobrodelno delo, osebno dopolnilno delo. Navaja tudi kje najdemo seznam posameznikov, ki opravljajo osebno dopolnilno delo. Kako je s prihodki iz naslova osebnega dopolnilnega dela. Opredeljuje tudi globe za: kršitev prepovedi dela na črno, omogočanje dela na črno, kršitev prepovedi zaposlovanja na črno ter druge globe. Zakon navaja pokojninsko in invalidsko zavarovanje ter zdravstveno zavarovanje oseb, ki opravljajo osebno dopolnilno delo ter kolikšna je višina prispevka za osebno dopolnilno delo.

Delo na črno je opravljanje dejavnosti ali dela, kadar:

- pravna oseba ali tuj pravni subjekt, ki je pravna oseba, opravlja dejavnost, ki ni določena v ustanovitvenem aktu, ali če nima z zakonom predpisanih listin o izpolnjevanju pogojev za opravljanje dejavnosti, določene v ustanovitvenem aktu;

- samozaposlena oseba ali tuj pravni subjekt, ki je samozaposlena oseba, opravlja dejavnost, ki ni vpisana v register, ali nima z zakonom predpisanih listin o izpolnjevanju pogojev za opravljanje te dejavnosti;
- pravna oseba, tuj pravni subjekt ali samozaposlena oseba opravlja dejavnost kljub prepovedi opravljanja dejavnosti;
- tuj pravni subjekt opravlja dejavnost v Republiki Sloveniji brez registrirane podružnice ali brez predpisanega dovoljenja;
- pravni subjekt, ki ima sedež v državi članici Evropske unije, Evropskem gospodarskem prostoru ali Švicarski konfederaciji, ne opravlja dejavnosti storitev v skladu z zakonom, ki ureja storitve na notranjem trgu;
- posameznik opravlja dejavnost ali delo in ni vpisan ali nima priglašenega dela, kakor to določa ta ali drugi zakoni.

Zaposlovanje na črno je, če pravna oseba ali podjetnik, ki izpolnjuje pogoje za opravljanje dejavnosti:

- z delavcem ni sklenil pogodbe o zaposlitvi oziroma pogodbe civilnega prava, na podlagi katere se lahko opravlja delo, in delavca ni prijavil v zdravstveno ter pokojninsko in invalidsko zavarovanje,
- zaposli tujca ali osebo brez državljanstva v nasprotju s predpisi o zaposlovanju tujcev,
- omogoči delo dijaka ali študenta brez ustrezne napotnice pooblaščene organizacije za posredovanje dela, ali če omogoči, da to napotnico uporabi za delo druga oseba,
- nezakonito zaposli državljana tretje države,
- kadar posameznik v svojem imenu in za svoj račun zaposli delavca, ki zanj opravlja delo na črno.

Nedovoljeno oglaševanje

Ni dovoljeno naročanje, objavljanje ali posredovanje oglasov in oglasnih sporočil v časopisih, revijah, na radiu, televiziji in v drugih elektronskih medijih ali na drug način, ki je dostopen javnosti, če pravna oseba, tuj pravni subjekt, samozaposlena oseba, delodajalec ali posameznik ponuja ali oglašuje dejavnost ali delo, ki se šteje za delo na črno po določbah tega zakona; če delodajalec objavi potrebo po delavcu za delo, ki ni vezano na njegovo registrirano ali priglašeno dejavnost. Naročnik oglasa mora ob naročilu oglasa podati izjavo z naslednjimi podatki: firmo in sedež firme ter

osebno ime odgovorne osebe, ali osebno ime in naslov naročnika, in izjavo, da ima dejavnost, vsebina katere se nanaša na objavo oglasa, opredeljeno v ustanovitvenem aktu oziroma vpisano v register. Oglaševalska organizacija ne sme objaviti oglasa, če naročnik oglasa ne poda teh podatkov.

Dejavnosti in dela, ki niso delo ali zaposlovanje na črno

Za delo na črno ne štejejo sosedska pomoč (opravljanje dela med sosedi posamezniki, kadar med njimi obstaja določena bližina v smislu prebivanja, če med njimi ni sklenjene pogodbe in je delo opravljeno brez plačila), sorodstvena pomoč, nujno delo, humanitarno delo, karitativno delo, delo za invalidske organizacije in prostovoljno ter dobrodelno delo, osebno dopolnilno delo. Zakon v delu, ki se nanaša na izvajanje osebnega dopolnilnega dela, prinaša kar nekaj sprememb (sistem vrednotnic), ki je začel veljati 1. 1. 2015.

Za zaposlovanje na črno ne štejejo kratkotrajno delo, nujno delo, humanitarno delo, karitativno delo, delo za invalidske organizacije in prostovoljno ter dobrodelno delo. Za delo ali zaposlovanje na črno tudi ne šteje brezplačna pomoč na kmetijah, planinah in skupnih pašnikih ob sezonskih konicah.

Nadzor

Za nadzor na tem področju so odgovorni različni organi, predvsem pa:

- Inšpektorat Republike Slovenije za delo,
- Tržni inšpektorat Republike Slovenije,
- Carinska uprava Republike Slovenije,
- Davčna inšpekcija,
- Prometni inšpektorat Republike Slovenije,
- Policija.

Kazni

Globe za kršitev prepovedi dela na črno znašajo od 2.000 do 26.000 evrov za podjetje ali podjetnika in od 520 do 2.600 evrov za odgovorno osebo. Z globo od 1.000 do 7.000 evrov se za prekršek kaznuje posameznik, kadar opravlja dejavnost ali delo in ni vpisan ali nima priglašenega dela. Globe za omogočanje dela na črno znašajo od 2.600 do 15.600 evrov za delodajalca in od 420 do 1.600 evrov za odgovorno osebo. Posameznik, ki omogoča delo na črno, je lahko kaznovan z globo od 1.000 do 5.000 evrov. Globe za kršitev prepovedi zaposlovanja na črno znašajo od 5.000 do 26.000

evrov za delodajalca in od 500 do 2.500 evrov za odgovorno osebo ter od 500 do 2.500 evrov za posameznika, ki dela na črno. Za podjetje ali podjetnika, ki oglašuje delo ali dejavnost na črno, znaša globa od 1.600 do 15.600 evrov.

Ministrstvo za delo, družino, socialne zadeve in enake možnosti v svoji kampanji boja proti delu in zaposlovanju na črno omenja naslednja negativna dejstva, ki jih prinese delo na črno:

- nimate obveznega zdravstvenega zavarovanja;
- niste zavarovani za primer nezgode pri delu ali poklicne bolezni, zato ostanete brez zaposlitve in brez nadomestila v primeru nezmožnosti za delo;
- so pogoji, v katerih delate, nenadzorovani ter pogosto slabši in težji (izpostavljeni ste večji možnosti nesreč);
- večje tveganje za izgubo dela;
- ste brez zagotovila, da boste dejansko prejeli plačilo za opravljeno delo;
- ste brez pravice do odpravnine, letnega dopusta, regresa za letni dopust, regresa za prehrano, povrnitve potnih stroškov ipd.;
- niste upravičeni do nadomestila za primer brezposelnosti;
- se vam opravljeno delo ne všteva v delovno dobo in se ne bo upoštevalo za pokojnino (MDDSZ, 2014).

3.1.2 Konvencija o kibernetski kriminaliteti

Hkrati s hitrim razvojem informacijsko komunikacijskih tehnologij se razvijajo tudi nove oblike kibernetske kriminalitete. To pomeni velik problem pri oblikovanju ustrezne kazenske zakonodaje, saj le-ta težko sledi hitremu razvoju. Dodatna težava je tudi mednarodni vidik kibernetske kriminalitete, kibernetski prostor ponavadi ni omejen samo na eno državo, ravno nasprotno, kazniva dejanja, izvedena v kibernetskem prostoru se večinoma raztezajo preko mnogih držav, kar pripelje do problematike multi-jurisdikcije. Zaradi vseh naštetih lastnosti kibernetske kriminalitete je ključnega pomena sodelovanje institucij na vseh ravneh kazenskega pregona. Potrebno je ustvariti temelje, ki omogočajo nadaljnjo gradnjo mednarodnih odnosov.

Ravno to so v okviru Komiteja za probleme kriminalitete, ki je pod okriljem Sveta Evrope, pripravili strokovnjaki iz držav članic ter tudi predstavniki držav opazovalk – ZDA, Kanade, Južnoafriške republike in Japonske. 23. novembra 2001 je bila sprejeta Konvencija o kibernetski kriminaliteti. Gre za temelj evropskega sodelovanja na

področju kibernetske kriminalitete z opredelitvijo priporočil za preoblikovanje kazenskopravne zakonodaje podpisnic. Ključni cilj Konvencije je uskladitev nacionalnih kazenskopravnih zakonodaj podpisnic ter opredelitev enotnih kazensko procesnopravnih pooblastil, ki so potrebni za odkrivanje in pregon kibernetske kriminalitete. Izrednega pomena je tudi vzpostavitev mreže mednarodnega sodelovanja (Dimc in Dobovšek, 2012).

Konvencija o kibernetski kriminaliteti

Leta 2001 je Svet Evrope pripravil prvi mednarodni pravni akt, ki sodobno kibernetsko kriminaliteto obravnava z vidika priporočil, ki naj bi jih podpisnice upoštevale pri oblikovanju in reformi svojega notranjega prava. Ta pravni akt se imenuje Konvencija o kibernetski kriminaliteti. Konvencija zahteva spremembe v kazenskem materialnem in procesnem pravu, spremeniti ali dopolniti pa je treba tudi predpise, ki urejajo telekomunikacije. Konvencija določa splošen okvir mednarodnega sodelovanja preiskovalcev, saj, kot smo že večkrat omenili, kibernetski kriminal pogosto presega meje nacionalnih jurisdikcij.

Preambula

V preambuli konvencija določa svoj širši mednarodno pravni kontekst, v katerem se sklicuje predvsem na Konvencijo Sveta Evrope o varstvu človekovih pravic in temeljnih svoboščin iz leta 1950, Mednarodni pakt Združenih narodov o državljanskih in političnih pravicah iz leta 1966, Konvencijo Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov iz leta 1981, Konvencijo Združenih narodov o otrokovih pravicah iz leta 1989, Konvencijo Mednarodne organizacije dela o prepovedi najhujših oblik dela otrok in takojšnjem ukrepanju za njihovo odpravo iz leta 1999, obstoječe konvencije Sveta Evrope o sodelovanju na kaznovalnem področju, podobne obstoječe pogodbe med državami ter ne nazadnje na pravni red Evropske unije. Konvencija upošteva dosedanji mednarodno pravni okvir, ki ga dopolnjuje in ga v ničemer ne omejuje.

1. poglavje: Pomen izrazov

V tem delu konvencije najdemo definicije posameznih izrazov, ki jih uporablja konvencija, saj je enotno razumevanje uporabljenih pojmov za uspešno mednarodno sodelovanje in skupno kriminalitetno politiko zelo pomembno. Konvencija na dovolj

jasen način definira pojme: računalniški sistem, računalniški podatki, ponudniki storitev in podatki o prometu.

2. poglavje: Kazensko materialno in procesno pravo ter sodna pristojnost

Drugo poglavje je sestavljeno iz ukrepov, ki jih morajo sprejeti države podpisnice na državni ravni na področjih kazenskega materialnega prava, kazenskega procesnega prava in jurisdikcije.

Kazensko materialni del: Konvencija v tem delu opredeli kazniva dejanja kibernetske kriminalitete, ki jih razvrsti v štiri skupine glede na osnovne značilnosti.

- **Kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov:** kazniva dejanja protipravnega dostopa, kazniva dejanja protipravnega prestrezanja, kazniva dejanja motenja podatkov, kazniva dejanja motenja sistemov in kazniva dejanja zlorabe naprav.
- **Kazniva dejanja povezana z uporabo računalnikov:** kaznivo dejanje računalniškega ponarejanja in kaznivo dejanje računalniške goljufije.
- **Kazniva dejanja povezana z vsebino digitalnega zapisa:** kaznivo dejanje otroške pornografije in z njo povezana dejanja in kazniva dejanja, povezana s kršitvami avtorskih in sorodnih pravic.

V materialnem delu so zapisana tudi pravila za ugotavljanje odgovornosti udeležencev pri kaznivih dejanjih (poskus, pomoč, napeljevanje, odgovornost pravnih oseb) in kazenske sankcije.

Kazensko procesni del: V kazensko procesnem delu konvencija uvaja proceduralne ukrepe, ki so jih države podpisnice dolžne sprejeti in vključiti v svojo nacionalno zakonodajo. Glavni namen tega dela konvencije je v določbah, ki se osredotočajo na zavarovanje, preiskovanje in zaseg računalniških podatkov ter na opredelitev sodne pristojnosti. Zaradi izjemne dinamičnosti kibernetskega prostora in zaradi velike verjetnosti, da se podatki v strežniških datotekah, ki se avtomatsko generirajo in opisujejo, kaj se je v sistemu dogajalo (kdo, kaj kdaj, kako, od kod, kaj je počel ...), izgubijo, še preden se formalna preiskava začne, je nujno in racionalno, da se podatke zavaruje, saj lahko vsebujejo ključen dokaz o kriminalni aktivnosti. Organi pregona lahko od ponudnikov omrežnih storitev ali od skrbnikov sistemov z *odredbo za pripravo* zahtevajo, da izročijo zavarovane podatke in podatke o uporabnikih storitev za namen kazenske preiskave. V kazensko-procesnem delu najdemo tudi

pravila, ki urejajo pogoje ter način zasega podatkov, pogoje o zbiranju podatkov v realnem času ter pogoje glede prestrezanja vsebinskih podatkov.

Sodna pristojnost: V tem delu najdemo pravila o izključni sodni pristojnosti (na lastnem ozemlju, ladji, letalu ali nad svojim državljanom) in o odstopu od izključne pristojnosti v primeru, ko izročitev storilca ni možna. Zapisana so tudi pravila o prednosti nacionalnega prava pred mednarodnim pravom ter o posvetovalnem postopku v primeru multilateralne pristojnosti.

3. poglavje: Mednarodno sodelovanje

To poglavje opredeljuje glavna načela mednarodnega sodelovanja vseh podpisnic, vključena so tudi načela za izročitev, medsebojno pomoč in izmenjavo informacij. Konvencija zavezuje države podpisnice, da se njihovi organi pregona vključijo v mednarodno mrežo, ki se bo v primeru incidenta nemudoma odzvala, saj mora vsak člen delovati 24 ur na dan in 7 dni v tednu.

4. poglavje: Končne določbe

Konvencija v končnih določbah opredeljuje določbe o postopku podpisovanja konvencije, začetku njene veljavnosti, postopku naknadnega pristopa h konvenciji. Opredeljuje tudi določila o ozemeljski veljavnosti, o uveljavljanju in umikanju pridržkov. Določa tudi postopke glede spreminjanja konvencije, postopke reševanja sporov ter postopke posvetovanja pogodbenic, postopke odpovedi in postopke uradnega obveščanja (o podpisih, ratifikacijah, sprejetjih, odobritvah, pristopih ...) (Rupnik, 2002).

Protokol o rasizmu in ksenofobiji: Leta 2003 je bil sprejet protokol o rasizmu in ksenofobiji z namenom harmonizacije kazenskopravne zakonodaje na področju boja proti takšnim dejanjem na internetu. Sam protokol pa tudi pripomore k boljšemu mednarodnemu sodelovanju na tem področju. Poleg tega da definira kazniva dejanja rasizma in ksenofobije v kibernetskem okolju, postavlja tudi temelje materialnega in procesnega prava podpisnicam tega protokola. Vključuje pa tudi postopke mednarodnega sodelovanja (Dimc in Dobovšek, 2012).

Določbe o rasizmu in ksenofobiji bi bile zapisane v Konvenciji o kibernetski kriminaliteti, vendar pa zaradi nasprotovanja nekaterih držav, predvsem ZDA, ki zagovarjajo svobodo govora in izražanja, niso bile vključene v ta protokol, saj je bilo

pripravljalcem velikega pomena, da konvencijo podpišejo ZDA kot tehnološko in kibernetsko najbolj razvita država na svetu, zato je bil kasneje z novo skupino strokovnjakov pripravljen Protokol o boju proti rasizmu in ksenofobiji na računalniških sistemih (Rupnik).

Leta 2004 je Slovenija podpisala in ratificirala Konvencijo o kibernetski kriminaliteti ter tudi Protokol o boju proti rasizmu in ksenofobiji na računalniških sistemih (Dimc in Dobovšek, 2012).

4 Empirični del

V empiričnem delu bomo povzeli obsežno raziskavo o neformalni ekonomiji in kibernetski kriminaliteti na Kitajskem. Iz poročila Symantec pa bomo poskušali izluščiti najbolj uporabne podatke, ki nam bodo vsaj delno pomagali ugotoviti, kje na svetu je največ neformalne ekonomije v kibernetskem svetu ter s katerimi podatki se najpogosteje trguje, kakšne so cene ipd.

4.1 Neformalna ekonomija in kibernetska kriminaliteta na Kitajskem

Povzeli bomo obsežno raziskavo avtorjev Jianwei, Liang in Haixin iz Univerze v Kaliforniji, ki je bila objavljena leta 2012.

Kitajska je leta 2008 postala prva na svetu po številu internetnih uporabnikov, ta številka pa se iz dneva v dan povečuje z neverjetno hitrostjo. Decembra 2011 naj bi bilo na Kitajskem 513 milijonov uporabnikov interneta. Tako kot se povečuje število uporabnikov, se povečuje tudi število spletnih aplikacij, spletnih iger, spletnih trgovin ter načinov spletnega nakupovanja.

Sočasno z rastjo uporabnikov so se začele pojavljati varnostne grožnje. Kitajski uporabniki interneta so se začeli soočati s krajami računov za takojšnje sporočanje, z vdori v igralne račune. Povečali so se poskusi ribarjenja[8], posledično pa so se povečala prestrežena spletna plačila ter kraje spletnih bančnih računov.

Marca 2012 so kitajski novinarji razkrili, da so zaposleni v več bankah prodajali zaupne informacije o svojih strankah. Stranke so bile skupno oškodovane za okoli 3 milijone RBM oziroma za okoli 350.000 evrov. Taki primeri so v javnosti sprožili veliko zaskrbljenost ter povečali zavedanje, kako pomembno je varovanje zasebnih informacij.

V ozadju teh in podobnih internetnih groženj obstaja podzemna oziroma neformalna ekonomija kibernetske kriminalitete. Poganja jo misel lahkega zaslužka, kibernetski

[8] **Spletno ribarjenje** ali **phishing** je v računalništvu nezakonit način zavajanja uporabnikov, namenjenega pridobivanju tujih občutljivih osebnih podatkov. Pri takšnem zavajanju poskuša oseba, ki to izvaja, pridobiti podatke, npr. številke kreditnih kartic, gesla, podatke o računih ali druge osebne podatke tako, da pod pretvezo prepriča žrtev o potrebi po posredovanju teh podatkov. Prevare »phishing« uporabniki običajno prejmejo z neželeno e-pošto ali kot pojavna okna (Wikipedia).

kriminalci pa uporabljajo večje število tehnik, ki izkoristijo najmanjše napake pri zaščiti občutljivih informacij. Kibernetska neformalna ekonomija je hierarhično organizirana, vsak član pa ima točno določene naloge. Z nenehnim razvojem in rastjo neformalne kibernetske ekonomije so kibernetski kriminalci razvili večje število skritih trgov v temnih kotih interneta. Ti trgi kriminalu omogočijo prostor za trgovanje in komuniciranje. S povezovanjem neštetih komponent neformalne ekonomije v kibernetskem prostoru pa se zagotavlja logistična in operativna podporo.

Spletni goljufi uporabljajo prikrite načine za izvedbo različnih spletnih napadov z namenom čim večjega dobička. Kibernetska neformalna ekonomija je skoraj v celoti odvisna od interneta. Napadanje uporabnikov, pridobljene nedovoljene informacije, kraje ter transakcije in komunikacije – vse to je možno le z uporabo interneta. Torej internet kot celota zagotavlja platformo za delovanje kibernetske neformalne ekonomije.

Marsikdo bi si mislil, da je neformalna kibernetska tržnica skrita, vendar to ne drži. Gre za relativno odprto delovanje, saj na ta način lažje pridobijo nove člane, hkrati pa se krepi tudi učinkovitost. Člani kibernetske neformalne ekonomije uporabljajo značilen žargon, da se na ta način skrijejo pred javnostjo, saj uporabljajo javno dostopen internet. Kriminalni žargon in sama kultura, daje preiskovalcem možnost za preiskovanje nedovoljenih kibernetskih trgov. Vendar imajo tudi spletni kriminalci mnogo načinov, s pomočjo katerih se jim uspe izmikati roki pravice. To jim uspeva s pomočjo spletnih forumov, z uporabo lažnih identitet, s prikrivanjem IP-naslovov in s pomočjo drugih metod.

Čeprav je to globalni problem, je kibernetska neformalna ekonomija na Kitajskem posebna v več primerih. Poseben je kitajski jezik, drugačna sta njihova ekonomija in pravni sistem, drugače delujejo nadzorni organi, navsezadnje je drugačna tudi njihova internetna kultura v primerjavi z zahodnim svetom. Podrobna raziskava kitajskega spletnega podzemlja bo močno pripomogla h globalnemu razumevanju kibernetske neformalne ekonomije. Pred raziskavo Univerze v Kaliforniji kitajsko spletno podzemlje še ni bilo podrobno raziskano.

Temelječ na raziskavi, so raziskovalci kitajsko kibernetsko neformalno ekonomijo razmejili na štiri dele, in sicer:

- Kraja realnega premoženja: kraja denarja iz ukradenih bančnih računov ali kreditnih kartic.
- Kraja virtualnega premoženja: kraja virtualnih valut iz igralnih računov ter prodaja le teh za pravi denar.

- Zloraba interneta in njegovega delovanja: gre za vdore v spletne strani, serverje, pametne telefone itd. z namenom čim večjega zaslužka.
- Blackhat hekerji[9]: prodaja trojanskih konjev in orodij za napade ter s tem zagotavljanje tehnične podpore kiberkriminalcem, učenje novincev.

Vsi štirje deli se med seboj dopolnjujejo. Blackhat hekerji zagotavljajo ekonomsko bazo in tehnično podporo za ostale tri dele verige. Del, ki je zadolžen za vdore v sisteme, pa pripravi vse potrebno, da lahko ostala dva dela kradeta pravi in virtualni denar. Treba je poudariti, da so vsi, ki sodelujejo pri kibernetski neformalni ekonomiji, zmožni tudi na dovoljen način zaslužiti dovolj denarja za preživetje. Glavni pogon vseh štirih delov je seveda ogromen zaslužek, ki tudi poganja nadaljnji razvoj ter širjenje kibernetske neformalne ekonomije.

Kraja realnega premoženja

Del verige kibernetske neformalne ekonomije, ki se ukvarja s krajo pravega premoženja, največkrat poseže po spletnih bančnih računih, kreditnih karticah, plačilnih računih itd. Glede na to, da večina teh in podobnih računov potrebuje geslo za prijavo, sta številka bančnega računa ter geslo prvi tarči spletnih kriminalcev.

Kitajski kiberkriminalci ponavadi uporabljajo dve tehniki, s pomočjo katerih pridobijo želene informacije (številke bančnih računov in gesla), in sicer s pomočjo ribarjenja[10] in uporabo trojanskih konjev. Pri ribarjenju gre za uporabo socialnega inženiringa in uporabo tehnike, ponavadi gre za uporabo lažnega e-poštnega sporočila, ki je poslan z namenom pretentati uporabnika. Trojanski konj pa je škodljivi program, ki je ustvarjen z namenom, da na uporabnikovem računalniku ukrade uporabne informacije, kot so gesla, številke bančnih računov ipd. Poleg teh dveh tehnik se kriminalci poslužujejo tudi goljufij preko telefona, skeniranja bančnih kartic in podobnih tehnik, s pomočjo katerih ravno tako pridobijo želene informacije. Te tehnike se izvajajo izven interneta, vendar so ravno tako podprte s strani neformalne kibernetske kriminalitete.

[9] Black hat – sinonim za hekerja, ki odkrite pomanjkljivosti ne posreduje javnosti, temveč jih zadrži zase in uporablja za vdore v sisteme ali proda na črnem trgu.
[10] Spletno ribarjenje ali phishing je v računalništvu nezakonit način zavajanja uporabnikov, namenjenega pridobivanju tujih občutljivih osebnih podatkov. Pri takšnem zavajanju poskuša oseba, ki to izvaja, pridobiti podatke, npr. številke kreditnih kartic, gesla, podatke o računih ali druge osebne podatke tako, da pod pretvezo prepriča žrtev o potrebi po posredovanju teh podatkov. Prevare »phishing« uporabniki običajno prejmejo z neželeno e-pošto ali kot pojavna okna.

Ko kiberkriminalci pridobijo številke računov in gesla, nadaljujejo s fazo pranja denarja. Ponavadi obstajata dve možnosti. Prva je, da pridobljene podatke prodajo na neformalni tržnici, druga pa je ta, da poskušajo s temi podatki pridobiti sredstva z računov žrtev. Da se izognejo organom pregona, si ustvarijo bančni račun z lažnimi osebnimi podatki. Denar iz bančnega računa žrtve prenesejo na svoj lažni bančni račun, preneseni denar pa dvignejo na bančnem avtomatu ali pa opravijo nakup z lažno kartico na prodajnem mestu (POS-terminalu).

Vloge in žargonski izrazi pri kraji realnega premoženja

Številke bančnih računov se v žargonu imenujejo »pripomočki« (liao, 料), gesla in ostali kriptirani podatki pa se imenujejo »sledilni pripomočki« (gui dao liao, 轨道料) oziroma poenostavljeno »sled« (gui dao, 轨道). Kriminalec, ki se ukvarja s krajo in prodajo ukradenih podatkov na neformalni tržnici kibernetske kriminalitete, se imenuje »mojster pripomočkov« (liaozhu, 料主).

Faza pranja denarja se imenuje »umivanje pripomočkov« (xi liao, 洗料), oseba, ki opravlja to dejavnost, pa se imenuje »čistilec pripomočkov« (xi liao ren, 洗料人). Faza ustvarjanja lažnega bančnega računa ter dvigovanja denarja na bančnih avtomatih oziroma plačevanja na POS-terminalih se imenuje »razpakiranje tovora« (shua huo, 刷货). Vodja skupine se imenuje »mojster prevoza« (che zhu, 车主), oseba, ki pa dviga denar na bančnih avtomatih, pa se imenuje »voznik« (che shou, 车手).

Kraja virtualnega premoženja

Na Kitajskem je v zadnjem desetletju prišlo do velikega razvoja video igric in spletne zabavne industrije. Večina popularnih spletnih iger ali zabavnih aplikacij je uvedlo virtualno valuto in članstvo ter na ta način izboljšalo igralno izkušnjo in povečalo dobičke. Igralci morajo plačati s pravim denarjem ali pa vložiti veliko časa, da si pridobijo virtualna sredstva. Ta virtualna sredstva je možno tudi prodati za pravi denar, torej če gledamo iz tega vidika, imajo virtualna sredstva realno vrednost.

Ker pa je kitajska zakonodaja za zaščito virtualnega premoženja še v začetni fazi, poleg tega pa je težko meriti realno vrednost virtualnega premoženja, to izkoriščajo kibernetski kriminalci, ki se zavedajo pomanjkljive zakonodaje ter na ta način izvršujejo kazniva dejanja z veliko manjšim tveganjem kot pri kraji realnega premoženja.

Kraja virtualnega premoženja ponavadi poteka v treh fazah. V prvi fazi kriminalci s pomočjo ribarjenja ali trojanskih konjev pridobijo uporabniška imena in gesla. V drugi fazi se prijavijo v račune s pomočjo ukradenih uporabniških imen in gesel ter na ta način ukradejo virtualno premoženje. V zadnji fazi pa pride do prodaje virtualnega premoženja za pravi denar ostalim spletnim igralcem.

Vloge in žargonski izrazi pri kraji virtualnega premoženja

Pri kraji virtualnega premoženja se ukradena uporabniška imena in gesla v žargonu imenujejo »kuverta« (xin feng, 信封) ali »poštni nabiralnik« (youxiang, 邮箱). Spletne aplikacije, ki pridobivajo »kuverte«, se imenujejo »škatla« (xiangzi, 箱子). Tisti, ki ustvari trojanskega konja, se imenuje »trojanski pisatelj« (muma zuozhe, 木马作者) ali »trojanski agent« (muma daili, 木马代理), medtem ko se tisti, ki izvajajo kraje uporabniških imen in gesel, imenujejo »prevzemniki trojancev« (baoma ren, 包马人). Ko je »kuverta« ukradena, se jo ponavadi proda »pralcu kuvert« (xixin ren, 洗信人), ki se ročno ali s pomočjo avtomatskih orodij prijavi v spletne račune, z namenom kraje sredstev ali z namenom pridobitve nadzora nad vrednimi računi. Ukradeno virtualno premoženje se nato proda »programskim prodajalcem« (baoxiao shang, 包销商), ki preko dovoljenih poti prodajo virtualno premoženje igralcem za pravi denar.

Zloraba interneta in njegovega delovanja

Zloraba interneta in njegovega delovanja se je razvila postopoma, zaradi splošnega pomanjkanja nadzora. Najbolj popularna sredstva na internetu so prostor za shranjevanje podatkov, IP-naslov, mrežni promet, občutljivi podatki itd. Več tovrstnih sredstev kot jih ima nekdo v svoji lasti, večjo moč ima. Kibernetski kriminalci ta sredstva zlorabljajo, posledično imajo večjo moč na neformalnem trgu kibernetske kriminalitete.

Trenutno najbolj popularna tehnologija za nadzor večjega števila računalnikov se imenuje botnet. Gre za omrežje okuženih računalnikov (zombijev), ki omogočajo tistemu, ki ima nadzor nad njimi, močan napad na želeno tarčo. Večina računalnikov se okuži preko škodljive e-pošte, velikokrat pa so povezani s trojanskimi konji.

Druga metoda, ki jo uporabljajo za nadzor večjega števila računalnikov, je preko programov, s pomočjo katerih uporabniki upajo da bodo zaslužili nekaj denarja preko interneta. Pri tej metodi se uporabniki strinjajo, da bo njihov računalnik v uporabi,

medtem ko ga sami ne bodo uporabljali. V bistvu gre vse skupaj za zelo razvejan in dobičkonosen marketing, ki pa uporabnikom plača minimalno vsoto denarja, le zato, da so pripravljeni sodelovati.

Serverji imajo veliko komercialno vrednost. Več kot ima neka spletna stran ogledov in klikov, več denarja lahko iztrži njen lastnik za oglaševanje. Tega se zavedajo tudi spletni kriminalci, ki poskušajo pridobiti te podatke z vdiranjem v spletne strani ali pa jih enostavno kupijo na neformalni spletni tržnici. Poleg prej opisanih podatkov se zlorablja tudi občutljive podatke na samem serverju.

Zadnja leta se podobne škodljive kode, ki so se in se še vedno pojavljajo na računalnikih, zdaj pojavljajo na pametnih telefonih. Verjetno gre za še večjo nevarnost, saj telefoni ponavadi vsebujejo več občutljivih podatkov kot računalniki.

Pri uporabnikih, okuženih z botnetom, obstaja velika nevarnost, da se uporabniku namesti še programe za ribarjenje, kot je recimo bančni trojanski konj, za izvedbo kraje pravega denarja, lahko pa se namesti igralni trojanski konj, ki krade virtualno premoženje. Okužene računalnike in serverje se lahko uporabi za pošiljanje nezaželene pošte, za izvajanje DDos napadov, za izsiljevanje, za goljufije pri številu klikov in ogledov strani, za krajo zasebnih informacij in za mnogo drugih nedovoljenih ali manipulativnih dejavnosti.

Pri okuženih pametnih telefonih so možnosti zlorabe zelo podobne, gre za pošiljanje nezaželenih SMS- in MMS-sporočil, zlorabo zasebnih informacij, večji pa je lahko tudi račun za plačilo mobilnih storitev zaradi nenadzorovane uporabe telefona.

Blackhat hekerji

Blackhat hekerji imajo močan vpliv na nastanek in razvoj neformalne kibernetske kriminalitete. Prisotni so praktično v vseh vidikih, zato so motor, ki poganja neformalno kibernetsko kriminaliteto.

Blackhat hekerji ponujajo svoje znanje na dva načina. Prvi način je s ponudbo produktov, kar pomeni, da odkrijejo programske napake ali pa ustvarijo škodljivo programsko opremo ter nato prodajo te produkte ostalim trem stebrom neformalne kibernetske kriminalitete. Brez teh produktov ostali kiberkriminalci, ki nimajo toliko znanja, nimajo možnosti se ukvarjati s kibernetskim kriminalom. Drugi način podajanja svojega znanja pa je s storitvami. Lahko kot način začasne zaposlitve, da deluje po navodilu delodajalca, ali kot učitelj novih članov, ki potrebujejo uvajanje. Torej blackhat hekerji so tisti, ki usposabljajo »nove moči« v podzemnem svetu kibernetskega kriminala.

Vloge in žargonski izrazi pri blackhat hekerjih

V žargonu se aktivnosti blackhat hekerjev imenujejo »hekerske naloge« (heike renwu, 黑客任务). Blackhat hekerji, ki ponujajo učenje blackhat tehnik, to oglašujejo kot »iskanje vajenca« (shoutu, 收徒), na drugi strani pa novi člani, ki se želijo naučiti blackhat tehnik, uporabijo žargonski izraz »iskanje mojstra« (baishi, 拜师). Izraz »trojanski konj« (muma, 木马) se ponavadi uporablja za trojanski virus, ki krade prijavne podatke za spletno bančništvo, plačila, spletne igre ter za ostale spletne strani. Blackhat heker, ki ustvari trojanski virus, se imenuje »trojanski pisatelj« (muma zuozhe, 木马作者). Poleg trojanskih konjev, ustvarijo tudi zaščito za trojanske konje, ki preprečijo, da bi se jih odkrilo s pomočjo antivirusnih programov. Žargonsko se te zaščite imenujejo »izogibanje odkritju« (miansha, 免杀). »Nič-dan« se imenuje napad na novo odkrito sistemsko napako, še preden je bil izdan popravek za to napako. Tovrstni napadi so postali zelo dobro tržno blago na neformalni kibernetski tržnici, saj so izredno močni in zanesljivi.

4.1.1 Statistika neformalne ekonomije in kibernetske kriminalitete na Kitajskem

Glede na pretekle raziskave so Jianwei, Liang in Haixin izvedli statistično analizo vseh delov neformalne kibernetske ekonomije ter naredili skupno oceno, ki jo je povzročila ta vrsta kriminala v letu 2011 na Kitajskem. Rezultati so povzeti v tabeli 1.

V letu 2011 je bil vsak dvanajsti uporabnik interneta na Kitajskem ogrožen zaradi spletne goljufije ali kraje realnega premoženja. To pomeni skoraj 40 milijonov uporabnikov, ki so se soočili z grožnjo. Od teh jih je več kot pol milijona bilo dejansko oškodovanih, kot kaže tabela 1.

Glede na to, da je virtualno premoženje bistveno slabše zaščiteno z zakonodajo, so virtualne valute toliko bolj na udaru kriminalcev. V letu 2011 je bilo oškodovanih skoraj 4 milijone igralcev, povzročena škoda pa je presegla 200 milijonov ameriških dolarjev, kar predstavlja več kot 3 % celotnega virtualnega trga.

Glede na raziskavo iz leta 2011 naj bi bilo več kot 60 milijonov uporabnikov oškodovanih zaradi zlorab spletnih strani, zlorab okuženih mobilnih telefonov ipd. Od teh 60 milijonov oškodovanih uporabnikov je bilo skoraj 50 milijonov uporabnikov z okuženimi pametnimi telefoni. Pri okuženem telefonu lahko pride do nenadzorovane porabe, nenadzorovanega pošiljanja SMS-/MMS-sporočil, do kraje zasebnih informacij

... Ocenjena škoda zaradi zlorab interneta in njegovega delovanja dosega skoraj 300 milijonov ameriških dolarjev.

Tabela 1: Delna ocena škode, ki jo je povzročila neformalna ekonomija kibernetske kriminalitete v letu 2011 (vir: Jianwei, Liang in Haixin, 2012).

	Najbolj uporabljena goljufija	**Oškodovana populacija (v milijonih)**	**Ocenjena škoda (v milijonih ameriških dolarjev)**
Kraja realnega premoženja	Kraje in goljufije pri spletnem bančništvu in pri spletnih plačilih	0,54	329
Kraja virtualnega premoženja	Kraja igralnega virtualnega premoženja	3,84	225
Zloraba interneta in njegovega delovanja	Zloraba spletnih strani, zloraba okuženih mobilnih telefonov ...	60,42	298

Blackhat tehnike, orodja ter učenje novincev ne prinesejo direktne škode internetnim uporabnikom. So pa osnova ostalim trem stebrom neformalne kibernetske ekonomije, saj zagotavljajo vse potrebne stvari, da lahko kibernetski kriminalci uspešno delujejo. Težko je predvidevati in še težje izmeriti dejansko škodo, ki jo povzročijo blackhat hekerji. Znano je, da blackhat hekerji odkrivajo in prodajajo sveže odkrite sistemske napake (žargonsko se imenuje »nič dan«), vendar razen tega, da so te informacije zelo zaželene na trgu kibernetske kriminalitete, ter tega, da imajo visoko ceno, ni veliko znanega. Zato je tudi težko meriti, kakšno škodo povzročijo blackhat hekerji.

Skupna ocenjena škoda Kitajske neformalne ekonomije kibernetske kriminalitete presega 852 milijonov ameriških dolarjev. Kljub vse večjemu zavedanju ter zaščiti uporabnikov na spletu je še vedno več kot 100 milijonov ali več kot 20 % vseh internetnih uporabnikov na Kitajskem ogroženih s strani kibernetske kriminalitete.

Neformalni trg kibernetske kriminalitete zaposluje veliko število ljudi. Njihovi letni prihodki so ogromni. Po nekaterih ocenah so letni prihodki podobni največjim Kitajskim internetnim podjetjem, kot sta na primer Baidu in Alibaba Group.

4.2 Poročilo Symantec glede neformalne ekonomije v kibernetskem svetu

Uvod

Poročilo Symantec o »podzemni ekonomiji« je raziskava o kibernetskem kriminalu in neformalni ekonomiji. Vključuje diskusijo o najbolj znanih skupinah, ki delujejo v tem okolju, razišče tudi največje oglaševalce ter najbolj popularne dobrine ter storitve na trgu. Vključuje tudi pregled strežnikov in kanalov, ki so bili prepoznani kot gostitelji za trgovanje. To poročilo je namenjeno analizi določenih vidikov neformalne ekonomije v kibernetskem svetu, ne zavzema pa celotnega kibernetskega kriminala. Symantec je opazoval strežnike, ki so bili prepoznani kot orodja za trgovanje med prvim julijem 2007 in tridesetim junijem 2008. Iz tega poročila bomo poskusili izluščiti najbolj pomembne ter najbolj zanimive podatke, s pomočjo katerih si bomo še izboljšali pogled na izbrano tematiko.

Symantec definira kibernetski kriminal kot katerikoli zločin, ki je storjen z uporabo računalnika, omrežja ali strojne opreme. Računalnik ali naprava sta lahko sredstvo za izvedbo kaznivega dejanja, posrednik pri kaznivem dejanju ali tarča kaznivega dejanja. Kibernetski kriminal lahko poteka na računalniku samem ali na drugih lokacijah. Dve najbolj pogosti platformi za udeležence v kibernetski neformalni ekonomiji so IRC-kanali in spletni forumi. Oboje predstavlja pogovorne skupine, ki jih udeleženci uporabljajo za nakup in prodajo nedovoljenih dobrin in storitev. Med prodane predmete in storitve spadajo podatki o kreditnih karticah, podatki o bančnih računih, e-poštni računi in vse ostalo, kar se da izkoristiti za profit. Storitve lahko vsebujejo prenos sredstev iz ukradenih računov v pravo valuto, lahko vsebujejo ribarjenje (phishing), gostovanje na ponarejenih straneh, obstaja tudi možnost oglaševanja, s pomočjo katerega kibernetski kriminalci izpostavijo svoje storitve.

4.2.1 Spletni forumi

Spletni forumi so priljubljeni načini trgovanja z ukradenimi informacijami. Eden od razlogov za priljubljenost je ta, da so objavljene ponudbe vidne vsem obiskovalcem foruma, dokler niso odstranjene. Večina forumov je kronološko organiziranih, kar olajša iskanje, forumu pa se lahko pridruži praktično kdorkoli, ponavadi je dovolj samo registracija z uporabniškim imenom. Nekateri forumi takoj dovolijo

novopridruženim članom, da objavijo svoje ponudbe oziroma stopijo v kontakt z ostalimi člani. Nekateri forumi pa imajo različne stopnje članstva, kar pomeni, da se morajo novi člani najprej izkazati, da lahko pridobijo enakovredne pravice. Novi člani morajo na več forumih najprej prestati obdobje ocenjevanja, preden lahko začnejo aktivno sodelovati. Da si vzpostavijo ugled ter se izkažejo, morajo potencialni prodajalci najprej zagotoviti vzorce svojih dobrin, da se jih preizkusi in potrdi. Veliko forumov poleg osnovnih stvari, ki jih lahko ponudi forum, ponujajo tudi razne vaje, navodila, kako narediti določeno stvar in podobne ugodnosti za člane (Symantec, 2008).

4.2.2 IRC-kanali

Kanali na IRC-strežnikih se prav tako uporabljajo za oglaševanje in promet ukradenih informacij ter za lajšanje ilegalnih aktivnosti. IRC je internetni komunikacijski protokol z velikim številom uporabnih vidikov za tiste, ki sodelujejo v »podzemnem« svetu kibernetske kriminalitete. Ponuja skupinske pogovore, zahteva majhno pasovno širino, programska oprema pa je brezplačno dostopna na vseh operacijskih sistemih.

Več IRC-strežnikov se lahko poveže ter tako ustvari večje omrežje. Obstaja zelo velik razpon v velikosti IRC-strežnikov ter številom kanalov na teh strežnikih. Symantec je v času raziskave preučeval IRC-strežnike, ki so imeli samo pet kanalov, kot tudi IRC-strežnike z več kot 28.000 kanali.

Uporabniki se lahko povežejo z IRC-strežnikom s pomočjo več brezplačnih programov. Podobno kot pri spletnih forumih uporabniki potrebujejo samo unikatno uporabniško ime, da se pridružijo kanalu, čeprav imajo določeni kanali omejitve, kot je recimo ta, da mora biti uporabnik povabljen s strani že obstoječega uporabnika ali pa odobren s strani administratorja.

Potencialni kupci zasebno kontaktirajo prodajalca ter se pogajajo za končno ceno ter način plačila. Prodajalec ponavadi pošlje storitve ali dobrine kupcu, potem ko prejme plačilo. Načinov plačila je več, najpogosteje pa se plačilo za storitve ali dobrine izvede s spletno valuto.

Udeleženci te »podzemne« ekonomije večinoma sami nadzorujejo dogajanje na strežnikih. Prijavljajo prevarante administratorju IRC-strežnika ter opozorijo tudi ostale o neprimernem vedenju. Na veliko strežnikih so administratorji ustvarili prav posebno stran, kamor se zapisuje prevarante, ki se je bolje izogniti. Uporabnike, ki večkrat kršijo pravila, se lahko odstrani iz strežnika (Symantec, 2008).

4.2.3 Dobrine in storitve

Symantec je med 1. julijem 2007 in 30. junijem 2008 raziskoval, katere nedovoljene dobrine in storitve se najbolje prodajajo na »podzemnih« strežnikih. Ugotovitve so razdelili na dva dela, in sicer na ponudbo in povpraševanje ter na škodljiva orodja.

Ponudba in povpraševanje

Neformalna ekonomija kibernetskega sveta je dozorela v pravi globalni trg, ki se srečuje z istimi pritiski glede ponudbe, povpraševanja in odzivnosti, kot katerakoli druga ekonomija. Obstaja ogromno kanalov, namenjenih oglaševanju dobrin in storitev. Možnost oglaševanja se zelo veliko uporablja, saj je kot na drugih trgih velika konkurenca, zato se hoče vsak najbolje izpostaviti in prikazati v najboljši luči. Veliko oglasov je tudi iz strani kupcev, ki izrazijo zahtevo po nečem, kar potrebujejo. Kot v ostalem oglaševanju, so tudi tukaj sporočila obogatena s privabljajočimi besedami, kot so na primer »sveže«, »neškodljivo« in »visoko uravnoteženo«. Tipična vsebina oglasa vsebuje storitev ali dobrino, cenovni razred, sprejemljive načine plačila ter kontaktne podatke.

Za namen tega poročila se je ponudbo in povpraševanje še nadalje razdelilo na naslednje štiri teme:

- **Dobrine in storitve oglaševane po kategoriji**

Symantec je razvrstil dobrine in storitve, ki so oglaševane na »podzemnih« strežnikih v kategorije (kot so npr. informacije o kreditnih karticah, bančnih računih ...). Merjenje po kategorijah nam omogoči vpogled v vzorce ponudbe in povpraševanja »podzemne » ekonomije.

Pri dobrinah in storitvah, ki so oglaševane po kategoriji, se je največkrat oglaševalo informacije o kreditnih karticah, in sicer kar 31 % od vsega oglaševanega, prav tako pa je bilo tudi povpraševanje najbolj pogosto po tej kategoriji (tabela 1). V to kategorijo spadajo številke kreditnih kartic, kreditne kartice s CVV2[11] številkami in kopije magnetnega zapisa kreditnih kartic.

[11] CVV2/CVC2 je trimestna varnostna šifra, odtisnjena na zadnji strani kreditne kartice (MasterCard, Visa, Diners club) in se na zadnji strani kartice lahko nahaja na podpisnem traku ali poleg njega. CVV/CVC številke pri Maestro karticah ni. Z uporabo CVV2 in CVC2 kode se doseže večja varnost transakcije in prepreči ilegalno uporabo številke kartice.

Tabela 2: Dobrine in storitve, oglaševane po kategoriji (vir: Symantec)

Rangiranje ponudb	Rangiranje Povpraševanja	Kategorija	Ponudba v %	Povpraševanje v %
1	1	Informacije o kreditnih karticah (Credit card information)	31	24
2	3	Finančni računi (financial accounts)	20	18
3	2	Informacije o ribarjenju in nezaželeni pošti (Spam and phishing information)	19	21
4	4	Storitve onemogočanja (Withdrawal service)	7	13
5	5	Kraja identitete (Identity theft information)	7	10
6	7	Računi strežnikov (Server accounts)	5	4
7	6	Okuženi računalniki (Compromised computers)	4	4
8	9	Spletni računi (Website accounts)	3	2
9	8	Škodljive aplikacije (Malicious applications)	2	2
10	10	(Retail accounts)	1	1

Eden od razlogov, zakaj je trgovanje z informacijami o kreditnih karticah tako pogosto, je ta, da obstaja veliko različnih načinov (ribarjenje, kopiranje magnetnega zapisa kartice, vdori v baze s podatki ...), s katerimi se lahko pridobi in uporabi informacije. Drugi razlog je pogosta uporaba kreditnih kartic, ki se vsako leto povečuje, in sicer za skoraj 8 procentov na leto. Če torej oba razloga združimo, dobimo zelo veliko frekvenco uporabe ter veliko načinov, s katerimi lahko pridobimo občutljive informacije, kar pripelje do velike zaloge teh informacij na »podzemnih« strežnikih.

Razlog za tako veliko povpraševanje po informacijah o kreditnih karticah pa se skriva v tem, da je uporaba le-teh dokaj enostavna za uporabo pri aktivnosti, kot je na

primer spletno nakupovanje. Spletno nakupovanje je zelo enostavno in hitro, za nakup pa ponavadi potrebujemo le informacije o kreditni kartici. Nekdo z dovolj znanja bi torej lahko opravil veliko transakcij z ukradeno kartico, preden bi bile te transakcije zaznane in bi banka posledično blokirala kartico. Do končnega zaslužka kupcu manjka samo še to, da prejeti predmet proda ter na ta način pride do denarja.

Tisti, ki zlorablja informacije o kreditnih karticah, poskuša biti čim manj sumljiv pri svojem početju in na ta način maksimalno izkoristiti kreditno kartico, oziroma povedano drugače, pridobiti čim več denarja, preden kartico blokirajo. To pa zato, ker izdajatelj kartice stalno nadzoruje transakcije svojih klientov ter išče nenavadne vzorce, lokacije in/ali vsote kot del njihove varnostne prakse. Na primer, pri transakcijah, kjer je kartica fizično prisotna, bi bilo zelo sumljivo, če bi se zaporedne transakcije zgodile na različnih koncih sveta. V takem primeru bi se sprožil alarm, ki bi privedel do blokiranja kartice s strani izdajatelja. Težje je nadzorovati spletne trgovine, ki nimajo geografskih meja, zato lahko različni ljudje z isto kreditno kartico izvedejo več nakupov na različnih lokacijah z manjšo verjetnostjo po hitrem odkritju.

Poleg informacij o kreditnih karticah se prodajajo tudi dostavna mesta, kamor se lahko naroči kupljene predmete v spletnih trgovinah ter na ta način zavarovati svojo identiteto. Izdajatelju kreditne kartice naslovi za dostavo, ki se ne ujemajo z naslovom kreditne kartice ne bodo takoj postali sumljivi, še posebej ne na vrhuncih prodajne sezone, kot je recimo božični čas in je dokaj pogosto, da se pošilja darila na tuje naslove, ponavadi celo na stroške spletne trgovine. Ti faktorji otežijo izdajatelju kartice nadzor nad samo kreditno kartico. Zaradi naštetih težav je goljufija ugotovljena šele takrat, ko je blago že plačano in odposlano.

Še eden od faktorjev, da je tako veliko povpraševanje po informacijah o kreditnih karticah, je, da se pogosto prodajajo v večjih količinah kot paketi. Ponavadi se dobi tudi popust ob večjem naročilu, to pa pomeni, da lahko kupec dobi več še neblokiranih kreditnih kartic po nižji ceni.

Drugo najbolj pogosto oglaševano med dobrinami in storitvami po kategorijah so finančni računi z 20 odstotki (tabela 1). V to kategorijo spadajo podatki o bančnih računih, naprave za skeniranje magnetnih zapisov kartic, storitve spletnega plačevanja, računi spletnih valut in spletni računi za trgovanje z delnicami. Ta kategorija je bila z 18 odstotki tretja po povpraševanju. Daleč najbolj pogosto pa je bilo oglaševanje o podatkih bančnih računov, in sicer kar 18 odstotkov od celotnih 20 odstotkov oglaševanja.

Finančni računi so zanimive tarče zaradi tega, ker se da pridobiti denar direktno in ne tako kot pri zlorabi kreditnih kartic, kjer je potrebno kupljen predmet najprej prodati, da se pridobi denarno korist.

V veliko bankah je dvig denarja možen samo v isti državi, kjer je matična banka. Zaradi tega se morajo goljufi znajti na razne načine. Eden od načinov je tudi ta, da najamejo nekoga iz države, kjer je matična banka, ta pa namesto njih dvigne denar s pomočjo ponarejenih dokumentov. Symantec je zaznal tudi dokaj veliko povpraševanje po ljudeh iz točno določene države ter tudi točno določenega spola, da bi na ta način bilo vse skupaj manj sumljivo.

Čeprav je postopek, da goljufi pridejo do denarja pri bančnih računih, mnogo daljši kot pri kreditnih karticah, pa je končni izplen ponavadi mnogo večji. Med raziskavo je bilo ugotovljeno, da je bila povprečna vrednost bančnega računa skoraj 40.000 dolarjev, kar je mnogo več v primerjavi s kreditnimi karticami, ki so v povprečju bile vredne okoli 4000 dolarjev.

Na tretjem mestu oglaševanih dobrin in storitev po kategoriji sta se znašla ribarjenje in nezaželena pošta z 19 odstotki. V to kategorijo spadajo e-poštni naslovi, e-poštna gesla, prevare in pošiljanje nezaželene pošte. Ta kategorija je bila po povpraševanju celo na drugem mestu s kar 21 odstotki. Nezaželena pošta lahko predstavlja veliko nevarnost, saj je z njeno pomočjo možno dostaviti škodljive programske kode ter poskuse ribarjenja. Ribarjenje se uporablja za pridobitev finančnih koristi ali zasebnih podatkov na način, da se ljudi preslepi s pomočjo oponašanja zaupanja vredne strani. S pomočjo ribarjenja se najpogosteje poskuša pridobiti informacije o kreditnih karticah ter podatke o bančnih računih.

Veliko različnih dobrin in storitev je oglaševanih na »podzemnih« ekonomskih strežnikih. Skupek vseh je dovolj obsežen, da tvori samovzdržujočo ekonomijo. Nezaželena pošta in ribarjenje sta zelo učinkovita pri zbiranju informacij o kreditnih karticah ter o bančnih računih. Prodajanje teh informacij ter tudi direktno pridobivanje finančnih koristi je že dovolj za začetek gradnje »podzemne« ekonomije. Dobički iz tega naslova pa se z lahkoto uporabijo za nadaljnja kazniva dejanja, na primer za najem ljudi z dobrim računalniškim znanjem, ki znajo razviti nova orodja za nadaljnje napade. Lahko pa se ta orodja tudi kupi brez najema programerjev.

S pomočjo ribarjenja lahko kibernetski kriminalci pridobijo tudi naše uporabniško ime in geslo e-pošte. To znajo uporabiti za več različnih kaznivih dejanj. Lahko se preko te e-pošte pošilja nezaželeno pošto vsem kontaktom te osebe. Nekateri uporabniki ob

odprtju e-poštnega računa pridobijo tudi spletni prostor kot brezplačno ugodnost. Ta prostor je redko izkoriščen, zato pa ga z veseljem izkoristijo kibernetski kriminalci, ki lahko ta prostor uporabijo za namene ribarjenja ali širjenja zlonamerne programske kode, brez da bi se lastnik poštnega računa zavedal. Velik problem, da ima nekdo nadzor nad našim e-poštnim naslovom, je tudi naslednji. Velika večina omrežnih storitev od nas zahteva registracijo, kjer si izberemo uporabniško ime (lahko tudi kar e-poštni naslov) in določimo geslo za dostop do storitve. V primeru, da se geslo pozabi, spletno mesto na naš e-poštni naslov pošlje spletno povezavo za nastavitev novega gesla. To pomeni, da kdor ima dostop do našega e-poštnega predala, lahko dostopa tudi do ostalih naših računov (socialna omrežja ...), ki smo jih povezali s tem poštnim računom.

- **Dobrine in storitve oglaševane glede na predmet**

V tem delu se je Symantec pri svoji raziskavi posvetil razvrstitvi najbolj oglaševanih in najbolj zaželenih dobrin in storitev v »podzemni ekonomiji« glede na predmet.

Najbolj pogosto (z 18 odstotki) so se v času raziskave oglaševali podatki o bančnih računih (številke računa in podatki za dokazovanje avtentičnosti) (tabela 2). Podatki o bančnih računih so bili tudi najbolj zaželeni (14 odstotkov).

Veliko zalogo podatkov o bančnih računih lahko razložimo z vedno večjo uporabo spletnega bančništva. V ZDA je v času raziskave kar 44 odstotkov internetnih uporabnikov že uporabljalo spletno bančništvo, še več pa v Kanadi, kjer se je že kar 67 odstotkov internetnih uporabnikov soočilo s spletnim bančništvom. Tolikšnemu številu uporabnikov seveda sledijo tudi poskusi napadov na spletne bančne račune.

Tabela 3: Dobrine in storitve oglaševane po predmetu (vir: Symantec)

Rangiranje ponudb	Rangiranje Povpraševanja	Dobrine in storitve	Ponudba v %	Povpraševanje v %	Razpon v cenah v $
1	1	Podatki o bančnih računih	18	14	10–1000
2	2	Kreditne kartice s CVV2 številkami	16	13	0.50–25
3	5	Kreditne kartice	13	8	0.10–25
4	6	E-poštni naslovi	6	7	0.30/MB-40/MB
5	14	E-poštna gesla	6	2	4–30
6	3	Celostne identitete	5	9	0.90–25
7	4	Storitve za izplačila	5	8	8 %–50 % celotne vrednosti izplačila
8	12	Proxiji	4	3	0.30–20
9	8	Goljufije	3	6	5–20
10	7	Nezaželena pošta	3	6	1–25

Podatki o bančnih računih so tako visoko na lestvici zaradi tega, ker je iz njih dokaj enostavno pridobiti premoženjsko korist. Pri kreditni kartici na primer je mnogo težje priti do končnega cilja, torej do denarja, saj je potrebnih več različnih komponent (številka kreditne kartice, datum veljavnosti, CVV2-številka, PIN-koda). Na drugi strani pa je dokaj enostavno priti do denarja s pomočjo podatkov o bančnih računih: preko varnega in neizsledljivega prenosa med računi ali pa s pomočjo storitev, ki jih nudijo »blagajničarji«, včasih tudi prej kot v 15 minutah.

Razlog, da so podatki o bančnih računih na prvem mestu (tabela 2) tako po oglaševanju kot po povpraševanju, je tudi ta, da je v povprečju na bančnem računu več denarja, kot ga ima kreditna kartica skupaj z limitom.

Cene bančnih računov na »podzemnih« serverjih so se med časom raziskave gibale od 10 do 1000 dolarjev (tabela 2). Cena pa je odvisna od tega, koliko denarja je na tem računu, od lokacije in tipa računa. Bančni računi podjetij imajo ponavadi veliko večjo vsoto denarja na računu in se posledično prodajajo za mnogo več kot osebni bančni računi. Bančni računi, ki se nahajajo v EU, so ponavadi dražji kot tisti iz ZDA, kar je verjetno zaradi tega, ker je bančnih računov iz EU manj kot iz ZDA. Bančni računi, ki so vsebovali še ime, naslov in datum rojstva, so bili dražji. Predvidevajo, da zato, ker bi se ti podatki lahko nadalje uporabili še za krajo identitete.

Druga najpogosteje oglaševana dobrina ali storitev glede na predmet je bila številka kreditne kartice skupaj s CVV2-številko. Bila je tudi druga najpogosteje zaželena dobrina (tabela 2). Razlog je veliko spletnih prodajaln, ki za zaščito svojih kupcev poleg številke kreditne kartice zahteva tudi CVV2-številko.

Kreditne kartice s CVV2-številkami se ponavadi prodajajo v paketih od 5 do 500. V času raziskave so se oglaševane cene gibale od pol dolarja do dvanajst dolarjev. Podobno kot pri bančnih računih, se tudi tukaj cene spreminjajo glede na lokacijo izdajatelja kartice. Cena je tudi odvisna od tega, koliko je številk kreditnih kartic v paketu: več kot jih je, nižja je cena na enoto.

Na nekaterih strežnikih je tudi možno preveriti, ali so kupljeni podatki o kreditni kartici pravilni in če je kreditna kartica še veljavna. Ena od možnosti je vdor v sistem trgovine in preizkus avtorizacije kreditne kartice. Če je avtorizacija uspešna, pomeni, da so podatki o kartici pravilni, kartici pa še ni potekel rok veljave. Symantec je med opazovanjem IRC-sporočil opazil več sporočil z naslednjo vsebino: Avtorizacija kreditnih kartic v zameno za majhno donacijo v dobrodelne namene. V tem primeru je šlo verjetno za testiranje veljavnosti kreditnih kartic. Majhne transakcije, kamor spadajo tudi donacije v dobrodelne namene, ne spadajo nujno med običajne potrošniške navade lastnika kartice, vendar običajno ne sprožijo alarma pri varnostnem sistemu izdajatelja kartice.

Številke kreditnih kartic brez CVV2 številk so bile na tretjem mestu po oglaševanju na »podzemnih« strežnikih ter na petem po povpraševanju. Ponavadi se prodaja številka kreditne kartice in datum veljavnosti, dodatno pa je lahko tudi ime lastnika kartice (ali podjetja, če je lastnik kartice podjetje), naslov na katerem je kreditna kartica registrirana, telefonska številka in PIN-koda.

Razlog, zakaj se manj povprašuje po številkah kreditnih kartic kot tistih s CVV2-kodo, je ta, da je brez CVV2-kode mnogo težje zlorabiti kreditno kartico. Sistemi za zaščito uporabnikov kreditnih kartic so vedno boljši ter tudi uporabniki sami so vedno bolj

previdni glede na informacije iz medijev, ki opozarjajo na večjo pogostost zlorab kreditnih kartic.

Na tretjem mestu po povpraševanju so se znašle celostne identitete. Polna identiteta je sestavljena iz: imena in priimka, naslova, datuma rojstva, telefonske številke/številk, EMŠO, številke vozniškega dovoljenja, materinega priimka, e-mail naslova ter tudi iz »skrivnega« vprašanja in odgovora, ki ga ta oseba uporablja na straneh, ki zahtevajo preverjanje. Ker je celostna identiteta sestavljena iz veliko komponent ter je na drugi strani težko pridobiti vse te podatke, je posledično manj celostnih identitet na voljo, kot pa je samo povpraševanje. Ravno zaradi tega so se podatki o celostnih identitetah znašli na tako visokem mestu po povpraševanju.

Konec leta 2007 je bilo v ZDA 8,1 milijona kraj identitet. To je 4 procente manj kot leto prej, kar pomeni, da se število kraj identitet zmanjšuje, to pa bi lahko pripisali večjemu zavedanju in pazljivosti ljudi pri vsakodnevnih aktivnostih.

V času raziskave so cene celostnih identitet nihale med 0,90 in 25 dolarji. Podobno kot pri ostalih dobrinah je tudi tukaj cena različna glede na to, čigava je identiteta ter od kod prihaja. Tudi v tem primeru so identitete iz držav Evropske unije dražje kot tiste iz ZDA. Razlog je verjetno ta, da je prost promet po celem ozemlju Evropske unije.

Ob opazovanju neformalne ekonomije na strežnikih je Symantec opazil, da je bilo v času raziskave število ponudb in povpraševanja dobrin in storitev na približno isti ravni. To sledi temeljnemu ekonomskemu pravilu o ponudbi in povpraševanju, kar pomeni, da je »podzemna« ekonomija že dozorela v pravo ekonomijo. Kot v legalni ekonomiji je tudi tukaj opazen dvig cen v primeru manjše ponudbe ter padec cen v primeru večje ponudbe. Pričakovati je tudi, da bi se v primeru dviga popularnosti neke dobrine ali storitve povečala tudi ponudba.

- **Vzorci občutljivih informacij**

Med julijem 2007 in junijem 2008 je Symantec spremljal 44.752 edinstvenih vzorcev, ki so vsebovali občutljive informacije in so bili javno objavljeni na »podzemnih« strežnikih. Ponudniki pogosto javno objavijo vzorce svojih dobrin ali storitev z naslednjimi nameni: dokazati, da ponudnik dejansko ima dobrino ali storitev v lasti; pokazati potencialnemu kupcu kvaliteto dobrine ali storitve; dvigovanje lastnega ugleda ter z namenom, da morebitni kupec preveri, če je to res dobrina ali storitev, ki jo potrebuje.

Največkrat so se v času raziskave na »podzemnih« strežnikih pojavili vzorci informacij o kreditnih karticah (CVV2 številke, številke kreditnih kartic, datum veljavnosti kreditne kartice), in sicer v kar 56 odstotkih (tabela 3).

Tabela 4: Vzorci občutljivih informacij (vir: Symantec)

Rangiranje ponudb	Vzorci občutljivih informacij	Ponudba v %
1	CVV2 številke	23
2	Številke kreditnih kartic	18
3	Datumi veljavnosti kreditnih kartic	15
4	Naslovi	12
5	Telefonske številke	11
6	E-poštni naslovi	6
7	PIN-številke za kreditne ali debetne kartice	5
8	EMŠO	4
9	Polna imena	4
10	Datum rojstva	2

Kot smo videli je na »podzemnih« strežnikih mogoče najti zelo veliko različnih vzorcev, ki jih ponujajo spletni kriminalci. Glede na to, da so podatki javno objavljeni na več kanalih in na različnih spletnih strežnikih, je jasno, da imajo zelo velik doseg, kar pa ne pomeni nič dobrega za žrtve kaznivih dejanj.

- **Vrednost vseh oglaševanih dobrin in storitev**

S to analizo je Symantec poskušal ugotoviti, kakšna je skupna vrednost vsega oglaševanega na opazovanih »podzemnih« strežnikih. Uporabili so povprečne vrednosti posamičnih dobrin ali storitev ter povprečne vrednosti pri dobrinah ali storitvah, ki se oglašujejo v paketih. Ocena skupne vrednosti na opazovanih strežnikih je bila preko 276 milijonov dolarjev. Najvišjo vrednost so predstavljale informacije o kreditnih karticah, in sicer kar 59 odstotkov vsega oglaševanega (tabela 4). To ni presenetljivo, saj so bile v času raziskave informacije o kreditnih karticah najbolj cenjene, hkrati pa je bilo največje povpraševanje na »podzemnih« strežnikih.

Tabela 5: Vrednosti vseh oglaševanih dobrin in storitev v odstotkih po kategoriji (vir: Symantec)

Rangiranje	Kategorija	Vrednost v %
1	Informacije o kreditnih karticah (Credit card information)	59
2	Kraja identitete (Identity theft information)	16
3	Računi strežnikov (Server accounts)	10
4	Finančni računi (Financial accounts)	8
5	Informacije o ribarjenju in nezaželeni pošti (Spam and phishing information)	6
6	Orodja za krajo premoženja (Financial theft tools)	<1
7	Okuženi računalniki (Compromised computers)	<1
8	Škodljivi programi (Malicious applications)	<1
9	Spletni računi (Website accounts)	<1
10	Spletni igralni računi (Online gaming accounts)	<1

Treba je opozoriti, da ocena skupne vrednosti ne upošteva vsote denarja, ki se nahaja na kreditnih karticah ali na bančnih računih. Ocenjena je bila samo vrednost teh informacij, s pomočjo katerih bi se nadalje lahko prišlo do premoženjske koristi. Če bi upoštevali tudi vsoto denarja na kreditnih karticah in bančnih računih, bi bila samo vrednost kreditnih kartic 5,3 milijarde dolarjev, vrednost bančnih računov pa 1,7 milijarde dolarjev.

Vsi ti podatki kažejo sliko, kolikšna je potencialna vrednost celotnega podzemlja. Finančni sektor se je na vse zgoraj našteto odzval z implementiranjem natančnejših preventivnih ukrepov in varnostnih politik, s pomočjo katerih bo poskušal zaščititi svoje in uporabnikovo premoženje (Symantec, 2008).

Zlonamerna orodja

Zlonamerna orodja imajo na »podzemnih« strežnikih dvojno funkcijo. Lahko se uporabljajo kot orodje za pridobivanje drugih dobrin in storitev, lahko pa tudi sami nastopajo kot dobrina. To zagotavlja neko stopnjo samozadostnosti »podzemne« ekonomije, saj znanje, storitve in orodja proizvedejo še več dobrin in storitev, ki se jih lahko ponudi na trgu.

Zlonamerna orodja se v glavnem delijo na:

- napadalna orodja (Attack tools),
- orodja pošiljanja nezaželene e-pošte in ribarjenja (Spam and phising tools),
- zlonamerne kode (Malicious code),
- izkoriščanje informacij (Exploits).

S pomočjo zlonamernih orodjih se na nedovoljen način pridobiva informacije, ki se nadalje lahko uporabijo za pridobivanje premoženjskih koristi. Te informacije se lahko proda na »podzemnih« strežnikih ali pa se jih uporabi direktno. Cene zlonamernih orodij so zelo različne, od nekaj dolarjev pa vse do tisoč in več dolarjev. Vse je odvisno seveda od tega, za kako zahtevno orodje gre, ter od vrednosti informacij, ki jih tako orodje lahko pridobi (Symantec, 2008).

4.2.4 Načini plačil za dobrine in storitve na »podzemnih« strežnikih

Večina plačil za dobrine in storitve na »podzemnih« strežnikih je opravljenih brez fizičnega kontakta, saj se uporabniki večinoma poslužujejo elektronskih načinov plačila. Prednost tega načina plačila je predvsem ta, da je plačilo takoj na prodajalčevem računu. Podobno kot v formalni ekonomiji tudi tukaj prodajalci preferirajo določen način plačila in ne sprejemajo drugih načinov. Na podlagi tega je Symantec ocenil, kateri so najpopularnejši načini plačevanja na »podzemnih strežnikih.

Najpogosteje se je plačevalo s pomočjo računov za izmenjavo spletnih valut, in sicer kar v 63 odstotkih. Spletno valuto se enostavno pridobi tako, da se preprosto pravi denar zamenja za spletno valuto. Prednosti takega načina plačevanja so takojšnje plačilo, storitev je na voljo po celem svetu, plačila so nepovratna (ko je transakcija zaključena, ni več možno pridobiti denarja nazaj), stroške transakcije nosi prodajalec, kar pomeni, da kupec ne občuti dodatnih stroškov.

Dodatne pozitivne strani plačevanja s pomočjo računov za izmenjevanje spletnih valut so tudi ta, da nekatera podjetja, ki se ukvarjajo s temi transakcijami, zahtevajo le veljaven e-poštni račun, uporabnik pa lahko uporabi proxy server ter si tako zakrije svoj IP-naslov[12]. Možno je imeti več računov, starostne omejitve ni. Podjetje ni dolžno nadzorovati svojih uporabnikov in sumljivih transakcij. Vse te

[12] IP-naslov je številka, ki natančno določa računalnik v omrežju internet. Kratica IP označuje Internet Protocol.

prednosti omogočajo kibernetskim kriminalcem uporabo lažnega imena pri izvajanju nedovoljenih transakcij. Junija 2007 je bilo že preko 5 milijonov tovrstnih spletnih računov. Vendar ni vse tako rožnato, kot se sliši, nekaj lastnikov podjetij, ki se ukvarjajo s spletnimi valutami, je že priznalo krivdo pranja denarja. Druga podjetja so tudi začela preiskovati račune svojih strank, kar je pri prodajalcih na »podzemnih« strežnikih vzbudilo precej strahu, kaj se bo dogajalo v prihodnosti.

Drugi najbolj pogost način plačila na »podzemnih« strežnikih je menjava dobrin ali storitev. Ta način plačila je bil uporabljen v 24 odstotkih. Pri tem načinu plačila gre za čisto preprosto logiko. Nekdo, ki je uspešen pri pridobivanju določenih informacij, jih z veseljem zamenja za neko dobrino ali storitev, za katero nima dovolj znanja ali pravega orodja.

Tretja najpogosteje uporabljena tehnika plačevanja je bila plačevanje s spletnimi računi, in sicer v 9 odstotkih. Ta način plačevanja je popularen zato, ker si kibernetski kriminalci lahko napolnijo svoje spletne račune s pomočjo ukradenih kreditnih kartic in tako kupijo še več dobrin in storitev od drugih prodajalcev. Možna je tudi uporaba ukradenega spletnega računa za nakup dobrin ali storitev (Symantec, 2008).

4.2.5 IRC-strežniki glede na lokacijo

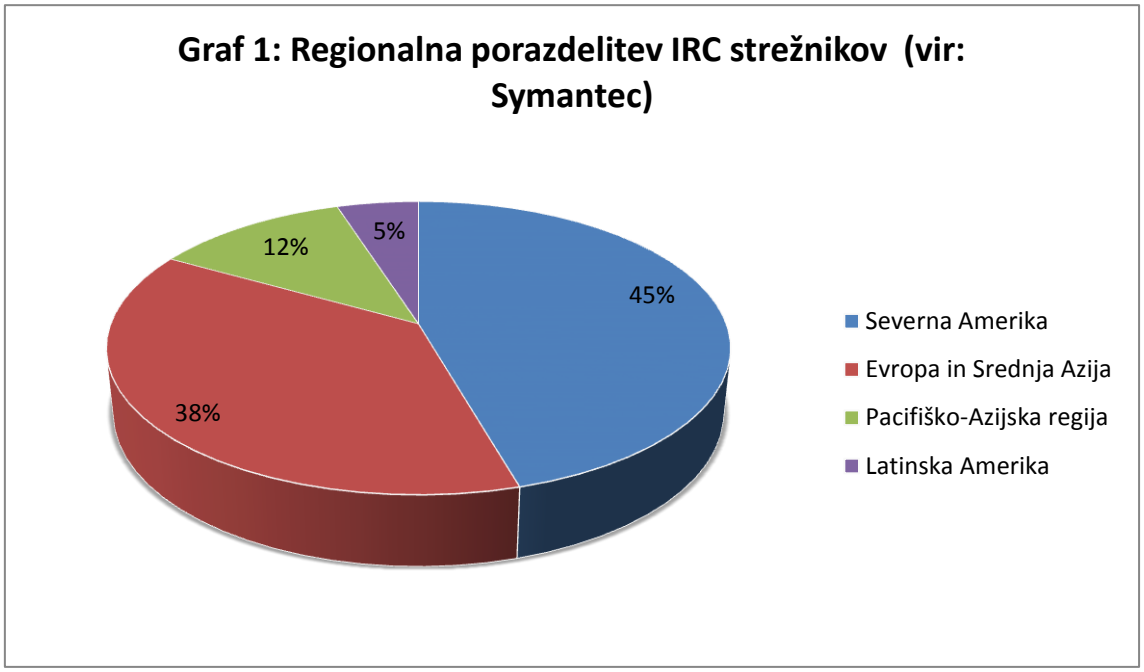
Geografske lokacije »podzemnih« strežnikov se ves čas spreminjajo. Ljudje na teh strežnikih pa delujejo po celem svetu ob vseh možnih urah. Primer: V nekem primeru, ko je šlo za vdor in krajo več kot 46,5 milijonov podatkov o kreditnih karticah, je bilo ugotovljeno, da je pri tem sodelovalo 11 oseb, ki so delovali na popolnoma različnih koncih sveta, vključujoč ZDA, Estonijo, Ukrajino, Kitajsko in Belorusijo. Podatke o ukradenih kreditnih karticah pa so pošiljali iz Ukrajine, Kitajske, Belorusije, Filipinov ter iz Tajske.

Symantec je poskušal ugotoviti, kje se je nahajalo največ IRC-strežnikov v času raziskave. S pomočjo teh rezultatov bi se dalo delno ugotoviti, kje je »podzemna« ekonomija najbolj razvita, čeprav sama lokacija strežnika ni nujno povezana z lokacijo, kjer se nahajajo uporabniki le-teh. Treba je tudi poudariti, da se na vseh IRC-strežnikih ne odvijajo nezakonite aktivnosti, lahko pa se na enem strežniku odvijajo tako zakonite kot tudi nezakonite aktivnosti.

V času raziskave je bilo največ IRC-strežnikov v Severni Ameriki, in sicer kar 46 odstotkov (graf 1). Evropa, srednja Azija in Afrika so pristali na drugem mestu z 38

odstotki, Azijsko-Pacifiška regija je imela 12 odstotkov, Latinska Amerika pa 5 odstotkov IRC-strežnikov.

Graf 1: Regionalna porazdelitev IRC-strežnikov (vir: Symantec)



Eden od razlogov za tako nizek odstotek IRC-strežnikov na ozemlju Latinske Amerike in Pacifiško-Azijske regije je ta, da v nekaterih državah, kot je recimo Kitajska, niso v tolikšni meri seznanjeni z IRC-strežniki, zato uporabljajo druge načine komunikacij, kot so na primer spletni forumi. Drugi razlog za nizek odstotek na prej omenjenih ozemljih pa je verjetno tudi ta, da se na ozemlju Latinske Amerike in Pacifiško-Azijske regije namenja manj nadzora že uveljavljenim načinom komunikacije, kot so spletni forumi in oglasne deske. Zaradi tega spletni kriminalci ne menjajo že uveljavljenega načina komuniciranja, saj jim zaradi tega ni treba vlagati dodatnega truda v ustanovitev in oglaševanje svojega strežnika. Ker pa je nadzor v Severni Ameriki in Evropi strožji, pa se uporabniki raje odločijo za IRC-strežnike. Organi pregona imajo več težav z nadzorovanjem IRC-strežnikov kot spletnih forumov.

Država z največjim številom IRC-strežnikov je bila v času raziskave ZDA z 41 odstotki (tabela 5). Eden od razlogov za tako velik odstotek je ta, da je imelo v času raziskave več kot 75 milijonov uporabnikov interneta v ZDA širokopasovno povezavo. Glede na prejšnje raziskave naj bi imele ZDA tudi največje število spletnih strani, namenjenih ribarjenju. Glede na to, da se velik odstotek kibernetskega kriminala zgodi v ZDA, ni presenetljivo, da je tam tudi največ IRC-strežnikov.

Tabela 6: Države z največjim številom IRC-strežnikov (vir: Symantec)

Rangiranje	Kategorija	IRC strežniki v %	Regija
1	Združene države Amerike	41	Severna Amerika
2	Romunija	13	Evropa in Srednja Azija
3	Nemčija	11	Evropa in Srednja Azija
4	Združeno kraljestvo	6	Evropa in Srednja Azija
5	Kanada	5	Severna Amerika
6	Avstralija	4	Pacifiško-Azijska regija
7	Brazilija	3	Latinska Amerika
8	Južna Koreja	2	Pacifiško-Azijska regija
9	Nizozemska	2	Evropa in Srednja Azija
10	Švedska	2	Evropa in Srednja Azija

Na drugem mestu se je po številu IRC-strežnikov znašla Romunija s 13 odstotki. Razlog za to je verjetno v občutnem povečanju kibernetskega kriminala na tem področju. V Romuniji je velik odstotek brezposelnih, priložnosti za delo pa je malo. Ima pa Romunija dobro zgodovino glede računalniškega znanja, kar je ob pomanjkanju zaposlitev pripeljalo do povečanega udejstvovanja v kibernetski kriminaliteti. V prejšnjih raziskavah je Symatec ugotovil, da je Romunija država z največ spletnimi stranmi v Evropi in Srednji Aziji, ki so namenjene ribarjenju, kar je tudi pokazatelj aktivnosti kibernetskega kriminala v določeni državi.

Glede na to, da gre tako v ZDA kot v Romuniji za veliko aktivnost na področju kibernetskega kriminala, je treba razložiti še, zakaj je tako velika razlika v številu IRC-strežnikov. Mogoče se na prvi pogled zdi, da je razširjenost veliko večja v ZDA, vendar če pogledamo število uporabnikov širokopasovne povezave v Romuniji (2,25 milijona) in jih primerjamo s številom v ZDA (75 milijonov), ugotovimo, da je 13 odstotkov izredno visoka številka. Manjše število uporabnikov širokopasovne povezave ponavadi pomeni manjšo možnost udejstvovanja na svetovnem spletu, vendar v primeru Romunije ni tako, kar je lahko eden od razlogov za skrb.

Nemčija je imela v času raziskave podoben odstotek IRC-strežnikov kot Romunija, in sicer 11 odstotkov. Tudi Nemčija ima zelo aktivno zgodovino na področju spletnega ribarjenja, še vedno pa se odvija veliko nedovoljenih aktivnosti na tem področju. Ima močno računalniško infrastrukturo ter spada med pet držav, ki imajo največ

širokopasovnih uporabnikov. Vendar ima še vedno 50 milijonov širokopasovnih uporabnikov manj kot ZDA, kar razloži tako veliko razliko po številu IRC-strežnikov.

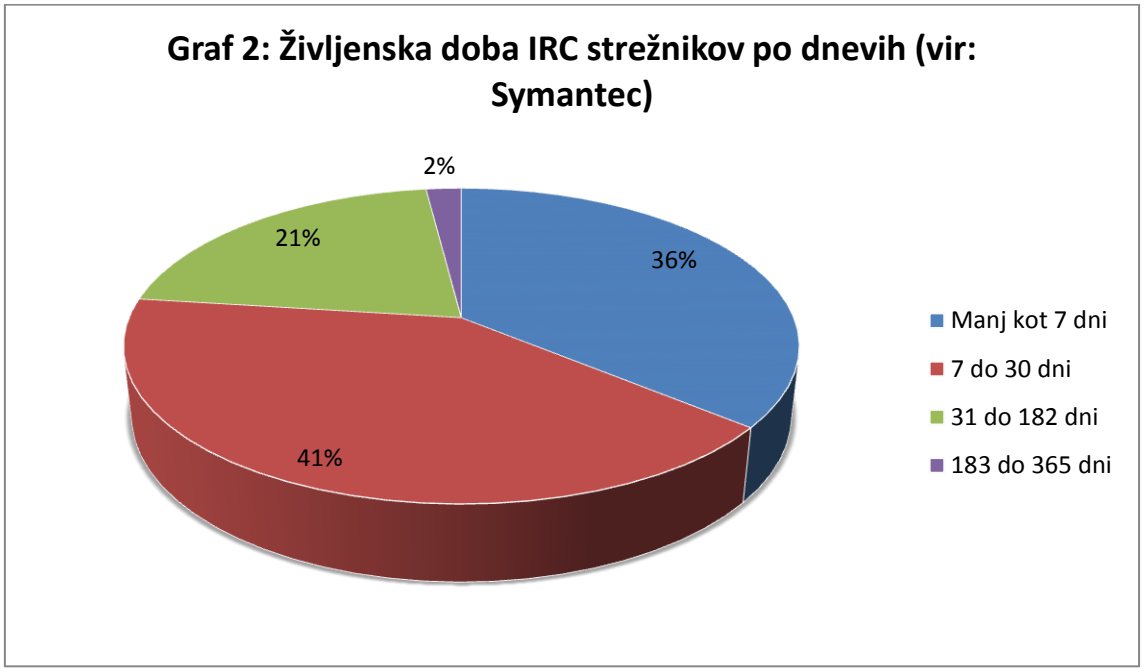
ZDA, Romunija in ostale države, ki visoko rangirajo po številu IRC-strežnikov, so bile zaznane kot varne države za »podzemne« strežnike, vsaj do te mere, da če strežnik ni postal prevelik ter zelo popularen, storilci kibernetskega kriminala niso bili ogroženi, da bi jih odkrili. Veliko število legitimno delujočih IRC-strežnikov je tudi dobra priložnost za IRC-strežnike, na katerih se odvijajo nezakonite aktivnosti, da se le-teh ne odkrije. Večji IRC-strežniki, ki imajo veliko število uporabnikov, so ravno tako bolj priljubljeni za kibernetske kriminalce kot IRC-strežniki z manjšim številom uporabnikov (Symantec, 2008).

4.2.6 Življenjska doba IRC-strežnikov

Glede na nedovoljeno delovanje »podzemnih« strežnikov so se kibernetski kriminalci bili primorani prilagoditi ter delovati preventivno, torej menjati lokacijo oziroma zapreti strežnik. Med časom raziskave je bila povprečna življenjska doba IRC-strežnika, na katerem so se dogajale nedovoljene aktivnosti, 10 dni. 36 odstotkov IRC-strežnikov je bilo aktivnih manj kot 1 teden (graf 2), 41 odstotkov jih je bilo aktivnih od 1 tedna do 1 meseca ter 21 odstotkov je bilo aktivnih od 1 meseca do pol leta. Le 2 odstotka IRC-strežnikov je bilo delujočih več kot pol leta.

Razlogov za zapiranje IRC-strežnikov je več, največkrat pa pride do zaprtja zaradi prevelikega prometa, predvsem na manjših IRC-strežnikih, kjer je povečana aktivnost hitro opažena. Do zaprtja lahko pride tudi zaradi premajhne aktivnosti uporabnikov ali pa ga zaprejo kar administratorji, če opazijo, da se dogajajo nedovoljene aktivnosti. Udeleženci »podzemne« ekonomije so sprejeli hitro menjavanje lokacij ter zapiranje IRC-strežnikov, saj imajo na ta način več možnosti, da jih organi pregona ne odkrijejo (Symantec, 2008).

Graf 2: Življenjska doba IRC-strežnikov po dnevih (vir: Symantec)



5 Zaključek

Skozi pisanje magistrske naloge smo prišli do zaključka, da je kibernetska kriminaliteta ustvarila neverjetno zrelo in samostojno neformalno ekonomijo, ki deluje po istih principih kot prava ekonomija. Cene na neformalnih tržnicah se prilagajajo povpraševanju in ponudbi, temu pa se prilagajajo tudi »zaposlitve« na določenih področjih. Kibernetska neformalna ekonomija je praktično povsod sestavljena iz štirih različnih delov. Prva dva dela sta sestavljena iz kraje denarja (realnega ali igralnega) ter iz ponujanja informacij o bančnih računih, kreditnih karticah, igralnih računih in podobno. Tretji del skrbi za vdiranje v spletne strani, pametne telefone, strežnike itd. Te vdore se izvaja z namenom pridobivanja zaupnih informacij s pomočjo različnih orodij, ki jih ustvari četrti del neformalne kibernetske ekonomije. Vsi deli so nujno potrebni za nemoteno in samostojno delovanje neformalne ekonomije.

Ker je bilo preiskovanje kibernetske kriminalitete izredno težko, saj le-ta nima geografskih omejitev in je delovala v državah, ki so imele različno zakonodajo, je bila konec leta 2001 sprejeta Konvencija o kibernetski kriminaliteti. Države podpisnice so se zavezale, da bodo svoje kazensko in materialno pravo poenotile z vsemi ostalimi članicami ter se na ta način rešile multijurisdikcije. Izrednega pomena je tudi ustanovitev mednarodne mreže, v kateri se neprestano izmenjuje informacije, izkušnje ter se sodeluje na različnih področjih kibernetske kriminalitete.

Neformalna ekonomija se na svetovnem spletu največkrat nahaja na spletnih forumih ter na IRC-strežnikih. Da lahko privablja nove člane, mora delovati na javnih mestih, torej tako na očeh potencialnih kupcev in začetnikov, ki si želijo postati del kibernetske kriminalitete, kot tudi na očeh organov pregona. Ravno zaradi tega morajo spreminjati svoje lokacije, da zmanjšajo tveganje po odkritju in morebitni kazni. Potrebno je vedeti, da bi se večina članov kibernetske kriminalitete lahko preživela tudi v pravi ekonomiji, saj posedujejo dovolj znanja za opravljanje različnih poklicev, vendar je glavni motiv zaslužek, ki je v neformalni ekonomiji lahko bistveno višji. Poseben primer pa je Romunija, kjer se je število ljudi delujočih v kibernetski kriminaliteti povečalo zaradi pomanjkanja služb. Posamezniki z znanjem računalništva so se ravno zaradi nastale situacije odločili sodelovati s kibernetsko kriminaliteto.

Cene dobrin in storitev so v neformalni ekonomiji kibernetske kriminalitete zelo različne, od nekaj dolarjev do več tisoč dolarjev. Razpon cen je odvisen od več

dejavnikov. Poleg povpraševanja in ponudbe ceno spreminja tudi kvaliteta dobrin in storitev. Bolj kot so informacije kvalitetne ali storitve tehnično dovršene, višjo ceno je možno iztržiti na »podzemni« tržnici.

Da se lahko morebitni kupci prepričajo, da kupujejo kvalitetne dobrine oz. storitve, pa prodajalci ponujajo vzorce, s pomočjo katerih dokažejo, da imajo to, kar kupec potrebuje.

Pri neformalni ekonomiji in kibernetski kriminaliteti gre za dva izredno kompleksna področja, ki ju je treba neprestano spremljati in nadzorovati. Organi pregona potrebujejo redna izobraževanja, ključnega pomena pa je mednarodno sodelovanje ter izmenjavanje informacij.

5.1 Odgovori na hipoteze

Na začetku smo postavili tri hipoteze.

Prva hipoteza se je glasila: *Neformalna ekonomija prehaja v kibernetski svet*.

To hipotezo potrjujemo. Jasno je, da svetovni splet ponuja marsikaj. Ker je število uporabnikov svetovnega spleta zelo veliko, je zaradi tega tudi toliko večji krog potencialnih strank, kot v realnem svetu. Zaradi tega in zaradi enostavnosti uporabe svetovnega spleta, se tudi neformalna ekonomija seli v kibernetski svet, vsaj tista, ki je tam boj uspešna. Veliko vrst goljufij se je preselilo na svetovni splet v praktično nespremenjeni obliki, predvsem zaradi veliko večjega dosega. Vendar pa kljub vsemu kibernetski svet in realni svet sodelujeta drug z drugim ter poskušata iz vsakega sveta izkoristiti maksimum. Kot smo videli v poročilu Symantec, je bilo na »podzemnih« strežnikih daleč največ oglasov s podatki o kreditnih karticah. Do teh podatkov pa se da priti v obeh svetovih ali s pomočjo ribarjenja v kibernetskem svetu ali pa s pomočjo skeniranja magnetnega zapisa kartice v realnem svetu (ter seveda tudi z ostalimi tehnikami iz obeh svetov). Torej, če povzamemo na kratko, kriminalci bodo vedno iskali lažji, učinkovitejši in dobičkonosnejši način za pridobitev določene dobrine ali storitve. Pri tem pa bodo izkoristili oba sveta, tako kibernetskega kot realnega. Vendar pa kibernetski svet ponuja večjo anonimnost ter s tem večjo varnost pred razkritjem, ponuja pa tudi mnogo hitrejše kroženje informacij in mnogo večji doseg od realnega sveta.

Druga hipoteza se je glasila: *Organi pregona so dobro izobraženi in usposobljeni za pregon tovrstne kriminalitete.*

To hipotezo potrjujemo. Največji korak za uspešen pregon tovrstne kriminalitete se je zgodil s sprejetjem konvencije o kibernetski kriminaliteti tehnološko razvitih držav, med njimi tudi ZDA. Glede na to, da je kibernetski kriminal mednarodno razširjen, je sodelovanje med državami nujno. Poenotenje zakonodaje je ključno, saj je samo na ta način možno normalno mednarodno sodelovanje. Do tega pa je s podpisom te konvencije tudi že prišlo pri državah podpisnicah. Konvencija se v kazensko procesnem delu tudi osredotoči na zavarovanje, preiskovanje in zaseg računalniških podatkov ter opredeljuje sodno pristojnost. Vse našteto ter še več organom pregona postavlja dobre temelje za pregon tovrstne kriminalitete. Vendar to ni dovolj, potrebno je redno usposabljanje ter aktivno spremljanje vseh novosti, ki se zgodijo v kibernetskem svetu, saj je le na ta način možno ostati v koraku z napredkom tovrstne kriminalitete.

Tretja hipoteza se je glasila: *V bolj razvitih državah sveta je stopnja kibernetskega kriminala višja kot v manj razvitih državah.*

To hipotezo zavračamo. Syamantec je pri raziskavi o geografskih lokacijah »podzemnih« strežnikov ugotovil, da je za razcvet kibernetskega kriminala možnih več različnih dejavnikov. Eden najpomembnejših dejavnikov je definitivno širokopasovna internetna povezava, ki je nekako osnovni pogoj za razvoj kibernetskega kriminala. To se je izkazalo v primeru ZDA za pravilno sklepanje, saj imajo daleč največ uporabnikov, ki imajo dostop do širokopasovne internetne povezave ter hkrati največ IRC-strežnikov, na katerih se dogajajo tako dovoljene kot tudi nedovoljene aktivnosti. Vendar pa je to pravilo odpovedalo v primeru Romunije, ki ima dokaj malo uporabnikov s širokopasovno povezavo, pa kljub temu izredno velik odstotek IRC-strežnikov. Ta pojav je Symantec razložil z veliko brezposelnostjo v Romuniji ter z dobro zgodovino računalniškega znanja, kar je privedlo do takega rezultata. S tem dejstvom zavračamo hipotezo, da je v bolj razvitih državah stopnja kibernetskega kriminala višja kot v manj razvitih državah. Res pa je, da je za storitev kibernetskega kriminala potreben dostop do svetovnega spleta (po možnosti širokopasoven) ter vsaj osnovna računalniška oprema.

6 Literatura

Andrić, Č. in Mijović, J. (2010). Project: Efficient combating the informal economy. Pridobljeno dne 4. 1. 2014 na http://www.socijalnoekonomskisavet.rs/en/doc/informal_economy_in_serbia.pdf

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana, Fakulteta za varnostne vede.

Bram, T. (2013). The Undergound Internet Economy Of Cybercrime. Pridobljeno dne 15. 6. 2014 na http://www.investopedia.com/financial-edge/0113/the-underground-internet-economy-of-cybercrime.aspx

Castell, M. (2013). Mitigating Online Account Takeovers: The Case for Eduaction. Federal Reserve Bank of Atlanta. Pridobljeno dne 1. 2. 2012 na http://www.frbatlanta.org/documents/rprf/rprf_pubs/130408_survey_paper.pdf

Danopoulos, C. in Žnidarič, B. (2007). *Informal economy, tax evasion and poverty in a democratic setting*. Mediterranean qartely, str. 67—84.

Dimc, M. in Dobovšek, B. (2012). *Kriminaliteta v informacijski družbi*. Ljubljana, Fakulteta za varnostne vede.

Europol. (2011). Internet facilitated organised crime. Pridobljeno dne 14. 6. 2014 na https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf

Europol. (2012). Payment card fraud in the European Union, Perspective of law enforcement agencies. Pridobljeno dne 26.1.2014 na https://www.europol.europa.eu/sites/default/files/1public_full_20_sept.pdf

International Mass-Marketing Fraud Working Group. (2010). Mass-Marketing Fraud: A Threat Assessment. Pridobljeno dne 3. 2. 2014 na https://www.europol.europa.eu/sites/default/files/publications/immftafinal_0.pdf

Internet Society. (2011). Perspecites on policy responses to online copyright infringement. Pridobljeno dne 23. 2. 2014 na http://www.internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape

Investopedia. (2014). Investment scams: Different types of scams. Pridobljeno dne 18. 2. 2014 na http://www.investopedia.com/university/scams/scams1.asp

Jianwei, Z., Liang, G. in Haixin, D. (2012). Investigating China`s Online Underground Economy. University of California, Institute on global conflict and

cooperation. Pridobljeno dne 8. 5. 2014 na http://igcc.ucsd.edu/assets/001/503677.pdf

Jones, E. (2012). Protect Yourself: What Is Auction Fraud. Pridobljeno dne 9. 2.2014 na https://www.edwardjones.com/groups/ejw_content/@ejw/documents/web_content/web233463.pdf

Ministrstvo za delo, družino, socialne zadeve in enake možnosti. (2014). Preprečevanje dela in zaposlovanja na črno. Pridobljeno dne 3. 8. 2014 na http://www.mddsz.gov.si/si/delovna_podrocja/delovna_razmerja_in_pravice_iz_dela/delovna_razmerja/delo_na_crno/

Rupnik, A. (2002). Konvencija o kibernetski kriminaliteti – »Budimpeštanska konvencija« Pridobljeno dne 13. 3. 2014 na http://uploadi.www.ris.org/editor/1132054990Kiber_kriminaliteta.pdf

Schneider, F. in Buehn, A. (2012). Shadow Economy in Highly Developed OECD Countries: What Are the Driving Forces? Pridobljeno dne 10. 8. 2014 na http://ftp.iza.org/dp6891.pdf

Seger, A. (2012). Cyber Crime and Economic Crime. V Edelbacher, M., Kratcoski, P., Theil, M. (ur.), Financial Crimes: A Threat to Global Security (str. 119—146).

Shapland, J. in Ponsaers, P. (2009). Potential effects of national policies on the informal economy. V Shapland, J., Ponsaers, P. (ur.), *The informal economy and connections with organised crime: the impactof national social and economic policies*. Hague: Bju legal publishers.

Svet Evrope, (2001). Convention on Cybercrime. Pridobljeno dne 27.6.2013 na http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Symantec, (2008). Symantec Report on the Underground Economy. Pridobljeno dne 9. 5. 2014 na http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

Urad RS za intelektualno lastnino. (2014). Kaj so avtorska dela? Pridobljeno dne 23.2.2014 na http://www.uil-sipo.si/uil/dodatno/koristni-viri/pogosta-vprasanja/avtorska-pravica/

Zakona o preprečevanju dela in zaposlovanja na črno (ZPDZC-1). (2014). Uradni list RS, (32/2014).

Žurnal24.si, (2014). »Država naj se s tajkuni poravna«. Pridobljeno dne 12. 8. 2014 na http://www.zurnal24.si/drzava-naj-se-s-tajkuni-poravna-clanek-229500

Delovni življenjepis kandidata

Rodil sem se 25. septembra 1987 v Ljubljani. Osnovno šolo sem prva štiri leta obiskoval na Podružnični šoli Kopanj, naslednja štiri leta pa na Osnovni šoli Louisa Adamiča Grosuplje. Po končani srednji šoli sem se vpisal na Srednjo zdravstveno šolo v Ljubljani, ki sem jo uspešno zaključil s poklicno maturo. Leta 2006 sem se vpisal na visokošolski študij varstvoslovja na Fakulteti za varnostne vede, kjer sem leta 2010 tudi diplomiral. Istega leta sem se vpisal še na podiplomski študij varstvoslovja.

Leta 2008 sem opravil obvezno prakso na štirinajstdnevnem študentskem vojaškem taboru.

Leta 2011 sem pridobil certifikat o nacionalni poklicni kvalifikaciji varnostni menedžer.

V času študija sem namenil ogromno časa tudi pridobivanju izkušenj s študentskim delom. Opravljal sem raznovrstna dela, od dela v proizvodnji, anketiranja do dela v oglaševanju.

Trenutno sem zaposlen v podjetju Antenna TV SL, d. o. o., kot traffic specialist.

Aktivno govorim angleški jezik ter poznam strokovno terminologijo v latinskem jeziku.

Dobro se znajdem v programskih okoljih Microsoft Windows in Office ter v programih MIS TV in Arianna.

Imam vozniški izpit B-kategorije in opravljen začetni tečaj jadralnega padalstva. Hobiji pa so več ali manj povezani z gibanjem v naravi.