YASHIRIN TARMOQ “DARKNET” ORQALI SODIR ETILADIGAN KIBER VA IQTISODIY JINOYATLAR VA ULARGA QARSHI KURASHISH MASALALARI

Muxsimov Ulug‘bek Timurbek o‘g‘li

Sergeli tuman prokuraturasi katta tergovchisi

ANNOTATSIYA

Kiber jinoyatchilikda “Darknet” bozorlarini monitoring qilish hamda duch keladigan muammolar va huquqni muhofaza qilish organlarining ushbu saytlarda jinoiy faoliyatga qarshi kurashish harakatlari muhokama qilindi. Unda anonimlik uchun ilg‘or texnologiyalardan foydalanish va bu muammoni hal qilishda huquqni muhofaza qiluvchi idoralar o‘rtasida hamkorlikda harakat qilish zarurligi ta’kidlangan. Maqolada, shuningdek, “Hyperion” operatsiyasi kabi darknetdagi noqonuniy faoliyatga qarshi muvaffaqiyatli operatsiyalar haqida so‘z yuritiladi, ammo bu platformalarda jinoiy faoliyatga qarshi kurashni davom ettirish zarurligi ta'kidlanadi. Platformalarni yopib qo‘yishdan ko‘ra, undagi sotuvchilarga e'tibor qaratish muhim va kiberjinoyatlarga qarshi samarali kurashish uchun huquqni muhofaza qilish idoralari o‘rtasidagi hamkorlikni kuchaytirish zarurdir.

Kalit so‘zlar: *Darknet, “Hyperion” operatsiyasi, kiberjinoyat, RAND korporatsiyasi, Dark Web Monitor, IP-manzil, VPN, FATF, Tor brauzer, anonim tarmoq.*

ANNOTATION

The problems faced in monitoring the “Darknet” markets and the efforts of law enforcement agencies to combat criminal activities on these sites were discussed. It emphasizes the need for the use of advanced technologies for anonymity and the need for cooperation between law enforcement agencies in solving this problem. The article

also mentions successful operations against illegal activity on the darknet, such as Operation Hyperion, but stresses the need to continue fighting criminal activity on these platforms. Rather than shutting down platforms, it is important to focus on the vendors on them and to strengthen cooperation between law enforcement agencies to effectively combat cybercrime.

Key words: *Darknet, "Hyperion" operation, cybercrime, RAND corporation, Dark Web Monitor, IP-address, VPN, FATF, Tor brauzer, anonymous network.*

Zamonaviy dunyoda axborotni yaratish va integratsiyalashuv jarayonlari (umumiy va shaxsiy foydalanishda) doimiy ravishda sodir bo‘lib, texnologik taraqqiyotning ta’sirchan natijalaridan foydalangan holda jinoyatchilik ham sifat jihatidan o‘zgarib bormoqda. Kapitalni masofaviy tasarruf etishning texnik va texnologik mavjudligi ma’lum ma’lumotlarga ega bo‘lgan jinoyatchilarga firibgarlik yo‘li bilan boshqa shahar, viloyat yoki mamlakatda yashovchi fuqarolardan pul o‘g‘irlash imkoniyatini beradi. Shu bilan birga, zamonaviy kompyuter texnologiyalari va aloqa vositalaridan foydalangan holda sodir etilgan jinoyatlar jiddiy o‘ziga xos xususiyatga ega bo‘lib, bu tajovuzkorning haqiqiy harakatlarini aniqlashda ham, jinoiy qilmish sodir etishning potentsial imkoniyatlarini aniqlashda ham qiyinchiliklar tug‘diradi.

Ayni paytda, huquqni muhofaza qilish organlari amaliyoti ko‘rsatganidek, ushbu chora-tadbirlar zarur bo‘lgani holda, umuman axborot-telekommunikatsiya makonida sodir etilgan jinoyatlarning, xususan, telekommunikatsiya va kompyuter tarmoqlaridan foydalangan holda sodir etilgan firibgarliklarning oldini olish masalalarida to‘liq emas.

“Darknet” bozorlarini tekshirishda bir qator tergov qiyinchiliklari mavjud. Doimiy takomillashib borayotgan anonimlashtirish usullari va o‘zgaruvchan tahdidlar manzarasi tufayli ma’lumotlarni topish va himoya qilish huquqni muhofaza qilish organlari uchun ko‘plab muammolarni keltirib chiqaradi. Bundan tashqari, ushbu holat Yevropa Ittifoqidagi turli xil huquqiy tashkilotlarning ushbu darknet bozorlariga qarshi birgalikdagi sa’y-harakatlarini murakkablashtirmoqda. Biroq, huquqni muhofaza

qilish organlarida onlayn jinoiy bozorlarga qarshi kurashish uchun samarali vositalar mavjud: nafaqat an'anaviy tergov usullari, balki elektron pochtani aniqlash va ushlash, shuningdek, darknet bozorlarini kuzatish imkonini beruvchi dasturiy ta'minotlar va ishchi guruhlar mavjud. Bu yerda asosiy misollar sifatida "Yevropolning Darknet Tergov guruhi va kiberpatrullari"ni keltirish mumkin.

Yevropa Ittifoqining jinoyatchilikka qarshi kurash agentligi Yevropol darknetda jinoyatni tekshirishning yangi yondashuvini e'lon qildi – bu a'zo davlatlar huquqni muhofaza qilish organlari o'rtasida muvofiqlashtirish kuchayishini ko'rsatadi. Yevropolning ta'kidlashicha, maxsus darknetdagi jinoyatlarga qarshi kurashish guruhi internetda giyohvand moddalar savdosi, o'qotar qurollar va xakerlik xizmatlari va yashirin iqtisodiyot kabi noqonuniy faoliyatlar hajmini kamaytirish bo'yicha sa'y-harakatlarni amalga oshiradi. Lekin Yevropol ilgari ham Yevropa kiberjinoyatchilik markazi orqali muvaffaqiyatli operatsiyalarni amalga oshirib kelgan.

Biroq, Groshkovaning ta'kidlashicha, huquqni muhofaza qilish operatsiyalari orqali darknet bozorlariga qarshi kurash platformalardan birining, yoki bir nechtasining yopilishiga olib keladi, lekin bu foydalanuvchilar – sotuvchilar, xaridorlar va yetkazib beruvchilarning bir bozordan ikkinchisiga o'tishiga to'sqinlik qilmaydi. Jinoiy faoliyatni butunlay tugatish uchun sotuvchi va xaridorning xatti-harakatlarini ham to'xtatish kerak.[1]

Dark internetda uyushgan jinoyatchilikka qarshi yangi kurashdagi birinchi operatsiyalardan biri 2016-yil oktabr oyida bo'lib o'tdi. AQSh huquqni muhofaza qilish idoralari tashabbusi bilan "Besh ko'z" (Five Eyes Law Enforcement Group) huquqni muhofaza qilish guruhi (Avstraliya, Kanada, Yangi Zelandiya, Buyuk Britaniya va Qo'shma Shtatlar) va Yevropol a'zolari, "Hyperion" operatsiyasi maqsadi darknetdagi noqonuniy xizmatlar sotuvchilari va xaridorlariga qaratilgan.[2]

[1] E.W. Kruisbergen, "Criminal markets: the dark web, money laundering and counterstrategies - an overview of the 10th research conference on organized crime". – URL: https://www.researchgate.net/publication/332685663

[2] Department of Homeland Security, ICE, "Law Enforcement Agencies around the World Collaborate on International Darknet Marketplace Enforcement Operation," press release, October 31, 2016.

Bu operatsiya shunchaki boshlanishi edi va qaysidir ma‘noda uyushgan jinoyatchilikni tergov qilishning birinchi bosqichini aks ettirdi. Lekin bu kelgusida ushbu sohada jamoaviy ishlash va hamkorlikni kengaytirishni talab qiladi.

Kiberjinoyat olamida anonimlik texnologiyalari huquqni muhofaza qilish organlarining shaxslarni jinoiy xatti-harakatlar bilan bog‘lashiga yo‘l qo‘ymaydi va u kiberjinoiy guruhlarga qo‘lga olish yoki ta’qib qilinishdan qo‘rqmasdan ochiq faoliyat yuritish imkonini beradi.[1] Biroq, anonimlik o‘z-o‘zidan jinoiy xususiyatga ega emas va anonimlik texnologiyalari qonuniy funksiyalarga ega.

Darknetdagi jinoyatlar bo‘yicha tadqiqot ishi olib borgan Kristin darknet bozor tarmoqlariga qarshi kurashish uchun huquqni muhofaza qilish idoralari tomonidan qo‘llaniladigan strategiyalar ichida asosiy e’tiborni darknet veb-sahifalaridagi sotuvchilarga qaratish ko‘proq ta’sir ko‘rsatishi mumkinligini ta’kidlaydi.[2] Bu fikr olimlar Daksber va Hayne tomonidan ham mustahkamlangan, ular ham darknet tarmog‘idagi sotuvchilarga qarshi chora-tadbirlar ishlab chiqishni taklif qilishadi.[3]

Shunga qaramay, darknet bozorlardagi faollik so‘nggi yillarda doimiy sur’atda o‘sib bordi. Huquqni muhofaza qilish organlari uchun mutanosib holda platformalarning moslashib borayotganligi va tez rivojlanayotganligi, kelgusida ularning tekshiruvlarini yanada qiyinlashtirishi mumkin.[4]

Huquqni muhofaza qilish idoralari doimiy ravishda darknet bozorlariga faol aralashish uchun yangi yondashuvlar va strategiyalarni izlaydilar. Hozirda darknet platformalari o‘rniga darknetdagi sotuvchilarga qaratilgan strategiyalar muhokama mavzusidir.

---

[1] EC3 (2014, February 9). European Cybercrime Center (EC3) - First year report. Retrieved March 3, 2015, from URL: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report

[2] Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. archive:1207.7139 [cs]. arXiv: 1207.7139. Retrieved February 28, 2019, from URL: http://arxiv.org/abs/1207.7139

[3] Duxbury, S. W. & Haynie, D. L. (2018). The Network Structure of Opioid Distribution on a Darknet Cryptomarket. Journal of Quantitative Criminology, 34(4), 921{941.doi:10.1007/s10940-017-9359-4

[4] Paquet-Clouston, M., Decary-Hetu, D. & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. International Journal of Drug Policy, 54, 87{98.doi:10.1016/j.drugpo.2018.01.003

Tadqiqot ishlarining natijalaridan shuni ko‘rish mumkinki, bir darknet bozorida faol bo‘lgan sotuvchilarning qariyb 80 foizi boshqa darknet bozorlarida ham faol yoki ular ham bor. Demak, faqat asosiy nishonni darknet bozorlariga qaratish jinoyatni to‘liq oldini olmaydi. Huquq-tartibot idoralari o‘z faoliyat doirasini kengaytirishi va bir vaqtning o‘zida faqat darknet bozorlari bilan cheklanmasligi kerak.

Hozirki kunda o‘g‘irlangan yoki buzilgan hisob ma’lumotlari uchun proaktiv monitoring xizmatini taqdim etuvchi kompaniyalar mavjud. Xizmat “Dark Web”da o‘g‘irlangan ma’lumotlarni aniqlaganida mijozlarni ogohlantiradi. 2020-yil may oyi o‘rtalarida “ImmuniWeb” veb-xavfsizlik kompaniyasi bepul “ImmuniWeb Domain Security Test” xizmatini taqdim etdi, bu esa korxonalar va tashkilotlarga qorong‘u internetdagi zaifliklarini baholash imkonini beradi. Onlayn test kompaniya ma’lumotlari va hujjatlarini “Darknet”da mavjudligini aniqlash imkonini beradi. Yangi bepul xizmat “ImmuniWeb” domen xavfsizligi testiga integratsiya qilingan bo‘lib, u shuningdek, barcha turdagi tashkilotlar uchun domen nomini sotish, o‘g‘irlangan ma’lumot, karta raqamlari, savdo belgisi buzilishi va soxta ijtimoiy media akkauntlarini aniqlay oladi. Darknetda tashkilot o‘zining buzilgan hisob ma’lumotlari va o‘g‘irlangan hujjatlari haqida ma’lumot olish uchun URL veb-sayt manzilini kiritishi. “ImmuniWeb” ma’lumotlariga ko‘ra, sun’iy intellekt algoritmi xizmatga doimiy ravishda xakerlik forumlari, ajratilgan IRC kanallari, darknet bozorlari, “TelegramChat” kanallari va o‘g‘irlangan ma’lumotlar sotiladigan qorong‘u internet va oddiy internetdan qidirish imkonini beradi.[1]

Yana bir muhim holat shundaki, darknetdagi sotuvchilar ochiq forumlardan darknet bozorlarida o‘z ish faoliyatlarini oshirish uchun reklama sifatida foydalanishlari mumkin. Bu huquq-tartibot idoralari potentsial maqsadlar haqida ko‘proq ma’lumot to‘plash uchun ochiq forumlardagi ma’lumotlardan samarali foydalanishi mumkinligini ko‘rsatadi.

[1] Запущен бесплатный сервис для мониторинга наличия данных компании в даркнете. URL: https://www.tadviser.ru/index.php/ Статья:Даркнет_(теневой_интернет,_DarkNet)

Birlashgan Millatlar Tashkilotining 2014 yilgi hisobotiga ko‘ra, FQB tomonidan 2013-yil 1-oktyabrda o‘chirilishidan oldin, “Silk Road” darknet bozori noqonuniy faoliyati natijasida ikki yarim yil ichida taxminan 1,2 milliard dollar to‘plagan.[1] Federal qidiruv byurosining muvaffaqiyatiga qaramay, “Silk Road 2.0” birinchi platforma yopilishidan atigi ikki hafta o‘tib internetga paydo bo‘ladi va 2014-yil noyabr oyida YEVROPOL va FQB qo‘shma operatsiyasi chog‘ida o‘chirilgunga qadar bir yildan ko‘proq vaqt davomida faoliyat ko‘rsatgan.[2]

FBI tomonidan “Freedom Hosting” ishida qo‘llanilgan texnikalar “Silk Road”ni olib tashlash uchun qo‘llanilgan taktikalardan sezilarli darajada farq qilgani aytilgan.[3] Keyinchalik FQB xalqaro hamkorlik orqali “Freedom Hosting” serverlarini tortib olganini va Tor brauzerining ayrim versiyalarida nol kunlik zaiflikdan foydalanish uchun ularni qayta konfiguratsiya qilganini tan olgan. Ushbu zaiflik FQBga dasturni yashirin ravishda masofaviy mashinalarga o‘rnatishga imkon berdi, bu esa tizimlarning IP manzilini Vashington okrugidagi ma’lumotlar markaziga yuboradi.[4] Ushbu uslub mijoz darajasidagi faol kuzatuv choralarining eng intruzivini va hozirgi kunga qadar FBI tomonidan qo‘llanilgan aylanib o‘tish texnologiyalarini yengishning eng murakkab, eng tajovuzkor vositalarini ifodalaydi.

2014-yilda RAND korporatsiyasining “Kiberjinoyat vositalari va o‘g‘irlangan ma’lumotlar xakerlari bozori” nomli tadqiqotida aytilishicha, huquqni muhofaza qiluvchi tashkilotlar kiberjinoyatchilik bilan hamqadam bo‘lish uchun kurashayotgan bo‘lsa-da, huquqni muhofaza qilish organlari jinoiy ta’qiblar sonini ko‘paytirmoqda va

[1] United Nations Office on Drugs and Crime (UNODC). (2014, June 1). World drug report 2014. Retrieved September 9, 2014, from URL: http://www.unodc.org/wdr2014/

[2] Greenberg, A. (2014, November 5). Global web crackdown arrests 17, seizes hundreds of DarkNet domains. Retrieved November 8, 2014, from URL: http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

[3] Poulsen, K. (2013, September 13). FBI admits it controlled Tor servers behind mass malware attack. Retrieved September 9, 2014, from URL: http://www.wired.com/2013/09/freedomhosting-fbi/

[4] Poulsen, K. (2014, August 14). Visit the wrong website, and the FBI could end up in your computer. Retrieved August 22, 2014, from URL: http://www.wired.com/2014/08/operation_torpedo/

aybdorlarni qidirish usullarini takomillashtirmoqda.[1] O‘zgarishlarning asosiy kuchi sifatida hisobotda yangi texnologiyalar va xalqaro hamkorlikning kuchayishi haqidagi iqtibos keltiriladi, bu esa ekstraditsiya jarayonlari va kiberjinoyatchilarni ta‘qib qilishni osonlashtiradi. Hisobotga ko‘ra, butun dunyo hukumatlari tomonidan kiberjinoyatlarga yangi e’tibor qaratilishi bilan yaqin va yaqin kelajakda kiberjinoyatlarga qarshi kurashda sezilarli yaxshilanishlar bo‘ladi. 2014-yil 7-noyabrda RAND korporatsiyasi hisobotiga ko‘ra, 16 ta Yevropa davlati va Qo‘shma Shtatlar 414 ta noqonuniy “Tor” darknet domenlarini o‘chirib tashlagan keng qamrovli operatsiyani amalga oshirgan.[2] Lekin FQB va YEVROPOL vakillari serverlarni qanday topishga muvaffaq bo‘lganliklarini tushuntirishga kelganda, bu usullarni oshkor eta olmasliklarini aytishgan. Ammo, “Tor” himoyalangan brauzeri yaratuvchilardan biri, Endryu Lyuman, keyinchalik huquqni muhofaza qilish organlari shunchaki Bitkoin kriptavalyuta tranzaksiya izini topishga erishganliklarini va ular “Tor”ning shifrlash tizimini buzishga erisha olmaganliklarni aytib o‘tgan. Lyumanning qo‘shimcha qilishicha, 414 domen o‘chirilgan bo‘lsa-da, bu 27 tadan kamroq individual veb-saytlarni anglatadi va bu miqdor kam, shuning uchun 414 domenning olib tashlanishi rasmiylar tomonidan bor yo‘g‘i 17 nafar shaxsning hibsga olinganini bildirgan.[3]

Biz ko‘rib chiqayotgan virtual makonda hatto “aqlli texnologiyalar”dan foydalangan holda ham jinoiy guruhlar faoliyatini to‘xtatish mushkul. Buning sababi, shifrlangan “VPN” ulanish xizmatlari yordamida anonim “TOR” tarmog‘i ichki qonunchilikni buzuvchi internet resurslarini chetlab o‘tishadi. Ya’ni bu orqali foydalanuvchining IP-manzilini Rossiya qonunchiligi qo‘llanilmaydigan har qanday joyga almashtirish tufayli bajaradi. Binobarin, saytga so‘rov sud qaroriga binoan internet-provayderlar veb-saytga kirishni bloklagan Rossiya Federatsiyasi hududidan

[1] Ablon, L., & Libicki, M. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Washington DC: RAND Corporation.

[2] Greenberg, A. (2014, November 5). Global web crackdown arrests 17, seizes hundreds of Dark Net domains. Retrieved November 8, 2014, from URL: http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

[3] Lee, D. (2014, November 10). Dark Net raids 'overblown' – Tor. Retrieved December 10, 2014, from URL: http://www.bbc.com/news/technology-29987379

emas, balki xorijiy davlat hududidan, ya’ni soxta IP-manzil tegishli bo‘lgan serverdan kirayoganini ko‘rsatadi.

G‘arblik hamkasblar tajribasidan kelib chiqib shuni aytish mumkinki, onlayn jinoyatchilarni qo‘lga olishning asosiy usuli bu tezkor-qidiruv harakatlari bo‘lib, ular bilan bevosita aloqada bo‘lish va jinoyatchilar orasiga kirishdir.

Ba’zilar huquqni muhofaza qilish organlari jinoyatchilarning xatolari yoki texnologiyadagi kamchiliklarga tayanishi mumkin, deb taxmin qilishadi. Masalan, 2013-yilda “Silk Road” sayt operatorining noto‘g‘ri qadamlari FQB toonidan uning qo‘lga olishiga olib kelgan.[1]

“RAND Europe” tadqiqot instituti darknet tarmog‘i jinoyatlariga qarshi kurashning quyidagi asosiy usullarini ta’kidlaydi:

– Ochiq veb-saytlardan ma’lumotlar olish. Kiberjinoyatchilar darknetdan faqat jinoyat sodir etish uchun platforma sifatida foydalanadilar, lekin ko‘pincha ular jamoat tarmoqlarida e’lon berib mijozlar qidiradi. Qonunga ko‘ra, ommaviy saytlar egalari huquqni muhofaza qiluvchi organlarga har qanday noodatiy qiziqish uyg‘otadigan ma’lumotlarni taqdim etishlari kerak. Misol uchun, “Silk Road” darknet bozori veb-sahifasi egasi Ross Ulbricht aloqa qilish uchun ochiq internet tarmog‘ida o‘z elektron pochta manzilini qoldirgani kabi;

– Pochtani ushlash. Huquq-tartibot idoralari yetkazib beruvchi kompaniyalar va pochta bo‘limlari bilan hamkorlikda shubhali jo‘natmalarni tekshirishlari kerak. Huquq tartibot idoralari, shuningdek, oluvchini kuzatish uchun shubhali buyumning raqam belgisini ham olishi mumkin;

– Dasturiy ta’minot yaratish. Huquqni muhofaza qiluvchi oganlar katta hajmdagi ma’lumotlardan foydalanishga majbur, aks holda darknet jinoyatlarini ochish imkonsiz. Dasturiy ta’minot IP-manzillar va internetda joylashtirilgan ma’lumotlarni to‘playdi, xulosa chiqaradi va asta-sekin ular bo‘yicha tekshiruv olib borish mumkin bo‘ladi. Bu qimmat va murakkab tizim, lekin u o‘zini oqlaydi;

[1] Donna Leinwand Leger, “How FBI Brought Down Cyber-Underworld Site Silk Road,” USA Today, May 15, 2014.

– Pul oqimlarini kuzatish. Kriptovalyuta yuqori darajadagi himoyaga ega bo‘lsa-da, zaif nuqta uni sotib olish yoki sotishdir. Huquq tartibot idoralari birjalardan kriptovalyuta bilan kim va qachon operatsiyalarni amalga oshirganligi haqidagi ma’lumotlarni so‘rashi mumkin.[1]

Shunday qilib, ushbu hodisaning ijtimoiy xavfliligi aniq va profilaktika ishlari samaradorligini oshirishni talab qiladi. Darknet ijtimoiy tarmog‘ida jinoyatchilikka qarshi xalqaro kurash tahlili bizga darknet jinoyatchiligiga qarshi kurashning asosiy usullarini ishlab chiqish va ularni hayotga muvaffaqiyatli joriy etish imkonini beradi.

Davlatlarga virtual aktivlarga asoslangan noqonuniy moliyaviy oqimlar va jinoiy daromadlarni legallashtirish xavfiga qarshi kurashish uchun BMTning “Narkotiklar va jinoyatchilikka qarshi kurash boshqarmasi”, “Moliyaviy harakatlar bo‘yicha ishchi guruhi” (FATF) va shu kabi tashkilotlar bilan hamkorlik qilish tavsiya etiladi.

Kiberjinoyatchilar, an’anaviy jinoyatchilar kabi, asosan foyda uchun harakat qilishadi. Kiberjinoyatchilar Darkweb forumlari va bozorlarida jismoniy shaxslar va korxonalardan o‘g‘irlangan shaxsiy va moliyaviy ma’lumotlar bilan savdo qiladilar. Jinoyatchilar onlayn xizmatlarga kirish uchun o‘g‘irlangan hisob ma’lumotlaridan (foydalanuvchi nomlari va parollar kabi) foydalanadilar –darknetda ko‘pincha “PayPal” elektron hamyoni ma’lumotlari sotiladi.[2]

Rossiya fuqarosi 2018-yilda Tailandda Darknet “Infraud Organization” bozorini boshqargan va o‘g‘irlangan kredit karta ma’lumotlari va apparat vositalarini sotgani uchun hibsga olingan. Ushbu darknet bozorida butun dunyo bo‘ylab 4,3 milliondan ortiq kredit kartalari, debet kartalari va bank hisoblari bilan savdo qilgan 11 000 a’zo bor edi. Bu 530 million AQSh dollaridan ortiq yo‘qotishga olib kelgan.[3]

[1] Taking Stock of the Online Drugs Trade / S. Hoorens, K. Kruithof [et al.] // URL: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html (дата обращения: 23.04.2021).

[2] Here’s how much your credit card is now worth on the Dark Web. URL: https://www.komando.com/security-privacy/criminals-targeting-paypal/806650/

[3] “US indicts Russian cybercrime Dark Web market “Infraud Organization” suspect Sergey Medvedev, arrested in Thailand - CBS News.” [Online]. Available: URL: https://www.cbsnews.com/news/usrussia-cybercrime-dark-web-market-suspect-sergeymedvedev-thailand/. [Accessed: 10-Mar-2020].

Moliyaviy jinoyatlarga qarshi kurash tarmog'ining vazifasi moliyaviy tizimni noqonuniy foydalanishdan himoya qilish, jinoiy daromadlarni legallashtirish va u bilan bog‘liq jinoyatlarga, shu jumladan terrorizmga qarshi kurashish va moliya organlaridan strategik foydalanish hamda moliyaviy ma'lumotlarni to'plash, tahlil qilish va tarqatish orqali milliy xavfsizlikni ta'minlashdan iborat.

Darknet tarmog‘i sayt operatorlari va foydalanuvchilari, ayniqsa, agar ularning harakatlari noqonuniy bo‘lsa, o‘z shaxsini yashirish yoki noto‘g‘ri yo‘naltirish uchun barcha imkoniyatlarni ishga soladi. Darknet tarmog‘idagi eng yuqori darajadagi jinoyatchilar shaxsini aniqlash ko‘pincha bir nechta davlatlar ishtirokidagi xalqaro operatsiyalarni talab qiladi.

2019-yil mart oyi oxirida yashirin internet tarmog‘ida o‘z noqonuniy faoliyatini amalga oshirgan jinoyatchilar ommaviy hibsga olingani ma’lum bo‘ldi. “Computer Weekly” portalining Yevropol bayonotiga tayanib xabar berishicha, “SaboTor” deb nomlangan qo‘shma operatsiya doirasida turli mamlakatlar, jumladan, AQSh, Kanada va Yevropa huquq-tartibot idoralari 61 nafar shaxsni hibsga olgan va noqonuniy biznes yuritish uchun foydalanilgan 50 ta veb-servisni yopgan. Bundan tashqari, “SaboTor” operatsiyasi davomida 122 kishi so‘roq qilingan. Yevropol ijrochi direktori Ketrin De Bollening aytishicha, darknet tarmog‘i ko‘pchilik o‘ylaganchalik yashirin emas.[1]

Moliyaviy harakatlar bo‘yicha ishchi guruhi (FATF) moliyaviy jinoyatlarga qarshi global va asosiy qoidalarni haqida tavsiya berib keladi. Kriptovalyutalarni tartibga solish asosiy muammoga aylandi. Bu esa darknet olamida iqtiodiy jinoyatlarning o‘sishiga olib kelmoqda. Ishchi guruh moliyaviy jinoyatlarga qarshi kurash bo‘yicha xalqaro sa’y-harakatlarni rag‘batlantirish va muvofiqlashtirish uchun 39 a’zo davlatdan iborat. 2019-yilda FATF “Virtual aktivlar va virtual aktivlarga xizmat ko‘rsatuvchi provayderlar uchun xavfga asoslangan yondashuv bo‘yicha qo‘llanma” e’lon qildi.

Global yondashuv asosiy va muhim hisoblanadi, chunki moliyaviy kiberjinoyatlarning tarkibiy qismlarining aksariyati kibermakonning chegarasiz

[1] Массовые задержания пользователей теневого интернета. URL: https://www.tadviser.ru/index.php

xususiyatlaridan kelib chiqqan holda bir nechta yurisdiktsiyalarni o‘z ichiga oladi. Ushbu jinoyatlarga qarshi kurashish uchun qoidalar va xavfsizlik choralari imkon qadar ko‘proq mamlakatlar, shu jumladan, ushbu mamlakatlarda faoliyat yuritayotgan moliyaviy institutlar va virtual aktivlarga xizmat ko‘rsatish provayderlari tomonidan implemintatsiya qilinishi kerak.

Yuqaoridagi tavsiyalarni amalga oshirishda turli mamlakatlarning suvereniteti, ularning qonunchiligi, mahalliy sharoit va yurisdiktsiyalarga moslashuvchan munosabat o‘rtasida muvozanatni saqlash kabi jihatlarni ham e’tiborga olish kerak.

FATFning turli tavsiyalari, huquqni qo‘llash yondashuvlari asosida quyidagi chora-tadbirlar belgilandi. Ushbu chora-tadbirlar Milliy Standartlar va Texnologiyalar Instituti (NIST) kiberxavfsizlik tizimi tomonidan tizimlashtirilgan.[1] Bu choralar quyidagilardir:

– Mijozlarni tekshirish (CDD);

– Operatsion kiber xavfsizlik (OPSEC);

– Ma’lumotlarni uzatish va ochiq manbali razvedka (OSINT) qobiliyati;

– Shubhali tranzaksiya monitoringi;

– Jinoiy infratuzilmalarga aralashuv;

– Asossiz orttirilgan boylik tartibga solish (Unexplained Wealth Order) va virtual aktivlarni musodara qilish.

Ushbu profilaktika chorasi soxta anonimlik, pul o‘tkazmalari va tranzaksiyaga asoslangan pul yuvishga qarshi kurashish uchun amaliy identifikatorlarini joriy qiladi. Bu, shuningdek, potentsial qonun va tartibga solishni osonlashtiradi. Ushbu tekshiruvlar noqonuniy moliyaviy oqimlarga qarshi kurashish bo'yicha moliya sanoatining asosiy faoliyatini tashkil qiladi. Virtual aktivlarga xizmat ko‘rsatish provayderlarini mijozlarning tekshirishi muhim profilaktika chorasidir, chunki jinoyatchilar operatsiyalar va to‘lovlarda anonim bo‘lib qolibga harakat qilishadi.

[1] Project Participate, December 2019, URL: https://www.thecryptoupdates.com/coalition-of-major-stakeholders-incryptocurrency-industry-issues-report-on-indicators-of-suspicious-activity/

“Dark Web Monitor” – bu CFLWning (Cyber Field and Law Enforcement) tekshiruv xizmati. CFLW kiberxavfsizlik va huquqni muhofaza qilish sohalarida 10 yildan ortiq tajribaga ega doktor Mark van Staalduinen tomonidan asos solingan. Doktor Mark van Staalduinen xavfsizlik ehtiyojlari va texnik tadqiqot asoslari o‘rtasidagi bo‘shliqni to‘ldirish maqsadida CFLWga asos solgan. CFLW tekshiruv xizmatlari “Dark Web Monitor va Virtual Assets” (Cryptocurrencies) tahlillarini uzoq muddat davomida to‘plangan ma’lumotlar asosida tavsiyalar ishlab chiqadi. “Dark Web Monitor” (DWM) ochiq manbali razvedka (OSINT) platformasi bo‘lib, u Dark Web va virtual aktivlardan foydalanish natijasida kelib chiqadigan jinoiy va firibgarlik faoliyati haqida strategik tushuncha va operatsion istiqbollarni taqdim etadi. Strategik tushunchalar va operativ istiqbollar tergovchilar uchun yangi tergov usullarini taqdim etadi va xavfsiz kibermakonga yo‘l ochadi. 2019-yil noyabr oyida Niderlandiya Amaliy Ilmiy Tadqiqotlar Tashkiloti (TNO) va Niderlandiya va Singapurda joylashgan “CyberDevOps” (CDO) kompaniyasi “Dark Web Monitor”ni xizmat sifatida litsenziyalashga kelishib oldilar. Litsenziya shartnomasi shartlariga ko‘ra, Kiber maydon va huquqni muhofaza qilish tashkiloti (CDO) “Dark Web Monitor” xizmatini huquqni muhofaza qilish idoralari, xavfsizlik tashkilotlari va kompaniyalari doirasiga yetkazib beradi.

Tahdidlarga qarshi kurashish TNO tashkilotining Milliy xavfsizlik bo‘yicha direktori Krishna Taneja shunday dedi: “Texnologiya bizning dunyomizni tez o‘zgartirmoqda va jinoyatchilar Dark Web kabi yangi imkoniyatlarni tez o‘zlashtirishdi. Bu yangi tahdidlarni keltirib chiqaradi. Ushbu tahdidlarga qarshi turish uchun innovatsiyalar talab qilinadi. “Dark Web Monitor” – Adliya va xavfsizlik vazirligining innovatsion dasturida o‘z kelib chiqishini topadigan bunday innovatsiyaning yorqin namunasidir. Ushbu yechim manfaatdor tomonlarimiz, jumladan, huquqni muhofaza qilish organlari, bir nechta banklar va xavfsizlik tashkilotlarining keng ko‘lamli talablari bilan belgilanadi. Kiber maydon va huquqni muhofaza qilish tashkiloti bilan ushbu hamkorlik “Dark Web Monitor”ni bizning

manfaatdor tomonlarimizga arzon xizmat sifatida taqdim etiladigan operativ va yaxshi ta’minlangan yechimga aylantirish imkonini beradi”.[1]

Kelajakda tashkilot direktori va hammuassisi janob Erre Roelevink shunday dedi: “Ushbu tashkilot huquqni muhofaza qilish va xavfsizlik dasturlari va vositalariga qaratilgan kiberxavfsizlik yechimi provayderidir. “Dark Web Monitor” Dark Web jinoyatlarini tadqiq qilish va tergov qilish kerak bo‘lgan huquqni muhofaza qilish organlari va xavfsizlik mutaxassislari uchun ajralmas vosita bo‘ladi.”[2]

Xulosa qilib aytganda, anonimlik uchun ilg‘or texnologiyalar tufayli kuzatilishi qiyin bo‘lgan noqonuniy faoliyat platformasi bo‘lgan darknetda jinoiy faoliyatni kuzatish va unga qarshi kurashish muammolari yetarli. “Silk Road” darknet bozori FQB tomonidan muvaffaqiyatli amalga oshirilgan operatsiyaning namunasi sifatida ta’kidlash mumkin, ammo keyingi saytlar huquqni muhofaza qilish organlarining sa’y-harakatlariga qaramay paydo bo‘lishda davom etmoqda va faol bo‘lib qolmoqda. Yangi texnologiyalardan foydalanish va xalqaro hamkorlikning kuchayishi kiberjinoyatlarga qarshi kurashni yaxshilashning kaliti sifatida qaralmoqda, biroq onlayn jinoyatchilarni ushlash hali ham qiyin. Tezkor qidiruv faoliyati va jinoyatchilar bilan to‘g‘ridan-to‘g‘ri aloqa qilish darknet jinoyatiga qarshi kurashning samarali usullari bolishi mumkin. Shuningdek, kiberjinoyatchilarni kuzatish uchun ochiq veb-saytlar va ijtimoiy tarmoqlardan ma’lumot olish muhimligini ham qayd etib o‘tish joizdir.

[1] TNO licenses Dark Web Monitor to CyberDevOps. URL: https://cflw.com/2019/11/13/tno-licenses-dark-web-monitor-to-cyberdevops/
[2] TNO licenses Dark Web Monitor to CyberDevOps. URL: https://cflw.com/2019/11/13/tno-licenses-dark-web-monitor-to-cyberdevops/

References:

1. E.W. Kruisbergen, “Criminal markets: the dark web, money laundering and counterstrategies - an overview of the 10th research conference on organized crime”. – URL: https://www.researchgate.net/publication/332685663

2. Department of Homeland Security, ICE, “Law Enforcement Agencies around the World Collaborate on International Darknet Marketplace Enforcement Operation,” press release, October 31, 2016.

3. EC3 (2014, February 9). European Cybercrime Center (EC3) - First year report. Retrieved March 3, 2015, from URL: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report

4. Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. archive:1207.7139 [cs]. archive: 1207.7139. Retrieved February 28, 2019, from URL: http://arxiv.org/abs/1207.7139

5. Duxbury, S. W. & Haynie, D. L. (2018). The Network Structure of Opioid Distribution on a Darknet Cryptomarket. Journal of Quantitative Criminology, 34(4), 921{941.doi:10.1007/s10940-017-9359-4

6. Paquet-Clouston, M., Decary-Hetu, D. & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. International Journal of Drug Policy, 54, 87{98.doi:10.1016/j.drugpo.2018.01.003

7. Запущен бесплатный сервис для мониторинга наличия данных компании в даркнете. URL: https://www.tadviser.ru/index.php/Статья:Даркнет_(теневой_интернет,_DarkNet)

8. United Nations Office on Drugs and Crime (UNODC). (2014, June 1). World drug report 2014. Retrieved September 9, 2014, from URL: http://www.unodc.org/wdr2014/

9. Greenberg, A. (2014, November 5). Global web crackdown arrests 17, seizes hundreds of DarkNet domains. Retrieved November 8, 2014, from URL: http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

10. Poulsen, K. (2013, September 13). FBI admits it controlled Tor servers behind mass malware attack. Retrieved September 9, 2014, from URL: http://www.wired.com/2013/09/freedomhosting-fbi/

11. Ablon, L., & Libicki, M. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Washington DC: RAND Corporation.

12. Greenberg, A. (2014, November 5). Global web crackdown arrests 17, seizes hundreds of Dark Net domains. Retrieved November 8, 2014, from URL: http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

13. Lee, D. (2014, November 10). Dark Net raids 'overblown' – Tor. Retrieved December 10, 2014, from URL: http://www.bbc.com/news/technology-29987379

14. Donna Leinwand Leger, "How FBI Brought Down Cyber-Underworld Site Silk Road," USA Today, May 15, 2014.

15. Taking Stock of the Online Drugs Trade / S. Hoorens, K. Kruithof [et al.] // URL: https://www.rand.org/ randeurope/research/projects/online-drugs-tradetrafficking .html (дата обращения: 23.04.2021).

16. Here's how much your credit card is now worth on the Dark Web. URL: https://www.komando.com/security-privacy/criminals-targeting-paypal/806650/

17. "US indicts Russian cybercrime Dark Web market "Infraud Organization" suspect Sergey Medvedev, arrested in Thailand - CBS News." [Online]. Available: URL: https://www.cbsnews.com/news/usrussia-cybercrime-dark-web-market suspect-sergeymedvedev-thailand/. [Accessed: 10-Mar-2020].

18. Массовые задержания пользователей теневого интернета. URL: https://www.tadviser.ru/index.php

19. Project Participate, December 2019, URL: https://www. thecryptoupdates.com/coalition-of-major-stakeholders-incryptocurrency-industry-issues-report-on-indicators-of-suspicious-activity/

20. TNO licenses Dark Web Monitor to CyberDevOps. URL: https://cflw.com/2019/11/13/tno-licenses-dark-web-monitor-to-cyberdevops/