KIBERXAVFSIZLIK SOHASIDA VUJUDGA KELAYOTGN MUAYYAN TURDAGI JINOYATLARNING SODIR ETILISH MEXANIZMI VA O'ZIGA XOS XUSUSIYATLARI

Muallif : Maxmudov Otabek Rustam uli

Kalit so'zlar: kiberjinoyat , Kiber firibgarlik, kibero'g'irlik, profilaktik choralar, oldini olish

Annotatsiya

Ushbu maqolda kibermakona sodir etilayotgan muayyan turdagi jinoyatlarning sodir etilish mexanizmlari ularnind sodir etilish usullari , kivermakondagi jinoyatlar sodir etgan shaxslarning xususiytalari , jinoyatning belgilari , kiberjinoyatlarning oldini olish usullari , kiberjinoyatlarga qarshi kurashish yuzasidan yuzaga kelayotgan muammolar va yechimlar keltirib o'tiladi.

Annotation

In this article, the mechanisms of certain types of crimes committed in cyberspace, their methods of commission, characteristics of persons who commit crimes in cyberspace, signs of crime, methods of prevention of cybercrimes, problems and solutions arising in the fight against cybercrimes are mentioned.

Kiberjinoyat — kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi[1][2]. Kompyuter jinoyat paytida maqsadli yo'naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi[3][4].

Maxfiy ma'lumotlar qonuniy tarzda himoyalangan holatda yuz beruvchi kiberjinoyatlar bilan bog'liq ko'pgina jinoyatlar mavjud. Xalqaro miqyosda hukumat ham, nodavlat subyektlar ham kiberjinoyatlar, jumladan, josuslik, moliyaviy o'g'irlik va boshqa transchegaraviy jinoyatlar bilan shug'ullanadi. Xalqaro chegaralarni kesib o'tuvchi va kamida bitta milliy davlatning xatti-harakatlarini o'z ichiga olgan kiberjinoyatlar ba'zan kiberurush deb ataladi. Uorren Baffet kiberjinoyatni „insoniyatning birinchi raqamli muammosi"[5] deb ta'riflaydi va „insoniyat uchun real xavf tug'diradi", deya qo'shimcha qilib o'tadi[6].

2014-yilda chop etilgan hisobotda (McAfee homiyligida) jahon iqtisodiyotiga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan[7]. Cybersecurity Ventures tomonidan 2016-yilgi hisobotda kiberjinoyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha, 2025-yilga kelib esa 10,5 trillion dollargacha ko'tarilishi bashorat qilingan edi[8].

2012-yilda AQShda onlayn kredit va debet kartalaridagi firibgarlik oqibatida taxminan 1,5 milliard dollar yo'qotilgan[9] 2018-yilda Strategik va xalqaro tadqiqotlar

markazi (CSIS) tomonidan McAfee bilan hamkorlikda o‘tkazilgan tadqiqot shuni ko‘rsatadiki, har yili global YaIMning qariyb bir foizi, ya’ni 600 milliard dollarga yaqini kiberjinoyatlar tufayli yo‘qoladi[10]. Jahon Iqtisodiy Forumi 2020 Global Risk hisobotida uyushgan kiberjinoyatlar idoralari jinoiy faoliyatni onlayn qilish uchun kuchlarni birlashtirayotganini tasdiqladi, shu bilan birga ularning aniqlash va jinoiy javobgarlikka tortilish ehtimoli AQShda 1 foizdan kamroqni tashkil qiladi[11].

Tasniflashi[tahrir | manbasini tahrirlash]

An’anaviy jinoyatchilikning kamayishi bilan global hamjamiyatlar kiberjinoyatlarning muntazam o‘sishiga guvoh bo‘lishda davom etmoqda[12]. Kiberjinoyat moliyaviy jinoyatlardan tortib firibgarlikgacha, kiberpornografik savdo va reklama firibgarliklari orqali keng ko‘lamli faoliyatni o‘z ichiga oladi[13][14].

Moliyaviy firibgarlik jinoyatlari[tahrir | manbasini tahrirlash]

Kompyuter firibgarligi — bu boshqa shaxsni yo‘qotishga olib keladigan biror narsa qilish yoki qilmaslikka imkon berish uchun haqiqatni har qanday noto‘g‘ri ko‘rsatish. Shu nuqtai nazardan, firibgarlik quyidagi yo‘llar bilan foyda olishga olib keladi:

- Ruxsatsiz tarzda o‘zgartirish. Bu kichik texnik tajribani talab qiladi va xodimlar tomonidan ma’lumotlarni kiritish yoki noto‘g‘ri ma’lumotlarni kiritishdan oldin ma’lumotlarni o‘zgartirish yoki ruxsatsiz ko‘rsatmalar kiritish yoki ruxsat etilmagan jarayonlardan foydalanish orqali o‘g‘irlashning keng tarqalgan shaklidir;
- Odatda ruxsatsiz tranzaktsiyalarni yashirish uchun chiqishni o‘zgartirish, yo‘q qilish, bostirish yoki o‘g‘irlash. Buni aniqlash qiyin;
- Saqlangan ma’lumotlarni o‘zgartirish yoki o‘chirish[15].

Boshqa firibgarlik shakllari kompyuter tizimlari yordamida osonlashtirilishi mumkin, jumladan bank firibgarligi, karding, shaxsni o‘g‘irlash, tovlamachilik va maxfiy ma’lumotlarni o‘g‘irlash. Ushbu turdagi jinoyatlar ko‘pincha shaxsiy ma’lumotlar yoki pul ma’lumotlarining yo‘qolishiga olib keladi.

Kiberterrorchilik[tahrir | manbasini tahrirlash]

Asosiy maqola: Kiberterrorchilik

Hukumat amaldorlari va axborot texnologiyalari xavfsizligi bo‘yicha mutaxassislar 2001-yil boshidan buyon Internet muammolari va server firibgarliklarining sezilarli darajada oshganini hujjatlashtirdi. Federal Qidiruv Byurosi (FQB) va Markaziy razvedka boshqarmasi (CIA) kabi hukumat idoralari orasida bunday bosqinlar kiberterroristik tashqi razvedka xizmatlari yoki boshqa guruhlar tomonidan potentsial xavfsizlik teshiklarini xaritalash uchun uyushtirilgan sa’y-harakatlarning bir qismi ekanligidan xavotir ortib bormoqda. muhim tizimlar.[16] Kiberterrorchi — bu hukumat yoki tashkilotni kompyuterlar, tarmoqlar yoki ularda saqlangan ma’lumotlarga qarshi kompyuter hujumi uyushtirish orqali

o‘zining siyosiy yoki ijtimoiy maqsadlariga erishish uchun qo‘rqitadigan yoki majburlaydigan shaxs.

Kiberterrorizm, umuman olganda, kibermakon yoki kompyuter resurslaridan foydalanish orqali sodir etilgan terrorchilik harakati sifatida ta’riflanishi mumkin (Parker 1983). Shunday qilib, bayram kunlarida bombali hujumlar sodir bo‘lishi haqida Internetda oddiy targ‘ibot materiali kiberterrorizm deb hisoblanishi mumkin. Shuningdek, ayrim shaxslarga, oilalarga qaratilgan, tarmoqlar ichida guruhlar tomonidan tashkil etilgan, odamlar o‘rtasida qo‘rquv uyg‘otish, hokimiyatni namoyish etish, odamlar hayotini barbod qilish uchun zarur bo‘lgan ma’lumotlarni to‘plash, talonchilik, shantaj va hokazolarga qaratilgan xakerlik faoliyati ham mavjud[17].

Kiber tovlamachilik[tahrir | manbasini tahrirlash]

Kiber tovlamachilik veb-sayt, elektron pochta serveri yoki kompyuter tizimi zararli xakerlar tomonidan qayta-qayta xizmat ko‘rsatishni rad etish yoki boshqa hujumlarga duchor bo‘lganda yoki tahdid qilinganda sodir bo‘ladi. Bu xakerlar hujumlarni to‘xtatish va „himoya“ taklif qilish evaziga pul talab qiladi. Federal Qidiruv Byurosiga ko‘ra, kiberjinoyat tovlamachilar korporativ veb-saytlar va tarmoqlarga tobora ko‘proq hujum qilmoqda, ularning ishlash qobiliyatiga putur etkazmoqda va xizmatlarini tiklash uchun to‘lovlarni talab qilmoqda. Har oy FQBga 20 dan ortiq holatlar haqida xabar beriladi va jabrlanuvchining ismini jamoatchilikka oshkor qilmaslik uchun ko‘plari xabar qilinmaydi. Jinoyatchilar odatda tarqatilgan xizmatni rad etish hujumidan foydalanadilar[18]. Biroq, boshqa kiber tovlamachilik usullari mavjud, masalan, doksing tovlamachilik va hasharotlar brakonerligi.

Ransomware — bu zararli dastur fayllarga kirishni cheklash uchun foydalaniladigan, ba’zida to‘lov to‘lanmasa, ma’lumotlarni doimiy ravishda o‘chirib tashlash bilan tahdid qiladigan kiberto‘plashning bir turi. Kapersky Lab 2016 Security Bulletin hisobotiga ko‘ra, biznes har 40 daqiqada Ransomware qurboni bo‘ladi[19]. 2021-yilda har 11 daqiqada biznesga hujum qilishni bashorat qilgan. Ransomware dunyodagi eng tez o‘sib borayotgan kiberjinoyatlardan biri bo‘lib qolmoqda, 2021-yilda Ransomware global zarari 20 milliard dollargacha tushishi taxmin qilinmoqda[20].

Kiberpornografik savdo[tahrir | manbasini tahrirlash]

Asosiy maqola: Kiberseksual savdo

Kiberpornografik savdo — bu qurbonlarni tashish, keyin esa veb-kamerada majburan jinsiy harakatlar va yoki zo‘rlashning jonli translyatsiyasidir[21][22][23][24]. Jabrlanuvchilar o‘g‘irlanadi, tahdid qilinadi yoki aldanib, „kiberseksiz uylariga“ o‘tkaziladi[25][26][27]. Uyalar kiberseks savdogarlari internetga ulangan kompyuter, planshet yoki telefonga ega bo‘lgan har qanday joyda bo‘lishi mumkin[23]. Jinoyatchilar ijtimoiy media tarmoqlari, videokonferentsiyalar, tanishuv sahifalari, onlayn chat xonalari, ilovalar, qorong‘u veb- saytlar[28] va boshqa platformalardan foydalanadilar[29]. Ular o‘z shaxsini yashirish uchun onlayn to‘lov

tizimlari[28][30][31] va kriptovalyutalardan foydalanadilar[32]. Har yili uning paydo bo‘lishi haqida millionlab hisobotlar hokimiyatga yuboriladi[33]. Ushbu turdagi kiberjinoyatlarga qarshi kurashish uchun yangi qonunchilik va politsiya tartiblari zarur[34].

Kiberseks savdosiga misol sifatida Janubiy Koreyada 2018-2020-yillardagi N-xona ishi hodisasini keltirsa bo‘ladi[35].

Kiberurush turlari[tahrir | manbasini tahrirlash]

AQSh Mudofaa vazirligi so‘nggi paytlarda geostrategik ahamiyatga ega bo‘lgan bir qancha voqealar tufayli kibermakon milliy darajadagi tashvishga aylanganini ta’kidlaydi. Ular orasida 2007-yilda Estoniya infratuzilmasiga rossiyalik xakerlar tomonidan qilingan hujum ham kiradi. 2008-yil avgust oyida Rossiya yana Gruziya davlatiga qarshi muvofiqlashtirilgan va sinxronlashtirilgan kinetik va kinetik bo‘lmagan kampaniyada yana kiberhujumlar uyushtirgani da’vo qilingan. Bunday hujumlar milliy davlatlar o‘rtasidagi kelajakdagi urushlarda odatiy holga aylanishi mumkinligidan qo‘rqib, kiberkosmik operatsiyalar tushunchasi ta’sir qiladi va kelajakda jangovar harbiy qo‘mondonlar tomonidan moslashtiriladi[36].

Kompyuterga yo‘naltirilgan[tahrir | manbasini tahrirlash]

Bu jinoyatlar tanlangan jinoyatchilar guruhi tomonidan sodir etiladi. Kompyuterni qurol sifatida ishlatadigan jinoyatlardan farqli o‘laroq, bu jinoyatlar aybdorlarning texnik bilimlarini talab qiladi. Shunday qilib, texnologiya rivojlanishi bilan jinoyatning tabiati ham o‘zgaradi. Bu jinoyatlar nisbatan yangi bo‘lib, kompyuterlar mavjud bo‘lgan vaqtdan beri mavjud bo‘lib, bu jamiyat va umuman dunyo ushbu jinoyatlarga qarshi kurashga qanchalik tayyor emasligini tushuntiradi. Internetda har kuni sodir bo‘ladigan ko‘plab jinoyatlar mavjud. Bu kamdan-kam hollarda yolg‘izlar tomonidan amalga oshiriladi, buning o‘rniga u katta sindikat guruhlarini o‘z ichiga oladi.

Asosan kompyuter tarmoqlariga qaratilgan jinoyatlarga quyidagilar kiradi:

- Kompyuter viruslari
- Xizmatni rad etish hujumlari
- Zararli dastur (zararli kod)

Kompyuter vosita sifatida[tahrir | manbasini tahrirlash]

Agar shaxs kiberjinoyatning asosiy maqsadi bo‘lsa, kompyuterni maqsad emas, balki vosita sifatida ko‘rish mumkin. Bu jinoyatlar odatda kamroq texnik tajribani o‘z ichiga oladi. Insonning zaif tomonlari odatda foydalaniladi. Yetkazilgan zarar asosan psixologik va nomoddiy bo‘lib, variantlarga nisbatan qonuniy choralar ko‘rishni qiyinlashtiradi. Bu oflayn dunyoda asrlar davomida mavjud bo‘lgan jinoyatlardir. Firibgarlik, o‘g‘irlik va shunga o‘xshash narsalar yuqori texnologiyali uskunalar rivojlanishidan oldin ham mavjud edi. Xuddi shu jinoyatchiga oddiygina

vosita berilgan, bu ularning potentsial jabrlanuvchilar hajmini oshiradi va ularni izlash va ushlashni qiyinlashtiradi[37].

- Firibgarlik va shaxsiy ma'lumotlarni o'g'irlash (garchi bu zararli dasturlar, xakerlik yoki fishingdan tobora ko'proq foydalansa ham, bu „kompyuter maqsad sifatida" va „kompyuter vosita sifatida" jinoyatlariga misol bo'ladi)
- Axborot urushi
- Firibgarlik
- Spam
- Noqonuniy odobsiz yoki haqoratli kontentni, jumladan, ta'qib va tahdidlarni targ'ib qilish

Tijoriy maqsadlarda (spam) ommaviy elektron pochta xabarlarini so'ralmagan holda yuborish ba'zi yurisdiktsiyalarda noqonuniy hisoblanadi.

Fishing asosan elektron pochta orqali tarqaladi. Fishing elektron pochta xabarlarida zararli dasturlardan ta'sirlangan boshqa veb-saytlarga havolalar bo'lishi mumkin.[38] Yoki ular shaxsiy hisob ma'lumotlarini o'g'irlash uchun foydalaniladigan soxta onlayn-banking yoki boshqa veb-saytlarga havolalarni o'z ichiga olishi mumkin.

Behayo yoki haqoratomuz kontent[tahrir | manbasini tahrirlash]

Veb-saytlar va boshqa elektron xabarlar mazmuni turli sabablarga ko'ra yoqimsiz, odobsiz yoki haqoratli bo'lishi mumkin. Ba'zi hollarda bu xabarlar noqonuniy bo'lishi mumkin.

Ushbu aloqalarning noqonuniyligi darajasi mamlakatlar o'rtasida va hatto davlatlar ichida katta farq qiladi. Bu sudlar kuchli e'tiqodga ega bo'lgan guruhlar o'rtasida hakamlik muhokamasida ishtirok etishi mumkin bo'lgan nozik sohadir.

Internet pornografiyasining bir sohasi cheklash bo'yicha eng kuchli sa'y-harakatlarning maqsadi bo'lgan bolalar pornografiyasi bo'lib, u dunyoning aksariyat yurisdiktsiyalarida noqonuniy hisoblanadi. Debarati Xolder va K.Jaishankar yana gender nuqtai nazaridan kiberjinoyatni ta'riflab, „ayollarga qarshi kiberjinoyat"ni „Internet va mobil telefonlar kabi zamonaviy telekommunikatsiya tarmoqlaridan foydalangan holda jabrlanuvchiga qasddan psixologik va jismoniy zarar yetkazish maqsadida ayollarga qarshi qaratilgan jinoyatlar" deb ta'riflaydilar[39].

Reklama firibgarligi[tahrir | manbasini tahrirlash]

Reklama firibgarliklari, ayniqsa, kiberjinoyatchilar orasida mashhurdir, chunki bunday firibgarliklar jinoiy javobgarlikka tortilish ehtimoli kamroq va ayniqsa, daromad keltiruvchi kiberjinoyatlardir[40].Sorbonna biznes maktabi professori Jan-Lup Richet kiberjinoyatchilar hamjamiyatlarida kuzatilgan reklama firibgarliklarining ko'p turlarini uchta toifaga ajratdi: (1) shaxsiy ma'lumotlar bilan bog'liq firibgarlik; (2) atribut firibgarligi; va (3) reklama-firibgarlik xizmatlari[41].

Identifikatsiya firibgarligi haqiqiy foydalanuvchilarni taqlid qilish va tomoshabinlar sonini oshirishga qaratilgan. Bir nechta reklama firibgarlik usullari ushbu turkumga

tegishli bo‘lib, botlardan (xosting kompaniyasi yoki ma’lumotlar markazidan yoki buzilgan qurilmalardan kelgan) trafikni o‘z ichiga oladi; pechene to‘ldirish; joylashuv va brauzer turi kabi foydalanuvchi xususiyatlarini soxtalashtirish; soxta ijtimoiy trafik (ijtimoiy tarmoqlarda foydalanuvchilarni e’lon qilingan veb-saytga kirishda adashtirish); va botni yanada qonuniy ko‘rinishga keltirish uchun soxta ijtimoiy signallarni yaratish, masalan, Twitter yoki Facebook akkauntini ochish.

Muvaffaqiyatli reklama-firibgarlik kampaniyasi reklama firibgarligining ushbu uch turining murakkab kombinatsiyasini o‘z ichiga oladi — soxta ijtimoiy akkauntlar va soxtalashtirilgan cookie-fayllar yordamida botlar orqali soxta trafik yuborish; botlar mashhur brendni soxtalashtiruvchi firibgarlar sahifasida mavjud bo‘lgan reklamalarni bosadi.

Kompyuter jinoyatlariga qarshi kurash[tahrir | manbasini tahrirlash]

Transchegaraviy hujumlarni qo‘llab-quvvatlash uchun internetdan foydalanishlari sababli kiberjinoyatchilarni topish va ularga qarshi kurashish qiyin. Internet nafaqat odamlarni turli joylardan nishonga olishga imkon beradi, balki etkazilgan zarar ko‘lamini oshirishi mumkin. Kiber jinoyatchilar bir vaqtning o‘zida bir nechta odamni nishonga olishlari mumkin. Davlat va xususiy sektorlar uchun virtual maydonlarning[42] mavjudligi kiberjinoyatlarning kundalik hodisaga aylanishiga imkon berdi[43]. 2018- yilda Internetdagi jinoyatlar bo‘yicha shikoyat markaziga kiberjinoyatlar bo‘yicha 351 937 ta murojaat kelib tushdi, bu esa 2,7 milliard dollar yo‘qotishga olib keldi[44].

Tekshiruv[tahrir | manbasini tahrirlash]

Kompyuter dalil manbai bo‘lishi mumkin (qarang, raqamli sud tibbiyoti). Agar kompyuter jinoiy maqsadlarda bevosita foydalanilmasa ham, u jurnal fayli ko‘rinishida jinoiy tergovchilar uchun qimmatli yozuvlarni o‘z ichiga olishi mumkin. Ko‘pgina mamlakatlarda[45] Internet-provayderlar qonunga ko‘ra, o‘zlarining log-fayllarini oldindan belgilangan vaqt davomida saqlashlari shart. Masalan; Yevropa bo‘ylab ma’lumotlarni saqlash direktivasi (barcha Yevropa Ittifoqiga a’zo davlatlar uchun amal qiladi) barcha elektron pochta trafigini kamida 12 oy davomida saqlanishi kerakligini ta’kidlaydi.

> Kiberjinoyatning sodir bo‘lishining ko‘plab usullari mavjud va tergov odatda IP-manzil izidan boshlanadi, ammo bu detektivlar ishni hal qilishlari mumkin bo‘lgan faktik asos bo‘lishi shart emas. Yuqori texnologiyali jinoyatlarning har xil turlari, shuningdek, past texnologiyali jinoyatlar elementlarini ham o‘z ichiga olishi mumkin va aksincha, kiber jinoyatlar bo‘yicha tergovchilarni zamonaviy huquqni muhofaza qilish organlarining ajralmas qismiga aylantiradi. Kiberjinoyatlar bo‘yicha detektiv ish usullari, yopiq politsiya bo‘linmalarida yoki xalqaro hamkorlik doirasida bo‘lsin, dinamik va doimiy ravishda takomillashtiriladi[46].

Senator Tommi Tubervil 2021- yilda Alabama shtatining Guver shahridagi Milliy kompyuter sud-tibbiyot institutiga tashrif buyurmoqda.

AQShda Federal qidiruv byurosi (FQB)[47] va Milliy xavfsizlik departamenti (DHS)[48] kiberjinoyatlarga qarshi kurashuvchi davlat idoralari hisoblanadi. FQB kiberjinoyatchilik bo‘yicha o‘qitilgan agentlar va tahlilchilarni o‘z idoralari va shtab-kvartiralarida joylashtirgan[47]. DHSga ko‘ra, Maxfiy xizmatda moliyaviy kiber jinoyatlarni nishonga olish uchun ishlaydigan kiber razvedka bo‘limi mavjud. Ular o‘zlarining razvedka ma’lumotlaridan xalqaro kiberjinoyatlardan himoyalanish uchun foydalanadilar. Ularning sa’y-harakatlari banklar kabi muassasalarni tajovuzlardan va axborot buzilishidan himoya qilishga qaratilgan. Alabama shtatida joylashgan Maxfiy xizmat va Alabama prokuratura idorasi Milliy kompyuter sud ekspertizasi institutini yaratish orqali huquqni muhofaza qilish sohasida mutaxassislarni tayyorlash uchun birgalikda ishlaydi[48][49][50]. Ushbu institut „huquqni muhofaza qilish hamjamiyatining davlat va mahalliy a’zolarini kiber hodisalarga javob berish, tergov va sud-tibbiyot ekspertizasi, kiber hodisalarga javob berish, tergov va sud-tibbiy ekspertiza bo‘yicha treninglar bilan ta’minlash“ uchun ishlaydi[50].

Kiberjinoyatchilar tomonidan ularning shaxsini va joylashuvini yashirish uchun shifrlash va boshqa usullardan keng tarqalgan foydalanish tufayli, jinoyat sodir etilganidan keyin jinoyatchini izlash qiyin bo‘lishi mumkin, shuning uchun oldini olish choralari juda muhimdir[51][52].

Ogohlik[tahrir | manbasini tahrirlash]

Texnologiya taraqqiyoti va ko‘proq odamlar bank yoki kredit karta ma’lumotlari kabi nozik ma’lumotlarni saqlash uchun internetga tayanishi sababli, jinoyatchilar bu ma’lumotlarni o‘g‘irlashga harakat qilmoqdalar. Kiberjinoyat butun dunyo bo‘ylab odamlar uchun ko‘proq xavf tug‘dirmoqda. Axborot qanday himoyalanganligi va jinoyatchilar ushbu ma’lumotni o‘g‘irlash uchun qo‘llaydigan taktikalar haqida xabardorlikni oshirishning ahamiyati ortib bormoqda. 2014-yilda FQBning Internetdagi jinoyatlar bo‘yicha shikoyat markazi ma’lumotlariga ko‘ra, 269 422 ta shikoyat kelib tushgan. Barcha da’volar jamlanganda 800 492 073 dollar zarar ko‘rgan[53]. Ammo kiberjinoyat hali ham oddiy odamning radarida bo‘lganga o‘xshaydi. Har yili 1,5 million kiberhujum sodir bo‘ladi, ya’ni kuniga 4000 dan ortiq hujumlar, har soatda 170 ta hujumlar yoki har daqiqada deyarli uchta hujum sodir bo‘ladi, tadqiqotlar shuni ko‘rsatadiki, qurbonlarning atigi 16 foizi buni amalga oshirayotgan odamlardan so‘ragan. hujumlarni to‘xtatish[54]. Har qanday sababga ko‘ra internetdan foydalanadigan har bir kishi qurbon bo‘lishi mumkin, shuning uchun onlayn rejimida qanday qilib himoyalanganligi haqida bilish muhimdir.

Intellekt[tahrir | manbasini tahrirlash]

Kiberjinoyatchilikning ko‘payishi natijasida kiberjinoyatchilik faoliyatidan foyda olishga intilayotgan shaxslar va guruhlarni qo‘llab-quvvatlash uchun professional

ekotizim rivojlandi. Ekotizim juda ixtisoslashgan, jumladan zararli dasturlarni ishlab chiquvchilar, botnet operatorlari, professional kiberjinoyat guruhlari, o‘g‘irlangan kontentni sotishga ixtisoslashgan guruhlar va boshqalar. Bir nechta yetakchi kiberxavfsizlik kompaniyalari ushbu shaxslar va guruh faoliyatini kuzatish uchun ko‘nikma, resurslar va ko‘rinishga ega[55]. Ushbu manbalardan mudofaa maqsadlarida foydalanish mumkin bo‘lgan juda ko‘p ma’lumotlar, jumladan, zararlangan fayllar xeshlari[56] yoki zararli IP/URLlar[56], kabi texnik ko‘rsatkichlar, shuningdek maqsadlar, usullar va usullarni profillovchi strategik ma’lumotlar mavjud. profilli guruhlarning kampaniyalari. Ulardan ba’zilari erkin nashr etiladi, lekin doimiy, doimiy kirish odatda dushman razvedka obuna xizmatiga obuna bo‘lishni talab qiladi. Individual tahdid aktyori darajasida tahdid razvedkasi ko‘pincha o‘sha aktyorning „TTP“si yoki „taktikalar, texnikalar va protseduralar“ deb ataladi, chunki infratuzilma, vositalar va boshqa texnik ko‘rsatkichlar tajovuzkorlar uchun ko‘pincha o‘zgarishi mumkin emas. Korporativ sektorlar sun’iy intellekt kiberxavfsizlikning hal qiluvchi rolini ko‘rib chiqmoqda[57][58].

INTERPOL Cyber Fusion Center Internet foydalanuvchilariga so‘nggi onlayn firibgarliklar, kiber tahdidlar va xavflar haqida ma’lumot tarqatish uchun kiberxavfsizlikning asosiy ishtirokchilari bilan hamkorlikni boshladi. Ijtimoiy ishlab chiqilgan firibgarliklar, to‘lov dasturlari, fishing va boshqalar bo‘yicha hisobotlar 2017-yildan beri 150 dan ortiq mamlakatlardagi xavfsizlik agentliklariga tarqatilgan[59].

Kiberjinoyatning tarqalishi[tahrir | manbasini tahrirlash]

Kiberjinoyatchilik faoliyatining keng tarqalishi kompyuter jinoyatlarini aniqlash va jinoiy javobgarlikka tortish masalasidir. Xakerlik hamjamiyatlari o‘z bilimlarini Internet orqali sezilarli darajada tarqatganligi sababli xakerlik kamroq murakkablashdi. Bloglar va hamjamiyatlar ma’lumot almashishga katta hissa qo‘shdilar: yangi boshlanuvchilar eski xakerlarning bilimlari va maslahatlaridan foydalanishlari mumkin.

Bundan tashqari, xakerlik har qachongidan ham arzonroq: bulutli hisoblash davridan oldin spam yuborish yoki firibgarlik qilish uchun maxsus server, serverlarni boshqarish, tarmoq konfiguratsiyasi va texnik xizmat ko‘rsatish bo‘yicha ko‘nikmalar, Internet-provayder standartlarini bilish va boshqalar kerak edi. Taqqoslash uchun, xizmat sifatida pochta dasturi marketing maqsadlari uchun kengaytiriladigan, arzon, ommaviy va tranzaksiyaviy elektron pochta xabarlarini yuborish xizmati bo‘lib, spam uchun osongina sozlanishi mumkin[60]. Bulutli hisoblash kiberjinoyatchi uchun parolni qo‘pol ravishda majburlash, botnetga kirishni yaxshilash yoki spam kampaniyasini osonlashtirish nuqtai nazaridan o‘z hujumidan foydalanish usuli sifatida foydali bo‘lishi mumkin[61].

Manbalar[tahrir | manbasini tahrirlash]

1. ↑ Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime, " Cleveland, Mississippi: Anderson Publishing.
2. ↑ „cybercrime | Definition, Statistics, & Examples“ (en). *Encyclopedia Britannica*. Qaraldi: 25-may 2021-yil.
3. ↑ *Bossler, Adam M.; Berenblum, Tamar (2019-10-20). „Introduction: new directions in cybercrime research“. Journal of Crime and Justice. 42-jild, № 5. 495–499-bet. doi:10.1080/0735648X.2019.1692426. ISSN 0735-648X.*
4. ↑ „cybercrime | Definition, Statistics, & Examples | Britannica“ (en). *www.britannica.com*. Qaraldi: 14-dekabr 2021-yil.
5. ↑ „BUFFETT: This is 'the number one problem with mankind'“. *Business Insider*. Qaraldi: 17-may 2021-yil.
6. ↑ „Warren Buffett: 'Cyber poses real risks to humanity'“ (en-US). *finance.yahoo.com*. Qaraldi: 17-may 2021-yil.
7. ↑ „Cyber crime costs global economy $445 billion a year: report“. *Reuters* (9-iyun 2014-yil). Qaraldi: 17-iyun 2014-yil.
8. ↑ „Cybercrime To Cost The World 80.5 Trillion Annually By 2025“ (en-US). *Cybercrime Magazine* (4-mart 2018-yil). Qaraldi: 17-may 2021-yil.
9. ↑ „#Cybercrime— what are the costs to victims - North Denver News“. *North Denver News* (17-yanvar 2015-yil). Qaraldi: 16-may 2015-yil.
10. ↑ *Lewis, James (February 2018). „Economic Impact of Cybercrime - No*