

DARKNET VA GLOBAL KIBERJINOYATCHILIK EVOLYUTSIYASI

Ruzibayev Eldorjon Xoshimjon o'g'li

E-mail: ruzibayeveldor@gmail.com +998933952659

*Toshkent amaliy fanlar universiteti Axborot texnologiyalar fakulteti
(Axborot xavfsizligi) yo'nalishi KAX 23-01guruh talabasi*

KIRISH

Raqamli texnologiyalar rivojlanishi bilan bir qatorda internetning yashirin qatlamlari ham shakllanib bordi. Ular orasida Darknet alohida o'rin egallaydi. Darknet — bu oddiy qidiruv tizimlari orqali topib bo'lmaydigan, maxsus dasturiy vositalar yordamida kiriladigan tarmoq segmenti bo'lib, u anonimlikni ta'minlashga qaratilgan texnologiyalar asosida ishlaydi. Ushbu muhitning asosiy xususiyati foydalanuvchilarning shaxsini yashirish va ularning faoliyatini kuzatishni murakkablashtirishdir.

Darknetning rivojlanishi bilan birga global kiberjinoyatchilik ham yangi bosqichga o'tdi. An'anaviy jinoyatchilik shakllaridan farqli ravishda, raqamli jinoyatlar endi geografik chegaralarga bog'liq emas va butun dunyo bo'ylab amalga oshirilishi mumkin. Darknet esa ushbu jarayon uchun qulay yashirin platforma sifatida xizmat qilmoqda.

Bugungi kunda Darknet orqali noqonuniy tovarlar savdosi, ma'lumotlar o'g'irlanishi, zararli dasturlar tarqatilishi va turli kiberhujumlar amalga oshirilishi mumkin. Shu bilan birga, kriptovalyutalarning paydo bo'lishi anonim to'lov tizimlarini yaratib, kiberjinoyatchilikni yanada murakkablashtirdi.

Mazkur maqolada Darknetning mohiyati, uning texnologik asoslari, global kiberjinoyatchilikning evolyutsiyasi hamda ushbu muhitda sodir bo'ladigan asosiy jinoyat turlari ilmiy jihatdan tahlil qilinadi. Shuningdek, Darknetga qarshi kurashish usullari va zamonaviy axborot xavfsizligi yondashuvlari ham ko'rib chiqiladi.

DARKNET TUSHUNCHASI VA UNING TUZILISHI

Darknet internetning yashirin qismi bo'lib, u oddiy qidiruv tizimlari orqali indekslanmaydi va bevosita kirish mumkin bo'lmagan tarmoq segmentlarini o'z ichiga oladi. Unga kirish uchun maxsus anonimlashtirish texnologiyalari, masalan, Tor (The Onion Router) kabi tarmoqlar yoki shunga o'xshash vositalardan foydalaniladi. Darknetning asosiy maqsadi foydalanuvchilarga yuqori darajadagi anonimlikni ta'minlashdir.

Tuzilish jihatidan Darknet markazlashmagan tarmoq hisoblanadi. Unda ma'lumotlar bir nechta qatlamli shifrlash orqali uzatiladi, bu esa trafikni kuzatish va foydalanuvchi manbasini aniqlashni juda murakkablashtiradi. Ushbu ko'p qatlamli shifrlash "onion routing" tamoyiliga asoslanadi, ya'ni ma'lumot bir nechta tugunlar orqali o'tadi va har bir bosqichda alohida shifrlash qatlamlari ochib boriladi.

Darknet odatda "deep web"ning bir qismi sifatida qaraladi, biroq ular bir xil tushunchalar emas. Deep web — bu qidiruv tizimlarida ko'rinmaydigan barcha ma'lumotlarni o'z ichiga olsa, Darknet aynan maxsus texnologiyalar orqali kiriladigan yashirin tarmoqlardan iborat. Bu farq ularning texnik va funksional jihatdan turlicha ekanini ko'rsatadi.

Darknet ichida turli platformalar mavjud bo'lib, ular forumlar, yashirin bozorlar va maxfiy aloqa tizimlaridan iborat bo'lishi mumkin. Bu muhitda anonimlik yuqori darajada ta'minlangani sababli, u nafaqat qonuniy maxfiylik maqsadlarida, balki noqonuniy faoliyatlar uchun ham ishlatilishi mumkin.

Umuman olganda, Darknetning tuzilishi murakkab shifrlash, ko'p qatlamli routing va markazlashmagan tarmoq arxitekturasida shakllangan bo'lib, u foydalanuvchilarga yuqori darajadagi maxfiylikni ta'minlaydi, shu bilan birga kiberxavfsizlik uchun jiddiy muammolarni ham yuzaga keltiradi.

DARKNETNING ISHLASH MEXANIZMI VA TEXNOLOGIK ASOSLARI

Darknetning ishlash mexanizmi asosan anonimlikni ta'minlash va foydalanuvchi identifikatsiyasini yashirishga qaratilgan murakkab texnologik jarayonlarga asoslanadi. Bu tarmoqda ma'lumotlar bevosita emas, balki bir nechta vositachi tugunlar orqali uzatiladi, natijada jo'natuvchi va qabul qiluvchi o'rtasidagi bog'liqlikni aniqlash juda qiyinlashadi.

Darknetning eng keng tarqalgan texnologik asoslaridan biri "onion routing" hisoblanadi. Bu usulda ma'lumot bir necha qatlamli shifrlash bilan himoyalangani va har bir tugunda faqat bitta qatlam ochiladi. Natijada har bir oraliq tugun faqat oldingi va keyingi nuqtani biladi, lekin butun yo'nalish haqida to'liq ma'lumotga ega bo'lmaydi. Shu sababli foydalanuvchining haqiqiy IP manzilini aniqlash deyarli imkonsiz bo'ladi.

Darknetda ishlatiladigan asosiy infratuzilmalardan biri Tor tarmog'i hisoblanadi. U global miqyosdagi ko'ngilli serverlar tarmog'idan iborat bo'lib, trafikni tasodifiy yo'nalishlar orqali uzatadi. Bu jarayonda ma'lumot bir nechta tugunlardan o'tadi va har safar qayta shifrlanadi, bu esa xavfsizlik darajasini oshiradi.

Bundan tashqari, Darknetda I2P va Freenet kabi alternativ anonim tarmoqlar ham mavjud bo'lib, ular ham shunga o'xshash prinsiplar asosida ishlaydi. Ushbu tizimlar markazlashmagan arxitektura va kuchli shifrlash algoritmlariga tayangan holda foydalanuvchilarning maxfiyligini ta'minlaydi.

Texnologik jihatdan Darknet DNS tizimlaridan mustaqil ishlaydi va ko'pincha maxsus domen zonalaridan (.onion kabi) foydalanadi. Bu esa uni oddiy internetdan ajratib turuvchi asosiy belgilaridan biridir.

Umuman olganda, Darknetning ishlash mexanizmi ko'p qatlamli shifrlash, markazlashmagan tarmoq tuzilmasi va anonim marshrutlash texnologiyalariga asoslanadi. Ushbu xususiyatlar uni yuqori darajadagi maxfiylikka ega tizimga aylantiradi, biroq shu bilan birga turli kiberxavfsizlik tahdidlarini ham yuzaga keltiradi.

GLOBAL KIBERJINOYATCHILIK EVOLYUTSIYASI

Global kiberjinoyatchilik rivojlanishi axborot texnologiyalarining taraqqiyoti bilan bevosita bog'liq holda shakllangan murakkab jarayon hisoblanadi. Internetning keng tarqalishi bilan birga jinoyatchilikning an'anaviy shakllari raqamli muhitga ko'chib, yangi ko'rinish va usullarni yuzaga keltirdi. Dastlabki bosqichlarda kiberjinoyatlar asosan oddiy viruslar tarqatish yoki tizimlarga ruxsatsiz kirish kabi cheklangan harakatlar bilan ifodalangan bo'lsa, vaqt o'tishi bilan ular yanada murakkab va professional shaklga ega bo'ldi.

Kiberjinoyatchilik evolyutsiyasining keyingi bosqichida moliyaviy motivlar asosiy o'ringa chiqdi. Onlayn banking tizimlarining rivojlanishi va elektron to'lovlarning keng qo'llanilishi natijasida xakerlik hujumlari orqali pul o'g'irlash, phishing va ma'lumotlarni shifrlab qo'yib to'lov talab qilish (ransomware) kabi jinoyatlar keng tarqaldi. Bu davrda kiberjinoyatchilik alohida guruhlar va tashkil etilgan tarmoqlar tomonidan amalga oshiriladigan faoliyatga aylandi.

So'nggi yillarda kiberjinoyatchilik global darajada transmilliy xarakter kasb etdi. Jinoyatchilar geografik chegaralardan mustaqil ravishda ishlay boshladi, bu esa huquqiy nazoratni

qiyinlashtirdi. Darknetning rivojlanishi ushbu jarayonni yanada kuchaytirib, noqonuniy xizmatlar, zararli dasturlar va o'g'irlangan ma'lumotlar savdosi uchun yashirin platforma sifatida xizmat qila boshladi.

Shuningdek, zamonaviy bosqichda kiberjinoyatchilik sun'iy intellekt va avtomatlashtirilgan vositalar yordamida amalga oshirilmoqda. Bu esa hujumlarning tezligi, murakkabligi va ko'lamini sezilarli darajada oshirdi. Natijada kiberjinoyatchilik oddiy texnik buzilishlardan global xavfsizlikka tahdid soluvchi strategik muammoga aylandi.

Umuman olganda, kiberjinoyatchilik evolyutsiyasi oddiy individual harakatlardan boshlab, bugungi kunda yuqori darajada tashkil etilgan, texnologik va global tarmoqlar orqali amalga oshiriladigan murakkab tizimga aylanganini ko'rsatadi.

DARKNETDA UCHRAYDIGAN KIBERJINOYATLAR TURLARI

Darknet turli anonimlik texnologiyalariga asoslanganligi sababli u yerda noqonuniy faoliyatni yashirin tarzda amalga oshirish imkoniyati nisbatan yuqori hisoblanadi. Shu sababli ushbu muhit kiberjinoyatchilar tomonidan turli noqonuniy faoliyatlarni tashkil etish va amalga oshirish uchun keng qo'llaniladi. Darknetdagi kiberjinoyatlar bir nechta asosiy yo'nalishlarga bo'linadi.

Eng keng tarqalgan jinoyat turlaridan biri noqonuniy tovarlar savdosidir. Bu yerda giyohvand moddalar, soxta hujjatlar, noqonuniy dasturiy ta'minotlar va boshqa taqiqlangan mahsulotlar savdosi amalga oshiriladi. Bunday platformalar ko'pincha kriptovalyutalar orqali to'lovlarni qabul qiladi, bu esa tranzaksiyalarni kuzatishni qiyinlashtiradi.

Ikkinchi muhim tur — ma'lumotlar o'g'irlanishi va ularning savdosidir. Darknetda o'g'irlangan bank kartalari ma'lumotlari, foydalanuvchi hisoblari, parollar va shaxsiy ma'lumotlar sotilishi mumkin. Bu holat kiberfiribgarlik va identifikatsion o'g'irlik xavfini keskin oshiradi.

Shuningdek, zararli dasturlar va kiberhujum vositalarining tarqatilishi ham keng tarqalgan. Darknet orqali ransomware, viruslar va xakerlik vositalari sotiladi yoki ijaraga beriladi. Bu esa hatto professional bilimga ega bo'lmagan shaxslarga ham kiberhujumlar uyushtirish imkonini yaratadi.

Bundan tashqari, Darknetda kiberhujum xizmatlari ham taklif etiladi. Masalan, DDoS hujumlari buyurtma asosida amalga oshirilishi mumkin. Bu turdagi xizmatlar "cybercrime-as-a-service" modeli sifatida rivojlanib bormoqda.

Umuman olganda, Darknetdagi kiberjinoyatlar turlari juda xilma-xil bo'lib, ular nafaqat texnik, balki iqtisodiy va ijtimoiy xavflarni ham keltirib chiqaradi. Bu esa kiberxavfsizlik tizimlarini yanada kuchaytirish zaruratini yuzaga keltiradi.

KRIPTOVALYUTALAR VA ANONIMLIKNING ROLI

Kriptovalyutalar zamonaviy raqamli iqtisodiyotning muhim tarkibiy qismlaridan biri bo'lib, ular markazlashmagan to'lov tizimi asosida ishlaydi. Ushbu texnologiya blokcheyn (blockchain) konsepsiyasiga tayangan holda tranzaksiyalarni qayd etadi va ularning o'zgarmasligini ta'minlaydi. Shu bilan birga, kriptovalyutalar Darknet muhitida anonimlikni kuchaytiruvchi asosiy vositalardan biri sifatida ham keng qo'llaniladi.

Kriptovalyutalarning asosiy xususiyati — foydalanuvchilar o'rtasidagi tranzaksiyalarda bevosita shaxsiy ma'lumotlarning oshkor etilmasligidir. Garchi barcha operatsiyalar blokcheynda ochiq ko'rinishda qayd etilsa-da, hamyon egasining shaxsini aniqlash har doim ham oson bo'lmaydi. Aynan shu jihat ularni Darknetdagi noqonuniy faoliyatlar uchun jozibador qiladi.

Anonimlik darajasini yanada oshirish uchun turli qo'shimcha texnologiyalar ham qo'llaniladi. Masalan, mikserlar (mixing services) kriptovalyuta tranzaksiyalarini aralashtirib, ularning manbasini aniqlashni qiyinlashtiradi. Bu esa moliyaviy oqimlarni kuzatish va jinoyatchilarni aniqlash jarayonini murakkablashtiradi.

Shu bilan birga, kriptovalyutalar faqat salbiy maqsadlarda emas, balki qonuniy raqamli iqtisodiyotda ham keng qo'llanilmoqda. Ular tezkor xalqaro to'lovlar, banklarsiz tranzaksiyalar va moliyaviy innovatsiyalarni rivojlantirishda muhim rol o'ynaydi. Biroq Darknet muhitida ularning anonimlik xususiyati ko'proq kiberjinoyatchilikni qo'llab-quvvatlovchi omil sifatida namoyon bo'ladi.

Umuman olganda, kriptovalyutalar va anonimlik texnologiyalari raqamli iqtisodiyotda ikki tomonlama rol o'ynaydi: bir tomondan innovatsiya va qulaylik yaratadi, ikkinchi tomondan esa Darknetda noqonuniy faoliyatlarni yashirish imkoniyatini kengaytiradi.

DARKNET MONITORINGI VA UNGA QARSHI KURASH USULLARI

Darknetdagi faoliyatni monitoring qilish va unga qarshi kurashish kiberxavfsizlik sohasining eng murakkab yo'nalishlaridan biri hisoblanadi. Buning asosiy sababi — Darknetning anonimlikka asoslangan tuzilishi bo'lib, u foydalanuvchilarni to'g'ridan-to'g'ri identifikatsiya qilishni qiyinlashtiradi. Shu sababli bu muhitda sodir bo'layotgan noqonuniy faoliyatlarni aniqlash uchun maxsus texnologik va analitik yondashuvlar talab etiladi.

Darknet monitoringining asosiy usullaridan biri ochiq manbali razvedka (OSINT) texnologiyalaridan foydalanishdir. Bu yondashuv orqali maxfiy forumlar, yashirin bozorlar va aloqa kanallaridagi ma'lumotlar tahlil qilinadi. Shuningdek, huquq-tartibot organlari va kiberxavfsizlik mutaxassislari Darknet ichidagi trafik va faoliyatni kuzatish uchun maxsus dasturiy vositalardan foydalanadilar.

Yana bir muhim usul — infiltratsiya va operatsion kuzatuvdir. Bu jarayonda mutaxassislar Darknet muhitiga kirib, jinoyatchilar faoliyatini ichkaridan o'rganadi. Ushbu yondashuv orqali noqonuniy tarmoqlar, savdo platformalari va kiberjinoyatchi guruhlar aniqlanishi mumkin.

Sun'iy intellekt va mashinaviy o'qitish texnologiyalari ham Darknet monitoringida tobora keng qo'llanilmoqda. Ushbu tizimlar katta hajmdagi ma'lumotlarni tahlil qilib, shubhali faoliyatlarni avtomatik aniqlash imkonini beradi. Masalan, zararli kontent, noqonuniy savdo belgilarini yoki kiberhujumga oid izlarni aniqlashda AI muhim rol o'ynaydi.

Darknetga qarshi kurashishda xalqaro hamkorlik ham katta ahamiyatga ega. Kiberjinoyatchilik transmilliy xarakterga ega bo'lgani uchun davlatlar o'rtasida axborot almashinuvi va birgalikdagi operatsiyalar samaradorlikni oshiradi. Interpol va boshqa xalqaro tashkilotlar bu yo'nalishda muhim rol o'ynaydi.

Umuman olganda, Darknet monitoringi va unga qarshi kurash usullari texnologik, analitik va huquqiy yondashuvlarning uyg'unligini talab qiladi. Faqat kompleks strategiya orqali ushbu yashirin muhitdagi kiberjinoyatchilikni samarali nazorat qilish mumkin.

XULOSA

Xulosa qilib aytganda, Darknet va global kiberjinoyatchilik evolyutsiyasi zamonaviy raqamli jamiyat uchun eng murakkab va dolzarb muammolardan biri hisoblanadi. Internetning yashirin qatlamlari sifatida shakllangan Darknet anonimlikni ta'minlash bilan birga, turli noqonuniy faoliyatlar uchun ham qulay muhit yaratib bermoqda.

Tahlillar shuni ko'rsatadiki, kiberjinoyatchilik oddiy texnik hujumlardan boshlab, bugungi kunga kelib yuqori darajada tashkil etilgan global tarmoqlarga aylangan. Unda kriptovalyutalar, shifrlash texnologiyalari va anonim aloqa vositalari keng qo'llanilishi jinoyatlarni aniqlash va ularning oldini olishni yanada qiyinlashtirmoqda.

Shu bilan birga, Darknetni to'liq salbiy hodisa sifatida baholash ham to'g'ri emas, chunki u ayrim holatlarda maxfiylik va xavfsiz aloqa uchun ham xizmat qiladi. Biroq uning noqonuniy maqsadlarda ishlatilishi kiberxavfsizlik sohasida jiddiy tahdidlarni yuzaga keltiradi.

Umuman olganda, Darknet va kiberjinoyatchilikka qarshi samarali kurashish uchun zamonaviy texnologiyalar, xalqaro hamkorlik va huquqiy nazoratni birgalikda qo'llash zarur. Bu esa raqamli muhitda xavfsizlikni ta'minlash va global axborot tizimlarining barqarorligini saqlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Chertoff, M., & Simon, T. (2015). *The Impact of the Dark Web on Internet Governance and Cybersecurity*. Center for Global Enterprise.
2. Moore, D., & Rid, T. (2016). "Cryptopolitik and the Darknet." *Survival: Global Politics and Strategy*.
3. Bartlett, J. (2014). *The Dark Net: Inside the Digital Underworld*. Melville House.
4. Finklea, K. (2017). *Dark Web*. Congressional Research Service Report.
5. Europol (2023). *Internet Organised Crime Threat Assessment (IOCTA)*.
6. UNODC (United Nations Office on Drugs and Crime). (2022). *Cybercrime and Darknet Markets Report*.
7. Ormsby, E. (2019). *Silk Road and Online Drug Markets*.
8. Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*.
9. Holt, T. J. (2020). "Darknet markets and cybercrime ecosystems." *Crime Science Journal*.
10. Europol & INTERPOL Joint Report (2024). *Global Cybercrime Trends and Darknet Activity Analysis*.