KIBERXAVFSIZLIK VA ZAMONAVIY TAHDIDLAR: RANSOMWARE HUJUMLARI TAHLILI

O'razova Muxlisa

Qarshi davlat universiteti talabasi

Annotatsiya. *Raqamli texnologiyalarning jadal rivojlanishi bilan kiberjinoyatchilik ham yangi va murakkab shakllarga ega bo'lmoqda. Ransomware (to'lov dasturlari) hujumlari bugungi kunda eng xavfli va keng tarqalgan kibertahdidlardan biri sifatida e'tirof etilmoqda. Mazkur tezisda ransomware hujumlarining texnik mohiyati, tarqalish mexanizmlari, global miqyosdagi iqtisodiy va ijtimoiy oqibatlari hamda ularga qarshi samarali himoya strategiyalari ilmiy jihatdan tahlil qilinadi. Tadqiqot natijalaridan kiberxavfsizlik sohasida amaliy qo'llanma sifatida foydalanish mumkin.*

Kalit so'zlar: *Ransomware, kiberhujum, to'lov dasturi, kiberxavfsizlik, shifrlash, zaxira nusxa, fishing, WannaCry, zararli dastur, kiber mudofaa.*

Annotation. *With the rapid advancement of digital technologies, cybercrime is evolving into increasingly sophisticated forms. Ransomware attacks are now recognized as one of the most dangerous and widespread cyber threats today. This thesis scientifically analyzes the technical nature of ransomware attacks, their propagation mechanisms, global economic and social consequences, and effective defense strategies against them. The research findings can be used as a practical guide in the field of cybersecurity.*

Keywords: *Ransomware, cyberattack, ransomware software, cybersecurity, encryption, backup, phishing, WannaCry, malware, cyber defense.*

Аннотация. *С быстрым развитием цифровых технологий киберпреступность приобретает всё более сложные формы. Атаки типа «программы-вымогатели» (ransomware) в настоящее время признаются одной из наиболее опасных и распространённых киберугроз. В данной тезисной работе проводится научный анализ технической природы атак*

ransomware, механизмов их распространения, глобальных экономических и социальных последствий, а также эффективных стратегий защиты от них.

Ключевые слова: *Программа-вымогатель, кибератака, кибербезопасность, шифрование, резервное копирование, фишинг, WannaCry, вредоносное ПО, киберзащита.*

XXI asrda raqamli iqtisodiyotning shakllanishi va axborot texnologiyalarining barcha sohalarga kirib borishi bilan birga, kibertahdidlar ham misli ko’rilmagan darajada o’sib bormoqda. Davlatlar, yirik korporatsiyalar, tibbiyot muassasalari, ta’lim tashkilotlari va oddiy fuqarolar – barchasi kiberhujumlarning nishoniga aylanishi mumkin. Bu hujumlarning eng xavflisi va keng tarqalgani – ransomware, ya’ni to’lov dasturlari hujumlaridir.

Ransomware – foydalanuvchining ma’lumotlarini shifrlash yoki tizimga kirishni bloklash orqali to’lov talab qiluvchi zararli dasturdir. Hujumchilar odatda to’lovni kriptovalyuta orqali, asosan Bitcoin ko’rinishida talab qiladi. So’nggi yillarda bu hujumlar nafaqat tez-tez takrorlanib, balki texnik jihatdan ham murakkablashib bormoqda. Hujum odatda uch asosiy bosqichda amalga oshiriladi:

Birinchi bosqich – Infiltratsiya: ransomware tizimga fishing elektron xabarlari, zararli havolalar yoki zaif dasturiy ta’minotdagi bo’shliqlar orqali kiradi.

Ikkinchi bosqich – Shifrlash: dastur tarqaladi va barcha muhim fayllarni shifrlaydi, ularni foydalanib bo’lmaydigan holga keltiradi.

Uchinchi bosqich – To’lov talabi: foydalanuvchiga to’lov to’lash bo’yicha ko’rsatma qoldiriladi, odatda vaqt chegarasi bilan birga.

Tadqiqotlar shuni ko’rsatadiki, ransomware ko’pincha quyidagi kanallar orqali tarqaladi. Fishing elektron xabarlari (Phishing) – bu eng keng tarqalgan usul bo’lib, hujumchilar qonuniy tashkilotlardan kelgandek ko’rinadigan xabarlar yuboradi. 2023-yil statistikasiga ko’ra, hujumlarning 75% dan ortig’i aynan shu yo’l orqali amalga oshirilgan.

Drive-by Download usulida foydalanuvchi zararli veb-saytga kirganda, uning xabarsiz holda ransomware yuklanadi. RDP (Remote Desktop Protocol) zaifliklari orqali esa hujumchilar masofaviy kirish protokollarini buzib, to’g’ridan-

to’g’ri tizimga kirib oladi. Shuningdek, ijtimoiy muhandislik usullari – psixologik manipulyatsiya orqali foydalanuvchini o’z-o’zidan zararli dasturni ishga tushirishga majbur qilish ham keng qo’llaniladi.

Zaif dasturiy ta’minot bo’shliqlaridan foydalanish ham muhim tarqalish yo’llaridan biridir. O’z vaqtida yangilanmagan dasturlar ransomware uchun ochiq eshik bo’lib xizmat qiladi.

Ransomware hujumlari nafaqat shaxslarga, balki yirik tashkilotlarga, kasalxonalarga, hukumat idoralariga va kritik infratuzilmalarga ham ulkan zarar yetkazadi. Cybersecurity Ventures kompaniyasining ma’lumotlariga ko’ra, global miqyosda 2023-yilda ransomware hujumlaridan ko’rilgan umumiy zarar 30 milliard dollardan oshgan.

Sog’liqni saqlash sohasi ayniqsa zaif hisoblanadi – kasalxonalar hujumga uchrasa, bemorlarning hayoti xavf ostiga qolishi mumkin. 2020-yilda Germaniyada bir kasalxonaga uyushtirilgan ransomware hujumi bemorni boshqa shifoxonaga ko’chirishni talab qildi va bu holat fojia bilan yakunlandi.

Ta’lim, moliya va energetika sohalari ham eng ko’p zarar ko’rgan tarmoqlar qatoriga kiradi. Hujumlar nafaqat moliyaviy yo’qotishlarga, balki obro’ ziyoni, ishlab chiqarish to’xtashi va davlat xavfsizligiga ham tahdid soladi.

Tarixdagi eng yirik ransomware hujumlari orasida bir nechta holat alohida o’rin tutadi. WannaCry (2017) – Microsoft Windows tizimlarining zaifligidan foydalanib, 150 dan ortiq mamlakatda 200 000 dan ziyod kompyuterni zararlagan. Jami zarar 4 milliard dollarga yetgan deb baholanadi. Britaniya milliy sog’liqni saqlash tizimi (NHS) ham bu hujumdan katta talofat ko’rgan.

REvil va Conti kabi zamonaviy ransomware guruhlari esa 2021-2022 yillarda ko’plab yirik korporatsiyalardan millionlab dollar to’lov undirishga muvaffaq bo’lgan.

Mutaxassislar ransomwarega qarshi kurashda quyidagi asosiy choralarni tavsiya etadi. Ma’lumotlarni muntazam zaxiralash – 3-2-1 qoidasi asosida: 3 ta nusxa, 2 ta turli muhitda, 1 tasi oflayn holda saqlash. Bu ransomware hujumida ham ma’lumotlarni tiklash imkonini beradi.

Dasturiy ta’minotni o’z vaqtida yangilash – WannaCry hujumi xuddi patch chiqarilgandan keyin kechikib yangilagan tizimlarga zarba bergan. Ko’p bosqichli autentifikatsiya (MFA) joriy etish – bitta parol o’g’irlansa ham tizimga kirishni qiyinlashtiradi. Zero-trust arxitekturasi tamoyillariga rioya qilish – “Hech kimga ishonma, hammasini tekshir” tamoyili asosida ishlash.

Xodimlarni kiberxavfsizlik bo’yicha muntazam o’qitish ham muhim ahamiyat kasb etadi, chunki hujumlarning aksariyati inson xatosidan boshlanadi. Tarmoqni segmentlarga bo’lish esa ransomware tarqalishini cheklashga yordam beradi. Ransomware tahdidiga qarshi kurash faqat texnik choralar bilan cheklanmay, balki kuchli qonunchilik bazasi va xalqaro hamkorlikni ham talab etadi. Kiberjinoyatchilar ko’pincha turli mamlakatlarda joylashib, global miqyosda faoliyat olib boradi. Shu sababli, bitta davlatning sa’y-harakatlari yetarli bo’lmaydi.

O’zbekistonda ham 2022-yilda qabul qilingan “Kiberxavfsizlik to’g’risida”gi qonun bu sohadagi muhim qadamlardan biridir.

Kriptovalyuta operatsiyalarini tartibga solish ham ransomware moliyasini cheklashda muhim ahamiyat kasb etadi, chunki to’lovlar asosan kriptovalyuta orqali amalga oshiriladi.

Xulosa. Ransomware hujumlari zamonaviy kiberxavfsizlikning eng dolzarb va xavfli muammolaridan biri bo’lib qolmoqda. Ularning texnik murakkabligi, global miqyosi va yetkazadigan zarari yildan-yilga ortib bormoqda. Ushbu tezisda ko’rib chiqilgan tahlillar shuni ko’rsatadiki, ransomware tahdidiga faqat kompleks va ko’p qatlamli yondashuv orqali munosib javob berish mumkin.

Samarali mudofaa uchun texnik himoya vositalari (zaxiralash, MFA, yangilash), xodimlar savodxonligi va xalqaro hamkorlikning uyg’un birlashuvi talab etiladi. Faqat shunday integrallashgan strategiya orqali tashkilotlar va davlatlar ransomware tahdidini minimallashtirib, raqamli xavfsizlikni ta’minlashi mumkin.

Kelajakda sun’iy intellekt asosidagi kiberhimoya tizimlari va kvant kriptografiyasi ransomwarega qarshi kurashda yangi imkoniyatlar ochishi kutilmoqda. Biroq, texnologiya qanchalik rivojlanmasin, inson omili – xodimlarning ogoh va savodli bo’lishi – har doim asosiy himoya qatlami bo’lib qoladi.

FOYDALANILGAN ADABIYOTLAR

1. Ablon, L., & Bogart, A. (2017). Bug Bounties vs. Ransomware: An Analysis of the Cybersecurity Marketplace. RAND Corporation.

2. CISA. (2023). Ransomware Guide: Best Practices for Prevention and Response. Cybersecurity and Infrastructure Security Agency.

3. Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.

4. Hasanov, A. R. (2022). Kiberjinoyatchilik va unga qarshi kurash usullari. Toshkent: O'zbekiston Milliy universiteti nashriyoti.

5. Saidova D. Teaching Programming Collaboratively Through Google Colab AND Github Integration //Green Economy and Development. – Т. 3. – №. 11. – С. 667884.

6. Ashurovna K. N., Hakimovna B. N., Ergashovna S. D. Teaching Energy Efficiency: Integrating Servers with Student Engagement.