SO‘NGGI YILLARDA ENG KENG TARQALGAN KIBERHUJUMLAR TURLARI VA ULARNI OLDINI OLISH USULLARI

Oxunboboyeva Charos Zuxriddin qizi

O‘zbekiston respublikasi ichki ishlar vazirligi Akademiyasi, Raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o‘qituvchisi.texnika fanlari bo‘yicha falsafa doktori, (PhD),

E-mail: charosoxunboboyeva@gmail.com

Isakov Abror Fakhriddinovich

O‘zbekiston respublikasi ichki ishlar vazirligi Akademiyasi, Raqamli texnologiyalar va axborot xavfsizligi kafedrasi dotsenti. texnika fanlari bo‘yicha falsafa doktori, (PhD),

E-mail: aisaqov921@gmail.com

Annotasiya. Ushbu maqolada 2020 yildan keyin global miqyosda eng ko‘p kuzatilayotgan va tashkilotlarga jiddiy xavf tug‘dirayotgan kiberhujumlarning asosiy turlari tahlil qilinadi. Jumladan, Ransomware (to‘lov talab qiluvchi viruslar), Fishing (Phishing) va APT (Advanced Persistent Threats) hujumlariga alohida e'tibor qaratiladi. Tadqiqotning maqsadi – ushbu tahdidlarning ishlash mexanizmini ko‘rib chiqish hamda ularni samarali oldini olishga qaratilgan zamonaviy texnik va tashkiliy choralarni (Zero Trust arxitekturasi, o‘quv dasturlari) ko‘rib chiqishdan iborat. Tahlillar shuni ko‘rsatadiki, ko‘p qavatli himoya (Defense in Depth) strategiyasi va doimiy xabardorlikni oshirish kiberxavfsizlikni saqlashning asosiy omili hisoblanadi.

Kalit so‘zlar: Kiberhujum, Ransomware, Fishing, APT, Axborot xavfsizligi, Zero Trust, Ma'lumotlar himoyasi.

Аннотация. В этой статье будут проанализированы основные типы кибератак, которые наиболее часто наблюдаются во всем мире после 2020 года и представляют серьезную угрозу для организаций. В частности, особое внимание уделяется атакам вымогателей (вирусы, требующие оплаты), фишинга (фишинг) и APT (Advanced Persistent Threats). Целью исследования является рассмотрение механизма действия этих угроз и рассмотрение современных технических и организационных мер (архитектура Zero Trust, образовательные программы), направленных на их эффективную профилактику. Анализ показывает, что стратегия многоуровневой защиты (Defense in Depth) и постоянное повышение осведомленности являются ключевыми факторами в поддержании кибербезопасности.

Ключевые слова: кибератака, вымогательство, Fishing, APT, Информационная безопасность, Zero Trust, защита данных.

Abstract. This article will analyze the main types of cyberattacks that have been observed most frequently worldwide since 2020 and pose a significant threat to

organizations. In particular, it focuses on ransomware attacks (viruses that require payment), phishing attacks (phishing), and APT (Advanced Persistent Threats). The purpose of this research is to examine the mechanisms of these threats and explore modern technical and organizational measures (Zero Trust architecture, educational programs) aimed at effectively preventing them. The analysis shows that a multi-layered defense strategy (Defense in Depth) and continuous awareness-raising are key factors in maintaining cybersecurity.

Keywords: cyberattack, ransomware, Fishing, APT, Information Security, Zero Trust, data protection.

Kirish.

Raqamlashuvning jadal sur'atlari jamiyatning barcha jabhalarida, jumladan, iqtisodiyot, davlat boshqaruvi va infratuzilmaga qaramligini oshirmoqda. Ushbu o‘sish bilan birga, kiberxavflarning murakkablashishi va sonining keskin ko‘payishi kuzatilmoqda. So‘nggi yillardagi global voqealar (pandemiya, geosiyosiy o‘zgarishlar) xususiy va korporativ tarmoqlarga qilingan hujumlarning ko‘payishiga sabab bo‘ldi.

Ushbu maqolaning maqsadi so‘nggi 3-4 yil ichida eng ko‘p qo‘llanilayotgan kiberhujumlarning asosiy vektorini aniqlash va bu tahdidlarga qarshi samarali mudofafa choralarini taklif qilishdan iborat. Tadqiqot vazifalari quyidagilardan iborat: eng ko‘p uchraydigan hujum turlarini tasniflash, ularning ishlash mexanikasini tahlil qilish va ularni oldini olish uchun amaliy tavsiyalar ishlab chiqish.

Metodlar. Ushbu tadqiqot tizimli tahlil va adabiyotlar qamrovi (Systematic Literature Review) uslubiga asoslangan. Mazkur uslub turli manbalardan olingan ma'lumotlarni xolis va ketma-ket tahlil qilish orqali umumlashtirilgan xulosalarga kelish imkonini beradi.

1. Adabiyotlarni tanlash va saralash:

Manbalar: Tadqiqot uchun 2020 yildan boshlab nashr etilgan ilmiy maqolalar, yirik kiberxavfsizlik kompaniyalarining tahlil hisobotlari (masalan, Microsoft, CrowdStrike, Mandiant, Kaspersky), xalqaro tashkilotlar (ENISA, CISA)ning statistik ma'lumotlari va yillik hisobotlari, shuningdek, mavzuga oid monografiyalar tanlab olindi.

Saralash mezonlari: Maqolalarning ilmiy avtoriteti, nashr etilganligi (peer-reviewed), dolzarbligi, keltirilgan ma'lumotlarning aniqligi va mavzuga mosligi asosiy mezonlar bo‘ldi.

2. Tahlil qilinadigan kiberhujum turlari: Tanlangan manbalar asosida eng keng tarqalgan va ta'siri kuchli uchta kiberhujum turiga e'tibor qaratildi:

ISSN 3030-3907

Ransomware (To‘lov talab qiluvchi viruslar): Ularning turlari (shifrlovchi, bloklaydigan), tarqalish usullari (matn, pochta, tijoriy exploits) va eng ko‘p nishonga olinadigan sohalar.

Fishing (Phishing) va uning murakkab shakllari: Klassik fishing, spear-phishing (maqsadli fishing), whaling (yuqori martabali shaxslarga qaratilgan), BEC (Business Email Compromise - tijoriy elektron pochtani buzish).

APT (Advanced Persistent Threats): Uzoq muddatli, yashirin, maqsadli va davlat yoki yirik korporasiyalarga qaratilgan hujumlar. Ularning bosqichlari (tarmoqqa kirish, ma'lumot to‘plash, ma'lumotlarni o‘g‘irlash/buzish).

3 Himoya usullarini tizimli tahlil qilish: Har bir hujum turi uchun aniqlangan mudofaa choralari quyidagi tizimli yondashuvlar doirasida guruhlandi:

Texnik choralar: Dasturiy va apparat vositalari (Firewall, IDS/IPS, EDR, MFA, shifrlash, pochta filtrlari, tizimlarni patchlash).

Tashkiliy choralar: Ichki siyosatlar, standartlar, xodimlarni o‘qitish va xavfsizlik madaniyatini shakllantirish, insidentlarga javob berish rejalari.

Arxitekturaviy yondashuvlar: Zero Trust, Defense in Depth, mikrosegmentasiya.

Natijalar. Tahlillar natijasida so‘nggi yillarda kiberxavfsizlik landshaftini shakllantirayotgan uchta asosiy hujum turi aniqlandi:

1. Ransomware (To‘lov talab qiluvchi viruslar):

•Tarqalganlik: Hujumlarning foiz ko‘rsatkichi miqdoran eng yuqori bo‘ldi. Ularning asosiy kirish yo‘llari – Fishing elektron xatlari yoki umumiy tarmoqdagi yamoqsiz (patch-less) serverlar hisoblanadi.

•Mexanizm: Virus tizimga kirgach, ma'lumotlarni shifrlaydi va tiklash uchun kriptovalyuta (asosan Bitcoin yoki Monero) orqali to‘lov talab qiladi.

2. Fishing va Unifikasiyalashgan Hujumlar:

•Tarqalganlik: Inson omiliga asoslangan bo‘lganligi sababli, fishing hujumlari hali ham eng ko‘p uchraydigan kirish nuqtasi bo‘lib qolmoqda.

•Mexanizm: Hozirgi fishing xatlari yuqori darajada maqsadli (spear-fishing) va tashkilotning ichki stiliga moslashtirilgan (Business Email Compromise - BEC) bo‘lmoqda.

3. APT (Advanced Persistent Threats):

•Xavf darajasi: Miqdoran kamroq bo‘lsa-da, ularning maqsadliligi va uzoq muddat yashirinishi sababli eng xavfli hisoblanadi. Asosan davlat yoki strategik ahamiyatga ega kompaniyalarga qaratilgan.

•Mexanizm: Tarmoqqa asta-sekin kirib, bir necha oy davomida ma’lumotlarni o‘g‘irlaydi va o‘z mavjudligini yashirishga harakat qiladi.

Muvaffaqiyatli mudofaa uchun quyidagi choralar samarali ekanligi aniqlandi:

ISSN 3030-3907

Hujum turi	Texnik choralar	Tashkiliy choralar
Ransomware	Ma'lumotlarning offlayn va muntazam bekAp nusxalari; Endpoint Detection and Response (EDR) tizimlari.	Muntazam xodimlar uchun simulyasion o‘quvlar.
Fishing	Ko‘p omilli autentifikasiya (MFA); Pochta shlyuzlarini kuchaytirish (antivirus, antispam).	Haftalik/oylik xavfsizlik madaniyati treninglari.
APT	Zero Trust arxitekturasini joriy etish; Tarmoqni mikrosegmentasiya qilish; Trafikni doimiy tahlil qilish.	Havfsizlikni kuzatish markazi (SOC) faoliyatini yaxshilash.

Muhokama. Natijalar shuni ko‘rsatadiki, kiberhujumlarning asosiy yo‘nalishi texnik jihatdan murakkablashish bilan birga, inson omiliga (Fishing) ta'sir qilishga qaratilmoqda. Ransomware hujumlarining ko‘payishi IT infrastrukturasidagi zaiflikdan (xususan, o‘z vaqtida patch o‘rnatilmaslikdan) foydalanishni ko‘rsatadi.

Zero Trust (Hech kimga ishonma) modelining joriy etilishi APT hujumlarining tarmoq ichida harakatlanishini cheklashda muhim qadam bo‘ldi. Biroq, bu texnologiyalarning samaradorligi faqatgina texnik o‘rnatilish bilan cheklanmaydi; ularni to‘g‘ri boshqarish va xodimlarni muntazam o‘qitish zarur.

Cheklovlar: Ushbu tahlil asosan ochiq ma'lumotlarga tayanganligi sababli, yashirin (dark web) ma'lumotlari va xavfsizlik kompaniyalarining yopiq hisobotlaridagi aniq ko‘rsatkichlardan cheklovlar mavjud bo‘lishi mumkin.

Xulosa. So‘nggi yillarda kiberxavflar murakkablashib bormoqda. Ransomware, Fishing va APT – bugungi tashkilotlar uchun eng asosiy uchta tahdiddir. Ularni samarali oldini olish uchun:

1.Texnik mudofaani kuchaytirish: MFA, EDR va Zero Trust tamoyillarini joriy etish.

2.Inson omilini himoya qilish: Doimiy va amaliy xavfsizlik madaniyati treninglarini o‘tkazish.

3.Ma'lumotlarni saqlash: Muhim ma'lumotlarning nafaqat onlayn, balki offlayn bekAp nusxalarini yaratish.

Kelgusi tadqiqotlarda sun'iy intellektning fishing xatlarini avtomatik aniqlash va APT hujumlarini erta bosqichda taxminiy aniqlash mexanizmlarini ishlab chiqishga e'tibor qaratish maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Gartner. (2023). Top Strategic Security and Risk Management Trends. [Manba havolasi].

ISSN 3030-3907

2. ENISA. (2022). Threat Landscape Report for European Critical Infrastructure. European Union Agency for Cybersecurity.
3. Smith, J., & Brown, L. (2021). The Evolution of Ransomware Tactics and Defenses. Journal of Cybersecurity Research, 15(2), 45-60.
4. Oxunboboeva Ch.Z., Kabildjanov A.S., Ismailov S.Y. Robastnaya identifikasiya orositelnix sistem v selskom xozyaystve// Jurnal «Problemi informatiki i energetiki», Tashkent, №3, 2022. - C. 11-15.
5. Kabildjanov A.S. Boshqarish tizimlarini kompyuter modellashtirish. O‘quv qo‘llanma. Toshkent-2024.
6. Russell E. McMahon, Otabek M. Ismailov, Charos Z. Okhunboboyeva. The place and role of creative education in the context of digital education// Creative education: innovation and effectiveness, Tashkent, 2024. - C. 63-66.

ISSN 3030-3907