**DOI: https://doi.org/10.5281/zenodo.15003453**

# RANSOMWARE HUJUMLARI: SHAXSIY VA KORPORATIV MA'LUMOTLARNI QANDAY HIMOYA QILISH MUMKIN?

**Sharofiddinov Husan Sirojiddinovich**
Talaba, Toshkent axborot texnologiyalari universiteti
Samarqand filiali
Samarqand, O'zbekiston
sharofiddinovhusan@gmail.com

**Aliqulova Hosila Akramovna**
Talaba, Toshkent axborot texnologiyalari universiteti
Samarqand filiali
Samarqand, O'zbekiston
hosilaaliqulova@gmail.com

**Xiysova Sevinch Rustamovna**
Talaba, Toshkent axborot texnologiyalari universiteti
Samarqand filiali
Samarqand, O'zbekiston
xiyasovasevinch@gmail.com

**Axtamov Safar Solejonovich**
Talaba, Toshkent axborot texnologiyalari universiteti
Samarqand filiali
Samarqand, O'zbekiston
sharofiddinovhusan921@gmail.com

***Annotatsiya:*** *Bugungi kunda raqamli texnologiyalar hayotimizning ajralmas qismiga aylangan. Internetdan foydalanish imkoniyatlari ortib borishi bilan birga, kiberjinoyatlar ham ko'payib bormoqda. Kiberjinoyatlar shaxsiy ma'lumotlarni o'g'irlash, moliyaviy firibgarlik, kompyuter tizimlariga buzib kirish va zararli dasturlarni tarqatish kabi ko'plab xatarlarni o'z ichiga oladi. Shunday ekan, kiberxavfsizlikni ta'minlash va o'zimizni himoya qilish muhim ahamiyat kasb etadi.*

***Kalit so'zlar:*** *Ransomware,DDoS hujumlari, fishing xabarlari, VPN, firewall, moliyaviy firibgarlik, antivirus.*

**Eng kuchli kiberjinoyat: Ransomware (Fidye dasturi) hujumlari**

Ransomware – bu eng xavfli kiberjinoyatlardan biri bo‘lib, xakerlar zararli dasturlar orqali qurilmalardagi ma’lumotlarni shifrlaydi va ularni qayta tiklash uchun foydalanuvchilardan pul talab qiladi. Ushbu hujumlar ko‘pincha kompaniyalar, kasalxonalar, davlat tashkilotlari va oddiy foydalanuvchilarni nishonga oladi.

**Ransomware hujumlari qanday amalga oshiriladi?**

1. Fishing xabarlari – firibgarlar elektron pochta yoki xabar orqali zararli fayllarni jo‘natib, foydalanuvchini ushbu faylni ochishga undaydi.
2. Zararli dasturlar – noma’lum manbalardan yuklab olingan dasturlar orqali tizimga zarar yetkaziladi.
3. Zaxira nusxalarini yo‘q qilish – xakerlar kompyuter tizimiga kirgandan so‘ng, barcha zaxira ma’lumotlarini o‘chirib yuboradi.
4. Shifrlash va to‘lov talabi – tizimdagi barcha fayllar shifrlanadi va ularni ochish uchun ma’lum miqdorda kriptovalyutada pul talab qilinadi.

**Ransomware hujumlaridan qanday himoyalanish mumkin?**

1. Muhim ma’lumotlarning zaxirasini yaratish – muhim fayllarni doimiy ravishda tashqi xotira qurilmalari yoki bulut xizmatlarida saqlash.
2. Antivirus va xavfsizlik devorlaridan foydalanish – kuchli antivirus dasturlarini o‘rnatish va ularni muntazam yangilash.
3. Elektron pochta xabarlariga ehtiyot bo‘lish – noma’lum jo‘natuvchilardan kelgan fayllarni ochmaslik.
4. Tizim va dasturlarni yangilash – operatsion tizim va dasturlarni muntazam ravishda yangilab turish, chunki yangilanishlar xavfsizlik zaifliklarini bartaraf etadi.
5. VPN va xavfsiz internet tarmog‘idan foydalanish – ochiq Wi-Fi tarmoqlaridan foydalanishda ehtiyotkor bo‘lish va VPN xizmatlaridan foydalanish.
6. Kiberxavfsizlik bo‘yicha xabardorlikni oshirish – foydalanuvchilar va kompaniya xodimlarini kiberjinoyatlar haqida xabardor qilish va ularni himoyalanish choralariga o‘rgatish.

**Kiberjinoyatlar turlari va ularning oldini olish usullari**

1. Shaxsiy ma’lumotlarni o‘g‘irlash – bu turdagi hujumlar foydalanuvchilarning login, parol va boshqa maxfiy ma’lumotlarini noqonuniy ravishda qo‘lga kiritishga qaratilgan.

Himoyalanish usullari:

1) Murakkab va uzoq parollardan foydalanish.
2) Har bir xizmat uchun alohida parol yaratish.
3) Shubhali havolalar va phishing sahifalariga kirmaslik.
4) Ikki bosqichli autentifikatsiyani yoqish.

2. Moliyaviy firibgarlik – soxta internet do‘konlari yoki xakerlik usullari orqali odamlarning pul mablag‘larini o‘g‘irlash.

Himoyalanish usullari:

1) Internet-do‘konlardan xarid qilishdan oldin ularning ishonchliligini tekshirish.
2) Moliyaviy tranzaksiyalarni faqat rasmiy va himoyalangan sahifalarda amalga oshirish.
3) Bank kartasi ma’lumotlarini noma’lum shaxslarga bermaslik.
4) Bankdan kelgan SMS yoki elektron pochta xabarlaridagi havolalarga shubha bilan qarash.

3. Fishing (Phishing) – elektron pochta yoki xabarlar orqali foydalanuvchilarni aldab, ularning maxfiy ma’lumotlarini olish.

Himoyalanish usullari:

1) Elektron pochta orqali kelgan shubhali xabarlarni tekshirish.
2) Rasmiy manbalardan kelmagan havolalarni ochmaslik.
3) Brauzerda HTTPS bilan boshlanuvchi xavfsiz sahifalarga ustunlik berish.
4) Antivirus dasturlarining fishing himoyasidan foydalanish.

4. DDoS hujumlari – veb-sayt yoki serverlarga ortiqcha yuklama berib, ularning ishlashini izdan chiqarish.

Himoyalanish usullari:

1) Kuchli xavfsizlik devorlari (firewall) va DDoS himoya xizmatlaridan foydalanish.
2) Serverlarni doimiy ravishda yangilab turish va monitoring qilish.
3) Resurslarni ortiqcha yuklamadan saqlash uchun xavfsiz tarmoq konfiguratsiyasini amalga oshirish.

**Xulosa**

Ransomware hujumlari bugungi kunda eng xavfli kiberjinoyatlardan biri bo‘lib, ularning oldini olish uchun ehtiyot choralarini ko‘rish juda muhim. Muhim ma’lumotlarni doimiy ravishda zaxiralash, antivirus dasturlaridan foydalanish, elektron pochta xabarlariga ehtiyotkorlik bilan yondashish kabi chora-tadbirlar orqali ransomware hujumlaridan himoyalanish mumkin. Umuman olganda, har bir inson va tashkilot kiberxavfsizlik qoidalariga qat’iy rioya qilish orqali o‘z ma’lumotlarini himoya qilishi lozim.

## FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. (2020). Computer Security: Principles and Practice. Pearson.
2. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
3. Kaspersky Lab (2023). "Cybersecurity Tips and Best Practices." www.kaspersky.com.
4. OWASP Foundation (2023). "Top 10 Web Application Security Risks." www.owasp.org.
5. Symantec Corporation (2022). "Internet Security Threat Report." www.symantec.com.