DOI: https://doi.org/10.5281/zenodo.13270782

BANK TO‘LOV TIZIMIGA BO‘LADIGAN RAQAMLI HUJUMLAR VA ULARNI TAHLILI

Jo‘ramirzayev I.A., Ibodullayeva S.O., Mardonov S.F., Tursunov F.F.

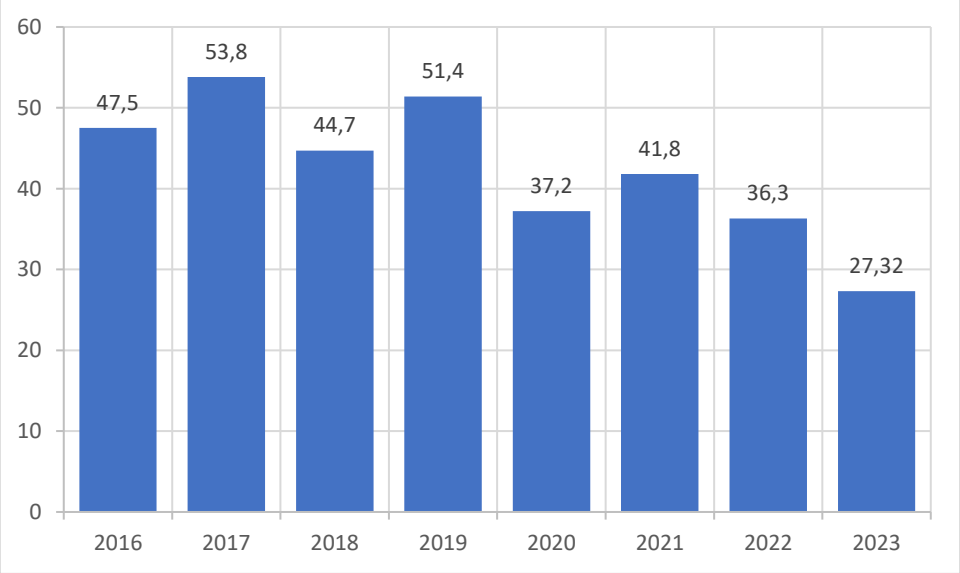
Annotatsiya: *Ushbu maqolada banklar va moliyaviy muassasalar uchun kiber xavflarni tushuntirish, ular bilan kurashish va kiberxavfsizlikni ta’minlashdagi muhimliklarini aks ettiradi.*

Kalit so‘zlar: *Raqamli hujumlar, maxfiy moliyaviy ma’lumotlar, kiber tahdidlar, moliyaviy yo‘qotishlar, normativ muvofiqlik, operatsion amallardagi uzilishlar, ma’lumotlar buzilishi, ma’lumotlar ushlash, zaifliklardan foydalanish, soxta operatsiyalar.*

Bank tizimlariga raqamli hujumlar maxfiy moliyaviy ma’lumotlar va xizmatlarning maxfiyligi, yaxlitligi va mavjudligini buzishga qaratilgan kiber tahdidlarning keng doirasini qamrab oladi.

Bank tizimlariga bo‘ladigan raqamli hujum turlari:

1. Fishing: fishing hujumlari foydalanuvchilarni kirish ma’lumotlari yoki moliyaviy ma’lumotlar kabi nozik ma’lumotlarni oshkor qilish uchun aldash yo‘li bilan qonuniy shaxslarni taqlid qiladigan firibgar elektron pochta xabarlari, SMS xabarlar yoki veb-saytlarni o‘z ichiga oladi.



1.8-rasm. 2016 yildan 2023 yilgacha butun dunyoda moliyaviy fishing hujumlari ulushi [https://www.statista.com/statistics/1319867/share-of-financial-phishing-attacks/]

2. Zararli dastur: viruslar, qurtlar, troyanlar va to‘lov dasturlari, shu jumladan zararli dastur bank tizimlariga kirib borish, maxfiy ma’lumotlarni o‘g‘irlash yoki operatsiyalarni buzish uchun mo‘ljallangan zararli dasturdir.

3. Xizmatni rad etish (DoS) va tarqatilgan xizmatni rad etish (DDoS): DoS va DDoS hujumlari bank veb-saytlari yoki tarmoqlarini trafik ortib ketishi bilan ularni qonuniy foydalanuvchilar uchun mavjud emas va xizmatlarning buzilishiga olib keladi.

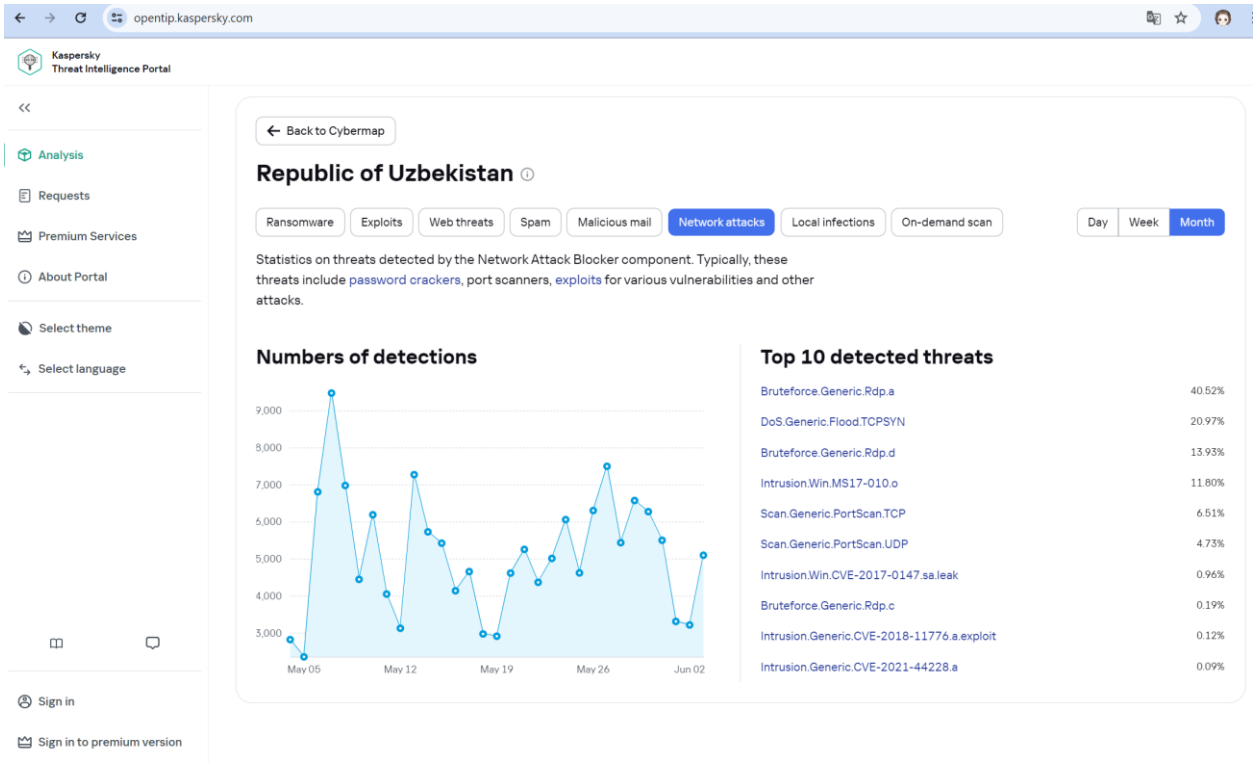
4. Insider tahdidlari: Insider tahdidlari bank tizimlariga kirish huquqiga ega bo‘lgan xodimlar, pudratchilar yoki biznes sheriklarining zararli yoki beparvo harakatlarini o‘z ichiga oladi, natijada ma’lumotlar buziladi, firibgarlik yoki ma’lumotlar sizib chiqishiga olib keladi.

5. SQL Injection: SQL injection hujumlari zararli SQL so‘rovlarini bajarish uchun veb-ilovalar yoki ma’lumotlar bazalaridagi zaifliklardan foydalanadi, bu esa tajovuzkorlarga backend tizimlarida saqlangan nozik ma’lumotlarga kirish yoki boshqarish imkonini beradi.

6. O‘rtada turgan odam (MitM, Men-in-the-Middle): MitM hujumlari bank tizimlari va foydalanuvchilar o‘rtasidagi aloqani ushlab oladi va boshqaradi, bu esa tajovuzkorlarga nozik operatsiyalarni tinglash, ma’lumotlarni o‘zgartirish yoki hisob ma’lumotlarini o‘g‘irlash imkonini beradi.

7. Hisob ma’lumotlarini to‘ldirish: hisob ma’lumotlarini to‘ldirish hujumlari avtomatlashtirilgan kirish urinishlari orqali bank hisob raqamlariga ruxsatsiz kirish uchun bitta veb-saytdan o‘g‘irlangan yoki sizdirilgan hisob ma’lumotlarini ishlatadi.

8. ATM Skimming: ATM skimming karta ma’lumotlarini va PIN kodlarini olish uchun bankomatlarga noqonuniy qurilmalarni o‘rnatishni o‘z ichiga oladi, bu jinoyatchilarga kartalarni klonlash va mablag‘larni firibgarlik yo‘li bilan olish imkonini beradi.



1.9-rasm. Tarmoq hujumlari statistikasi
[https://statistics.securelist.com/country/uzbekistan/intrusion-detection-scan/month]

Bank tizimlariga raqamli hujumlar turli xil yo‘llar bilan amalaga oshiriladi, jumladan, ijtimoiy muhandislik, zaifliklardan foydalanish, ma’lumotlarni ushlab olish, soxta operatsiyalar usullari kirishi mumkin:

- ijtimoiy muhandislik: ko‘pgina raqamli hujumlar foydalanuvchilarni yoki xodimlarni maxfiy ma’lumotlarni oshkor qilish, zararli havolalarni bosish yoki zararli dasturlarni yuklab olish uchun aldash yo‘li bilan ijtimoiy muhandislik texnikasiga tayanadi.

- zaifliklardan foydalanish: tajovuzkorlar ruxsatsiz kirish yoki hujumlarni amalga oshirish uchun bank tizimlari, tarmoqlar yoki ilovalardagi zaifliklardan, masalan, tuzatilmagan dasturiy ta’minot, noto‘g‘ri tuzilgan serverlar yoki zaif autentifikatsiya mexanizmlaridan foydalanadilar.

- ma’lumotlarni ushlash: tajovuzkorlar zararli maqsadlar uchun kirish ma’lumotlari, hisob raqamlari yoki tranzaksiya tafsilotlari kabi maxfiy ma’lumotlarni olish uchun tarmoq trafigi yoki aloqa kanallarini ushlab, tahlil qiladi.

- soxta operatsiyalar: raqamli hujumlar soxta operatsiyalarni o‘z ichiga olishi mumkin, ya’ni tajovuzkorlar pul o‘tkazish, xarid qilish yoki noqonuniy faoliyatni amalga oshirish uchun o‘g‘irlangan hisob ma’lumotlari yoki buzilgan hisoblardan foydalanadilar.

Raqamli hujumlar bank tizimlariga ko‘plab ta’sirlar ko‘rsatishi mumkin, masalan, moliyaviy yo‘qotishlar, obro‘ga zarar yetishi, operatsion amallardagi uzilishlar, ma’lumotlar buzilishi, normative muvofiqlik kabi zararli ta’sirlarni ko‘rsatishimi mumkin:

- moliyaviy yo‘qotishlar: raqamli hujumlar banklar uchun to‘g‘ridan-to‘g‘ri moliyaviy yo‘qotishlarga olib kelishi mumkin, jumladan o‘g‘irlangan mablag‘lar, firibgarlik operatsiyalari, tartibga soluvchi jarimalar va ma’lumotlar buzilishi yoki muvofiqlikni buzish bilan bog‘liq huquqiy xarajatlar.

- obro‘ga zarar yetishi: xavfsizlikning buzilishi va kiberhujumlar mijozlar, investorlar va manfaatdor tomonlar o‘rtasidagi banklarning obro‘si va ishonchiga putur etkazishi mumkin, bu esa mijozlarning ishdan chiqishiga, tovar eroziyasiga va bozor ulushining yo‘qolishiga olib keladi.

- operatsion amallardagi uzilishlar: raqamli hujumlar tufayli bank xizmatlarining uzilishi, masalan, veb-sayt ishdan chiqishi, bankomatlarning nosozliklari yoki to‘lovlarni qayta ishlashda nosozliklar mijozlar ehtiyojini qondirish, daromad oqimlari va biznesning uzluksizligiga ta’sir qilishi mumkin.

- ma’lumotlar buzilishi: raqamli hujumlar ma’lumotlar buzilishiga olib kelishi mumkin, bunday shaxsiy aniqlash ma’lumotlar (PII- personal identifiable information), hisobga olish ma’lumotlari va moliyaviy yozuvlar kabi nozik mijoz ma’lumotlarni ruxsatsiz shaxslarga fosh etilishi o‘g‘irlanishi natijasida, firibgarlik, va normativ jazolarga olib keladi.

- normativ muvofiqlik: banklar mijozlar ma’lumotlarini himoya qilmaslik, ma’lumotlar maxfiyligi qoidalariga rioya qilmaslik yoki xavfsizlik hodisalari haqida o‘z vaqtida xabar berish, ularning moliyaviy salomatligi va operatsion barqarorligiga ta’sir ko‘rsatmaganliklari uchun tartibga solish tekshiruvi, jarimalar va qo‘shimcha pul undurishlariga duch kelishi mumkin.

Raqamli hujumlar bank tizimlariga jiddiy tahdid soladi, turli xil hujum vektorlari nozik moliyaviy ma’lumotlar, xizmatlar va infratuzilmaga qaratilgan. Raqamli hujumlarning turlari, usullari va ta’sirini tushunib, banklar tahdidlardan himoya qilish va kiber jinoyatlar bilan bog‘liq xavflarni kamaytirish uchun kuchli kiberxavfsizlik choralarini qo‘llashlari mumkin.

Xulosa

Raqamli hujumlar banklar uchun moliyaviy yo‘qotishlar, operatsion uzilishlar, ma’lumotlar buzilishi va normativ muvofiqlik kabi zararli ta’sirlarni tugatishi mumkin. Bu sababli, banklar kiberxavfsizlik choralarini oshirish va ta’sirlarini kamaytirish uchun kuchli kiberxavfsizlik tedbirlerini qo‘llashi kerak.

FOYDALANILGAN ADABIYOTLAR

1. Whitman, Michael E., and Herbert J. Mattord. "Principles of Information Security." Cengage Learning, 2018.

2. Pfleeger, Charles P., and Shari Lawrence Pfleeger. "Security in Computing." Pearson Education, 2015.

3. Whitman, Michael E., et al. "Management of Information Security." Cengage Learning, 2018.

4. Scarfone, Karen, and Murugiah Souppaya. "Guide to Computer Security Certification and Accreditation." CRC Press, 2006.

5. NIST Special Publication 800-37 Revision 2: "Risk Management Framework for Information Systems and Organizations." National Institute of Standards and Technology, 2018.

6. Anderson, James A., and Peter D. Nash. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2008.

7. NIST Special Publication 800-53 Revision 5: "Security and Privacy Controls for Information Systems and Organizations." National Institute of Standards and Technology, 2020.

8. Carroll, John M., et al. "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies." McGraw-Hill, 2014.

9. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11: "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products." Committee on National Security Systems, 2010.

10. Chapple, Mike, et al. "CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide." Sybex, 2018.

11. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 6: "National Policy for Telecommunications and Automated Information Systems Security." Committee on National Security Systems, 2003.

12. Schou, Corey, and Steven Hernandez. "Information Assurance for the Enterprise: A Roadmap to Information Security." McGraw-Hill, 2007.

13. National Institute of Standards and Technology. "Security Standards for Federal Information Systems and Organizations." National Institute of Standards and Technology, various editions.