JOSUSLIK DASTURLARI VA BANK TROYANLARI: MOLIYAVIY MA’LUMOTLARNING O‘G‘IRLANISHI

Samarqand iqtisodiyot va servis instituti

"XALQARO IQTISODIY MUNOSABATLAR" fakulteti

Iqtisodiy xavfsizlik yo‘nalishi

IKX-123 4-KURS

Abdusalomova Sevinch Bozorboy qizi

+998990942500

sevinchabdusalomova2500@gmail.com

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrasi asistenti

Rustamov Sherzod Norxudjayevich

Annotatsiya. Maqolada josuslik dasturlari (spyware) va bank troyanlarining moliyaviy ma’lumotlarni o‘g‘irlash mexanizmlari, ularning evolyutsiyasi va himoya choralari tahlil qilinadi. Tadqiqotning dolzarbligi raqamli bank xizmatlari va mobil to‘lovlarning keng tarqalishi bilan bog‘liq: foydalanuvchining qurilmasi moliyaviy ma’lumotlarni o‘g‘irlash uchun asosiy nishonga aylandi. Tadqiqotda tizimli va qiyosiy tahlil, normativ-huquqiy hujjatlarni o‘rganish, xalqaro ilmiy nashrlar va rasmiy hisobotlarni kontent-tahlil qilish hamda hujum samaradorligini miqdoriy baholash usullaridan foydalanildi. Natijada hujum vektorlari (keylogging, veb-inyeksiya, brauzerdagi odam hujumi, ekran ustiga qoplama, SMS-kodlarni ushlash) tasniflandi, bir omilli autentifikatsiyaning yetarli emasligi asoslandi, hujum zanjirining har bir bosqichiga mos himoya vositalari muvofiqlashtirildi va ko‘p qatlamli himoya modeli taklif etildi. Maqola yakunida normativ bazani takomillashtirish bo‘yicha takliflar hamda banklar va foydalanuvchilar uchun amaliy tavsiyalar berilgan.

Kalit so‘zlar: josuslik dasturlari, bank troyanlari, moliyaviy ma’lumotlar, kiberxavfsizlik, mobil bank, keylogging, brauzerdagi odam hujumi, ko‘p omilli autentifikatsiya, zararli dasturlar, firibgarlik.

SPYWARE AND BANKING TROJANS: THEFT OF FINANCIAL DATA

Abstract. The article analyzes how spyware and banking trojans steal financial data, their evolution, and protective measures. The relevance of the study is determined by the spread of digital banking and mobile payments: the user’s device has become the main target for financial data theft. The research employed systematic and comparative analysis, the study of regulatory and legal acts, content analysis of international scholarly publications and official reports, and quantitative estimation of attack effectiveness. As a result, attack vectors (keylogging, web injection, man-in-the-browser, screen overlay, and SMS interception) were classified, the insufficiency of single-factor authentication was substantiated, defenses were mapped to each stage of the attack chain, and a multi-layered protection model was proposed. In conclusion, proposals for improving the regulatory framework and practical recommendations for banks and users are presented.

Keywords: spyware, banking trojans, financial data, cybersecurity, mobile banking, keylogging, man-in-the-browser, multi-factor authentication, malware, fraud.

KIRISH

Raqamli bank xizmatlari va mobil to‘lovlarning kengayishi moliyaviy ma’lumotlarni o‘g‘irlashga qaratilgan zararli dasturlarning ham ko‘payishiga sabab bo‘ldi. Josuslik dasturi foydalanuvchi bilmagan holda uning faoliyati va ma’lumotlarini yig‘adi; bank troyani esa bank mijozlarining kirish ma’lumotlari va tranzaksiyalarini nishonga oladi. Ularning ommaviy tarqalishi Moshchuk va hammualliflarining veb-saytlardagi josuslik dasturlari bo‘yicha tadqiqotida ham qayd etilgan.[1]

[1] Moshchuk A., Bragin T., Gribble S. D., Levy H. M. A Crawler-based Study of Spyware on the Web // Proceedings of the Network and Distributed System Security Symposium (NDSS 2006). – Internet Society, 2006.

Mavzu konstitutsiyaviy jihatdan ham dolzarb: O‘zbekiston Respublikasi Konstitutsiyasining 2023-yil 30-aprelda qabul qilingan yangi tahririda shaxsiy hayot, shaxsga doir ma’lumotlar va mol-mulk daxlsizligi kafolatlangan.[2] Prezidentning 2020-yil 5-oktyabrdagi PF-6079-son Farmoni bilan tasdiqlangan «Raqamli O‘zbekiston – 2030» strategiyasi esa raqamli xizmatlarni kengaytirish bilan birga axborot xavfsizligini ta’minlashni ham vazifa qilib qo‘ygan.[3]

So‘nggi yillarda qabul qilingan qonunlar mavzu bilan bevosita bog‘liq. 2022-yil 15-apreldagi O‘RQ-764-son «Kiberxavfsizlik to‘g‘risida»gi Qonun kiberxavfsizlikni ta’minlash tamoyillari, subyektlarning vakolatlari va kiberhodisalarga javob berish asoslarini belgilaydi.[4] 2019-yil 2-iyuldagi O‘RQ-547-son «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun operatorlarning ma’lumotlarni himoya qilish majburiyatlarini belgilaydi, o‘g‘irlangan moliyaviy ma’lumotlar esa aynan shu qonun doirasidagi ma’lumotlardir.[5] «Banklar va bank faoliyati to‘g‘risida»gi O‘RQ-580-son Qonun bank sirini himoyalaydi,[6] «To‘lovlar va to‘lov tizimlari to‘g‘risida»gi O‘RQ-578-son Qonun esa to‘lov xizmatlari va to‘lov tizimlari faoliyatini tartibga soladi.[7] Zararli dasturlarni yaratish,

[2] O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahrir). – URL: https://lex.uz

[3] O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi PF-6079-son Farmoni bilan tasdiqlangan «Raqamli O‘zbekiston – 2030» strategiyasi. – URL: https://lex.uz

[4] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – URL: https://lex.uz

[5] O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. – URL: https://lex.uz

[6] O‘zbekiston Respublikasining 2019-yil 5-noyabrdagi O‘RQ-580-son «Banklar va bank faoliyati to‘g‘risida»gi Qonuni. – URL: https://lex.uz

[7] O‘zbekiston Respublikasining 2019-yil 1-noyabrdagi O‘RQ-578-son «To‘lovlar va to‘lov tizimlari to‘g‘risida»gi Qonuni. – URL: https://lex.uz

tarqatish va kompyuter axborotini ruxsatsiz olish uchun javobgarlik Jinoyat kodeksining «Axborot texnologiyalari sohasidagi jinoyatlar» bobida belgilangan.[8]

Tadqiqotning maqsadi moliyaviy ma’lumotlarni o‘g‘irlovchi zararli dasturlarning ish mexanizmini tizimlashtirish va himoya modelini asoslashdir. Gipoteza: hujum zanjirining bitta bosqichiga qaratilgan himoya yetarli emas, samarali himoya zanjirning bir nechta bosqichini birdaniga to‘sishi kerak.

ASOSIY QISM

Bank troyanlarining klassik namunasi Zeus bo‘lib, Binsalleeh va hammualliflari uning tuzilishini tahlil qilib, dastur boshqaruv serveri, sozlash fayli va brauzerga kirib, tanlangan bank sahifalariga qo‘shimcha shakl maydonlari qo‘shish (web injection) imkoniyatiga ega ekanini ko‘rsatgan.[9] Bunday dasturlar botnet tarkibida ishlaydi: Stone-Gross va hammualliflari Torpig botnetini nazoratga olib, kuzatuv davomida katta hajmdagi bank va karta ma’lumotlari, jumladan yuzlab moliya muassasalari hisoblarining kirish ma’lumotlari o‘g‘irlanganini aniqlagan.[10] Hujumning muhim turi — «brauzerdagi odam» (man-in-the-browser) hujumi: zararli kod brauzer ichida ishlagani uchun TLS kanali buzilmasa ham, foydalanuvchi ko‘rayotgan va yuborayotgan ma’lumotni o‘zgartira oladi, masalan, to‘lov oluvchisini almashtiradi.[11] Shu sababli kanal shifrlash (HTTPS) o‘zi qurilma zararlangan bo‘lsa himoya bermaydi.

[8] O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr), XX¹ bob «Axborot texnologiyalari sohasidagi jinoyatlar». – URL: https://lex.uz

[9] Binsalleeh H., Ormerod T., Boukhtouta A., Sinha P., Youssef A., Debbabi M., Wang L. On the Analysis of the Zeus Botnet Crimeware Toolkit // 2010 Eighth Annual International Conference on Privacy, Security and Trust (PST). – IEEE, 2010. – P. 121–128.

[10] Stone-Gross B., Cova M., Cavallaro L., Gilbert B., Szydlowski M., Kemmerer R., Kruegel C., Vigna G. Your Botnet Is My Botnet: Analysis of a Botnet Takeover // Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS’09). – New York: ACM, 2009. – P. 635–647.

[11] Dougan T., Curran K. Man in the Browser Attacks // International Journal of Ambient Computing and Intelligence. – 2012. – Vol. 4, No. 1. – P. 29–39.

Mobil qurilmalarda hujum yo‘nalishi o‘zgaradi. Zhou va Jiang Android zararli dasturlarini tahlil qilib, ularning ko‘pchiligi qonuniy ilovalar ichiga joylashtirilib tarqalishini va maxfiy ma’lumot yig‘ish, SMS xabarlarini ushlash kabi imkoniyatlarga ega ekanini ko‘rsatgan.[12] Fratantonio va hammualliflarining «Cloak and Dagger» tadqiqoti foydalanuvchi interfeysi ustiga qoplama chizish va maxsus imkoniyatlar ruxsatidan foydalanib, foydalanuvchi kiritayotgan ma’lumotni kuzatish va boshqarish mumkinligini ko‘rsatgan; bu bank ilovasi ustiga soxta kirish oynasini qo‘yadigan troyanlar mantiqiga mos keladi.[13] SMS orqali yuboriladigan bir martalik kodlar ham xavfsizlikni to‘liq ta’minlamaydi: NIST SP 800-63B ommaviy telefon tarmog‘i orqali yuboriladigan kodlarni «cheklangan» autentifikator sifatida tasniflab, qurilmaga ruxsatsiz kirish xavfini hisobga olishni talab qiladi.[14] Zararli dasturlarni aniqlash tomonida Arp va hammualliflarining Drebin tizimi ilovaning ruxsatlari va chaqiriqlari kabi statik belgilariga asoslanib, zararli Android ilovalarini yuqori aniqlikda topish mumkinligini ko‘rsatgan.[15]

Moliyaviy zararning miqyosi haqida AQSh Federal tergov byurosining Internet jinoyatlari markazi 2023-yil uchun hisobotida kiberjinoyatlardan xabar qilingan umumiy zarar o‘n milliard dollardan ortiq ekanini ko‘rsatgan; bu raqam faqat troyanlarga tegishli emas, shuningdek ko‘p qurbonlar xabar bermaydi.[16] Himoya samaradorligini ko‘rsatish uchun muallif faraziy hisob-kitob keltiradi (bu real statistika emas). Hujum muvaffaqiyati zanjir bosqichlari ehtimollarining ko‘paytmasi deb olinsin: qurilmaning zararlanishi 0,10; kirish ma’lumotlarining olinishi 0,80; bir martalik kodning chetlab o‘tilishi 0,50; firibgar

[12] Zhou Y., Jiang X. Dissecting Android Malware: Characterization and Evolution // 2012 IEEE Symposium on Security and Privacy. – IEEE, 2012. – P. 95–109.

[13] Fratantonio Y., Qian C., Chung S. P., Lee W. Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop // 2017 IEEE Symposium on Security and Privacy. – IEEE, 2017. – P. 1041–1057.

[14] Grassi P. A., Garcia M. E., Fenton J. L. et al. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. – Gaithersburg: NIST, 2017.

[15] Arp D., Spreitzenbarth M., Hübner M., Gascon H., Rieck K. Drebin: Effective and Explainable Detection of Android Malware in Your Pocket // Network and Distributed System Security Symposium (NDSS 2014). – Internet Society, 2014.

[16] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). Internet Crime Report 2023. – Washington, D.C.: FBI, 2024. – URL: https://www.ic3.gov

tranzaksiyaning o‘tishi 0,60. Unda umumiy ehtimol 0,10 × 0,80 × 0,50 × 0,60 = 0,024, ya’ni 2,4 foiz. Agar bank operatsiya summasi va oluvchisini alohida tasdiqlashni joriy etib, oxirgi ehtimolni 0,10 ga tushirsa, natija 0,10 × 0,80 × 0,50 × 0,10 = 0,004, ya’ni 0,4 foiz bo‘ladi: xavf olti marta kamayadi. Bu hisob gipotezamizni tasdiqlaydi: bir bosqichdagi kuchli to‘siq butun zanjir samaradorligini keskin kamaytiradi, ammo bir nechta bosqichni to‘sish eng ishonchli yo‘ldir.

Josuslik dasturlarining o‘ziga xos xavfi shundaki, ular odatda sezilmaydi va uzoq muddat ishlaydi. Klaviatura kiritilishini yozib oluvchi (keylogger), ekran tasvirini oluvchi va buferdan nusxa oluvchi modullar foydalanuvchi karta raqami, CVV-kod, parol va bir martalik kodni kiritayotgan paytda ularni qo‘lga kiritadi; bank ilovasi o‘zi xavfsiz bo‘lsa ham, zararlangan qurilmada kiritish bosqichining o‘zi himoyasiz qoladi. Shu sababli moliyaviy ma’lumotlarning o‘g‘irlanishi ko‘pincha bir martalik emas, balki bosqichma-bosqich jarayondir: avval qurilma zararlanadi, keyin ma’lumot yig‘iladi, so‘ngra qo‘lga kiritilgan hisobdan firibgarlik tranzaksiyasi amalga oshiriladi. Huquqiy nuqtayi nazardan bu jarayonning har bir bosqichi yuqorida tahlil qilingan normalar bilan bog‘lanadi: zararli dasturni tarqatish — Jinoyat kodeksi bobi bilan, ma’lumotlarning oshkor bo‘lishi — shaxsga doir ma’lumotlar to‘g‘risidagi qonun bilan, bankning himoya majburiyati esa bank va kiberxavfsizlik qonunlari bilan. Banklar uchun bundan amaliy xulosa kelib chiqadi: foydalanuvchi qurilmasi ishonchsiz muhit deb qabul qilinib, tranzaksiya xavfsizligi server tomonida ham tekshirilishi kerak.

Xalqaro tajribada ana shunday yondashuv me’yoriy darajada mustahkamlangan. Yevropa Ittifoqining 2018/389-sonli Delegirlangan reglamenti kuchaytirilgan mijoz autentifikatsiyasi talablarini va tranzaksiyani summa hamda oluvchi bilan dinamik bog‘lashni belgilaydi, bu esa brauzerdagi odam hujumi orqali oluvchini almashtirishni qiyinlashtiradi.[17] Shu asosda muallif besh qatlamli himoyani taklif etadi: qurilma qatlamida

[17] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication // Official Journal of the European Union. – L 69, 13.3.2018.

tizim va ilovalarni yangilash hamda faqat rasmiy do‘konlardan o‘rnatish; ilova qatlamida qoplamani aniqlash va xavfli muhitni tekshirish; autentifikatsiya qatlamida SMS-kodlarni tobora kuchliroq vositalar (ilova asosidagi yoki apparat kalit) bilan almashtirish; tranzaksiya qatlamida summa va oluvchini alohida tasdiqlash hamda g‘ayrioddiy operatsiyalarni monitoring qilish; tashkiliy qatlamda mijozlarni fishing va noma’lum ilovalar xavfi haqida muntazam xabardor qilish.

XULOSA

Tadqiqot natijasida shunday xulosaga kelindi: josuslik dasturlari va bank troyanlari moliyaviy ma’lumotlarni qurilma darajasida, ya’ni kanal shifrlanganidan keyin o‘g‘irlaydi, shuning uchun faqat HTTPS yoki bir omilli autentifikatsiyaga tayanish yetarli emas. Faraziy modelda bitta kuchli bosqichli to‘siq (tranzaksiyani dinamik tasdiqlash) xavfni sezilarli kamaytirdi, ko‘p qatlamli yondashuv esa eng ishonchli yo‘l hisoblanadi.

Takliflar: 1) banklar uchun SMS-kodlardan kuchliroq autentifikatsiya va tranzaksiyani summa hamda oluvchi bilan bog‘lab tasdiqlash tamoyilini joriy etish; 2) mobil bank ilovalarida qoplama va xavfli muhitni aniqlash funksiyalarini kiritish; 3) vakolatli organlar tomonidan moliyaviy zararli dasturlar hodisalari bo‘yicha anonim statistikani e’lon qilish; 4) aholi raqamli savodxonligi dasturlariga qurilma xavfsizligi bo‘yicha modul qo‘shish. Kelgusi tadqiqotlar mahalliy sharoitdagi hodisalar bo‘yicha empirik ma’lumotlar asosida taklif etilgan modelni sinashga yo‘naltirilishi lozim.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Moshchuk A., Bragin T., Gribble S. D., Levy H. M. A Crawler-based Study of Spyware on the Web // Proceedings of the Network and Distributed System Security Symposium (NDSS 2006). – Internet Society, 2006.

2. O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahrir). – URL: https://lex.uz

3. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi PF-6079-son Farmoni bilan tasdiqlangan «Raqamli O‘zbekiston – 2030» strategiyasi. – URL: https://lex.uz

4. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – URL: https://lex.uz

5. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. – URL: https://lex.uz

6. O‘zbekiston Respublikasining 2019-yil 5-noyabrdagi O‘RQ-580-son «Banklar va bank faoliyati to‘g‘risida»gi Qonuni. – URL: https://lex.uz

7. O‘zbekiston Respublikasining 2019-yil 1-noyabrdagi O‘RQ-578-son «To‘lovlar va to‘lov tizimlari to‘g‘risida»gi Qonuni. – URL: https://lex.uz

8. O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr), XX[1] bob «Axborot texnologiyalari sohasidagi jinoyatlar». – URL: https://lex.uz

9. Binsalleeh H., Ormerod T., Boukhtouta A., Sinha P., Youssef A., Debbabi M., Wang L. On the Analysis of the Zeus Botnet Crimeware Toolkit // 2010 Eighth Annual International Conference on Privacy, Security and Trust (PST). – IEEE, 2010. – P. 121–128.

10. Stone-Gross B., Cova M., Cavallaro L., Gilbert B., Szydlowski M., Kemmerer R., Kruegel C., Vigna G. Your Botnet Is My Botnet: Analysis of a Botnet Takeover // Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS’09). – New York: ACM, 2009. – P. 635–647.

11. Dougan T., Curran K. Man in the Browser Attacks // International Journal of Ambient Computing and Intelligence. – 2012. – Vol. 4, No. 1. – P. 29–39.

12. Zhou Y., Jiang X. Dissecting Android Malware: Characterization and Evolution // 2012 IEEE Symposium on Security and Privacy. – IEEE, 2012. – P. 95–109.

13. Fratantonio Y., Qian C., Chung S. P., Lee W. Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop // 2017 IEEE Symposium on Security and Privacy. – IEEE, 2017. – P. 1041–1057.

14. Grassi P. A., Garcia M. E., Fenton J. L. et al. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. – Gaithersburg: NIST, 2017.

15. Arp D., Spreitzenbarth M., Hübner M., Gascon H., Rieck K. Drebin: Effective and Explainable Detection of Android Malware in Your Pocket // Network and Distributed System Security Symposium (NDSS 2014). – Internet Society, 2014.

16. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). Internet Crime Report 2023. – Washington, D.C.: FBI, 2024. – URL: https://www.ic3.gov

17. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication // Official Journal of the European Union. – L 69, 13.3.2018.