SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

TELEGRAM ORQALI TARQALAYOTGAN APK VIRUSLARGA QARSHI CHORALAR

A.A. Iminov

O'zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig'i

Anvarov Jasurbek Akram o'g'li

O'zbekiston Respublikasi IIV Akademiyasi 3-kurs kursanti

Toshkent. sh

https://doi.org/10.5281/zenodo.20694152

Annotatsiya: Mazkur ilmiy maqolada respublikamizda ommalashgan Telegram messenjeri orqali tarqalib, fuqarolarning shaxsiy ma'lumotlari va bank hisob raqamlarini o'g'irlashga qaratilgan APK formatidagi zararli dasturlarga (viruslarga) qarshi kurashishning kiber-profilaktik va ma'muriy-huquqiy mexanizmlari tahlil qilingan. Kiberjinoyatchilarning "ijtimoiy muhandislik" usullaridan foydalangan holda yoshlar va raqamli savodxonligi past qatlamni aldash taktikasi (soxta jarimalar, rasmlar, yordam pullari) ilmiy asoslangan. Jinoyatlarni fosh etish va ularning barvaqt oldini olishda ichki ishlar organlarining "High-tech policing" (yuqori texnologik politsiya) imkoniyatlari yoritilgan. Janubiy Koreya, Singapur va Yevropa Ittifoqi davlatlarining kiber-gigiyena hamda raqamli xavfsizlik borasidagi ilg'or xorij tajribasi qiyosiy o'rganilib, milliy qonunchilik va amaliyotni takomillashtirish yuzasidan aniq ilmiy-amaliy takliflar ishlab chiqilgan.

Kalit so'zlar: kiberxavfsizlik, APK virus, Telegram messenjeri, ijtimoiy muhandislik, bank troyanlari, High-tech policing, kiber-profilaktika, raqamli savodxonlik, xorij tajribasi.

Raqamlashtirish jarayonlari jadal rivojlanayotgan bugungi kunda jamiyatdagi jinoyatchilik o'zining an'anaviy ko'rinishidan kiber-makonga to'liq ko'chib o'tmoqda.

O‘zbekiston aholisi orasida eng ommabop aloqa vositasi hisoblangan Telegram messenjeri so‘nggi vaqtlarda kiber-firibgarlar uchun asosiy "ov maydoni"ga aylandi. Fuqarolarning ishonchiga kirish orqali ularga **.apk** (Android Package Kit) kengaytmasidagi zararli fayllarni yuborish va shu orqali ularning mobil qurilmasini masofadan boshqarish holatlari keskin ko‘paydi.

Bu turdagi jinoyatlar jamoat xavfsizligiga va iqtisodiy barqarorlikka jiddiy tahdid soladi. Jabrlanuvchilar nafaqat o‘zining barcha moliyaviy mablag‘laridan ayriladi, balki ularning nomidan boshqa tanishlariga ham virusli fayllar tarqatilib, jinoyatning **"Domino effekti"** (zanjir reaksiyasi) yuzaga keladi. Mazkur jarayonda ichki ishlar organlari (IIO) faqatgina jinoyat sodir bo‘lgandan so‘ng tergov harakatlarini olib borish bilan cheklanmasdan, zamonaviy "High-tech" profilaktika mexanizmlari orqali aholini bunday tahdidlardan himoya qilishi davr talabidir.

Kiberjinoyatchilar hech qachon "bu virus, shuni o‘rnating" deb fayl yubormaydi. Ular inson psixologiyasining zaif nuqtalariga ta'sir qiluvchi **Ijtimoiy muhandislik (Social Engineering)** usullaridan foydalanadilar:

- **Niqoblangan fayllar (Troya oti):** Foydalanuvchiga Telegram orqali rasm, video yoxud muhim hujjat ko‘rinishidagi fayl keladi (masalan, *rasm.apk*, *jarima_nasiyasi.apk*, *moddiy_yordam.apk*). Aslida, Android tizimida rasm (.jpg) yoki video (.mp4) formatida bo‘lishi kerak, ammo foydalanuvchilar fayl kengaytmasiga e'tibor bermasdan uni yuklab, "O‘rnatish" (Install) tugmasini bosadilar.
- **Ruxsatlarni (Permissions) tortib olish:** APK fayl o‘rnatilgach, u smartfon egasidan SMS-xabarlarni o‘qish, kontaktlarga kirish va ekranni yozib olish ruxsatini so‘raydi. E'tiborsiz fuqaro barcha ruxsatlarni bergan zahoti, virus yashirin rejimga o‘tadi (ekranda ikonka ko‘rinmaydi).

- **Mablag‘larni o‘g‘irlash va zanjirli tarqalish:** Virus fuqaroning bank ilovalariga (Click, Payme, Uzcard) kirish uchun kelgan SMS-tasdiq kodlarini yashirincha kiber-jinoyatchiga jo‘natadi. Shu bilan birga, fuqaroning Telegram profilini egallab olib, barcha kontaktlariga o‘sha virusni tarqata boshlaydi.

APK troyanlariga qarshi kurashishda tezkor-qidiruv va profilaktika xizmatlari quyidagi zamonaviy chora-tadbirlarni amalga oshiradi:

- **Raqamli profilaktika (Cyber Patrol):** Kiberxavfsizlik bo‘linmalari ijtimoiy tarmoqlardagi "Qarmoq" (Phishing) guruhlarini doimiy monitoring qiladi. Tarqalayotgan zararli APK fayllarning manbasini (IP manzili va botnet serverlarini) o‘rganib, ularni O‘zbekiston hududida bloklash bo‘yicha vakolatli organlarga (O‘zkomnazorat) tezkor taqdimnomalar kiritadi.
- **Ogohlantirish va kiber-gigiyena:** Mahallalarda, xususan, yoshlar va raqamli savodxonligi nisbatan past bo‘lgan katta yoshli qatlamlar o‘rtasida profilaktika inspektorlari tomonidan tushuntirish ishlari olib borilishi. Bunda quruq so‘zlar bilan emas, balki real voqealar asosida tayyorlangan infografikalar, qisqa videoroliklar orqali "Begona APK faylni ochish = Hamyonni o‘g‘riga berish" ekanligini vizual singdirish.
- **Ma'muriy-huquqiy nazorat:** Telekommunikatsiya tarmoqlaridan foydalanish qoidalariga rioya etilishini ta'minlash, firibgarlikda foydalanilayotgan SIM-kartalarning noqonuniy savdosiga (qora bozoriga) chek qo‘yish bo‘yicha muntazam tezkor-profilaktik tadbirlar o‘tkazish.
- Telegram orqali tarqalayotgan APK viruslar asosan foydalanuvchilarning ishonuvchanligi va texnik savodsizligi sababli o‘z maqsadiga yetmoqda. Jinoyatning oldini olish va jamoat xavfsizligini ta'minlash maqsadida quyidagi ilmiy-amaliy takliflar ilgari suriladi:
- **Birinchidan,** O‘zbekiston Respublikasi IIV Kiberxavfsizlik markazi va Raqamli texnologiyalar vazirligi hamkorligida fuqarolarning smartfonlari uchun

mo‘ljallangan milliy **"Antifishing-UZ" identifikatorini** ishlab chiqish. Bu tizim Telegram orqali kelayotgan shubhali APK fayllarni yuklab olishdan avval avtomatik tekshirib, xavf mavjud bo‘lsa, ekranga bloklovchi ogohlantirish chiqarishi lozim.

- **Ikkinchidan,** Ma'muriy javobgarlik to‘g‘risidagi kodeksga o‘zganing shaxsiy ma'lumotlariga noqonuniy kirish va ziyon yetkazishga mo‘ljallangan dasturlarni **bila turib ijtimoiy tarmoqlarda tarqatganlik (hamma ko‘radigan guruhlarga yuborganlik) uchun** tegishli ma'muriy jazo choralarini kiritish. Bu zanjirli tarqalishning oldini olib, fuqarolarni har qanday havola va fayllarni guruhlarga uzatishda (forward) mas'uliyatli bo‘lishga o‘rgatadi.
- **Uchinchidan,** Maktab va oliy ta'lim muassasalarida "Kiber-gigiyena va axborot xavfsizligi" qisqa o‘quv kurslarini majburiy fanga aylantirish. Profilaktika inspektorlarining o‘zini ham kiberxavfsizlikning elementar qoidalari va OSINT asoslariga o‘qitish orqali, ularning mahalladagi fuqarolar bilan axborot-texnologik tilida to‘g‘ri tushuntirish ishlarini olib borishini ta'minlash.
- Xulosa o‘rnida ta'kidlash kerakki, jinoyatchilar smartfonni buzib kirmaydi — ular insonning ongini buzadi va o‘z qo‘llari bilan eshikni ochdiradi. Raqamli tahdidlarga qarshi faqatgina huquq-tartibot organlarining harakatlari bilan emas, balki jamiyatning yalpi kiber-savodxonligini oshirish orqaligina ishonchli himoya devorini qurish mumkin.

REFERENCES

1. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni. 15.04.2022 yildagi O‘RQ-764-son.
2. O‘zbekiston Respublikasining Jinoyat kodeksi. [Elektron resurs] // Qonunchilik ma’lumotlari milliy bazasi, https://lex.uz.

3. Xudoyberdiyev A.A. "Ma’muriy ishlarni yuritish kafolatlari va huquqni qo‘llash amaliyoti". O‘quv qo‘llanma. – Toshkent: IIV Akademiyasi, 2024.
4. G‘ofurov I. va boshq. "Axborot xavfsizligi va kiberjinoyatlarga qarshi kurashish asoslari". – Toshkent: IIV Malaka oshirish instituti, 2022.