ISSN 2181-3187

MOBIL QURILMALAR VA ILOVALARNI ZARARLI DASTURLARDAN HIMOYA QILISH

Jo‘rayev To‘lqinjon Omonovich
Toshkent davlat yuridik universiteti magistranti

Annotatsiya. Ushbu maqolada mobil qurilmalar va ilovalarni zararli dasturlardan himoya qilish mavzusi yoritilgan. Shu bilan birga, zararli dastur turlari, ularni mobil qurilmalarga yuqtirishning oldini olish, himoyalanish va zararlangan qurilma bilan qanday munosabat qilish kerakligi haqida aniq tavsiyalar berilgan.

Kalit so‘zlar. Zararli dastur, virus, troyan, adware, texnologiya, kiberhujum.

PROTEKT MOBILE DEVICES AND APPLICATIONS FROM MALWARE

Abstract. This article covers the topic of protecting mobile devices and applications from malware. At the same time, there are clear recommendations on the types of malware, how to prevent them from infecting mobile devices, how to protect yourself and how to deal with an infected device.

Key words. Malware, virus, trojan, adware, technology, cyber attack.

Hozirgi kunda raqamli texnalogiyalarning shiddat bilan rivojlanishi va raqamlashtirish hayot tarzimizni o‘zgartirish bilan birga kiberjinoyatchilik faoliyatini ham keltirib chiqardi. Dunyo miqyosida ma’lumotlar markazlari, mudofaa, energetika, hukumat va moliya sektorlariga kiberhujumlarning ortib borayotgan tahdidi barchaga birdek o‘ziga xos muammo tug‘dirmoqda. Ushbu kiberhujumlar moliyaviy o‘g‘irlik, josuslik, sabotaj, intellektual mulkni o‘g‘irlash va siyosiy maqsadlar uchun zararli dasturlardan foydalanmoqda. Kiberjinoyatchilar murakkablashib borayotgan va ilg‘or zararli dastur hujumlarini amalga oshirayotgan bir paytda, bunday hujumlarni aniqlash va ularga javob berish kiberxavfsizlik bo‘yicha mutaxassislar uchun juda muhim vazifaga aylanmoqda. Masala qanchalik dolzab ekanligini, O‘zbekiston Respublikasi Prezidentining «Yangi O‘zbekistonning 2022–2026-yillarga mo‘ljallangan taraqqiyot strategiyasi to‘g‘risida»[1]gi Farmonida kiberjinoyatchilikning oldini olish tizimini yaratish bandi mavjudligi bilan ham izohlasak bo‘ladi. Zararli dasturlar orqali sodir etilayotgan kiberjinoyatlar o‘ta murakkabligi, fosh etish qiyinligi, izlarni topish mushkulligi bilan boshqa turdagi jinoyatlardan keskin farq qiladi. Mobil qurilmalar va ilovalarni zararli dasturlardan himoya qilishni o‘rganishdan oldin zararli dastur nima,

[1] O‘zbekiston Respublikasi Prezidentining Farmoni, 28.01.2022 yildagi PF-60-son

ISSN 2181-3187

uning turlari qanday ekanligini va u mobil ekotizimga qanday ta’sir qilishi mumkinligini bilish lozim.

Mobil zararli dasturlarning eng mashhur turlari.

Viruslar (Viruses). Zararli dasturlarning eng mashhur turi – virusdir. Garchi zararli dasturlarning ko‘p turlari viruslar deb atalsa ham, ular bir narsa emas. Virus – bu o‘z nusxalarini ilovalar, ma’lumotlar va kompyuter ma’lumotlarni saqlash tizimlarining muhim qismlariga (masalan, qattiq disklar, xotira kartalari va boshqalar) yuqtirish uchun yozilgan dasturiy ta’minotdir. Viruslar kompyuterdagi muayyan ilovalarga biriktiriladi va dastur ishga tushirilganda faollashadi. Ushbu jarayonda virus qattiq diskda o‘z nusxasini yaratishi yoki yuklanishda davom etishi yoki dastur har safar foydalanilganda ishga tushishi mumkin. Hozirgi vaqtda, viruslar flesh xotiralar orqali yoki global internet tarmog‘i orqali tarqalmoqda. Ba’zi viruslar zarar yetkazish uchun mo‘ljallanmagan bo‘lsa-da, biroq, ularni faollashuvi foydalanuvchilarga tegishli ma’lumotlarini o‘zgartirish, operatsion tizimga hujum qilish yoki jinoyatchilarga kompyuter tizimiga kirish uchun “yashirin yo‘l” qoldirishi bilan ham havfli hisoblanadi. Foydalanuvchiga zarar yetkazmagan holda ham viruslar raqamli qurilma xotirasi, quvvati yoki disk muhitiga ta’sir etadi[12].

Troyanlar (Trojans). Zararli dasturlarning asosiy turlaridan yana biri bu troyandir (yoki troyan oti) – yunon askarlarini qadimiy Troya shahriga olib kirgan yog‘och ot nomi bilan atalgan. Troyan o‘zini butunlay qonuniy dastur sifatida namoyon etib, shu yo‘l bilan o‘zini yashirib, sahna ortidan turib zarar yetkazadi – bu jarayon boshqa birovning kompyuterini boshqarish, shaxsiy ma’lumotlarini nusxalash, ma’lumotlarni o‘chirish, tugmachalarni bosishni kuzatish yoki elektron pochta dasturidan foydalanib, o‘zini boshqa kompyuterlarga yetkazishda namoyon bo‘ladi. Viruslar va qurtlardan farqli o‘laroq, troyanlar o‘z-o‘zidan takrorlanmaydi - ular kompyuterlar o‘rtasida tarqalish uchun o‘zlarining ko‘rinadigan foydaliligiga tayanadilar. Ba’zi troyanlar alohida ishlaydi. Biroq, ba’zilari parollar, bank hisoblari ma’lumotlari yoki kredit karta raqamlari kabi o‘g‘irlangan ma’lumotlarni uzatish yoki buzilgan kompyuterlarga orqa eshik sifatida tarmoqlarga tayanadi. Ular tajovuzkorlarga operatsion tizimning xavfsizlik xususiyatlarini chetlab o‘tishga va ma’lumotlarga kirishga yoki hatto tarmoq orqali mashinani boshqarishga imkon beradi.[32]

Tovlamachi dastur (Ransomware). Ransomware bu kriptovirusologiyaning zararli dasturi bo‘lib, agar to‘lov to‘lanmasa, jabrlanuvchining shaxsiy ma’lumotlarini nashr qilish yoki unga kirishni butunlay blokirovka qilish bilan tahdid qiladi. Ba’zi oddiy to‘lov dasturlari hech qanday faylga zarar bermasdan tizimni bloklashi mumkin bo‘lsada, ilg‘or zararli dasturlar kriptovirus to‘lov dasturi deb ataladigan usuldan

[2] https://www.open.edu/openlearn/mod/oucontent/view.php?id=48320&printable=1
[3] https://www.open.edu/openlearn/mod/oucontent/view.php?id=48320&printable=1

ISSN 2181-3187

foydalanadi. U jabrlanuvchining fayllarini shifrlaydi, ularga kirish imkoni bo‘lmaydi va ularning shifrini ochish uchun to‘lov talab qiladi.[4][5][6][7]

E-pochta ilovasini ochish, reklamani bosish, havolaga o‘tish yoki hatto zararli dastur o‘rnatilgan veb-saytga tashrif buyurib, tasodifan to‘lov dasturini kompyuteringizga yuklab olishingiz mumkin. Kod kompyuterga yuklab olingandan so‘ng, u kompyuterning o‘ziga yoki u erda saqlangan ma’lumotlar va fayllarga kirishni bloklaydi. Yana xavfli versiyalar mahalliy drayvlar, xaritalangan drayvlar va hatto tarmoqqa ulangan kompyuterlardagi fayl va papkalarni shifrlashi mumkin. Ko‘pgina hollarda, siz kompyuteringiz infeksiyalanganligini bilmaysiz. Buni odatda ma’lumotlaringizga kirish imkoni bo‘lmaganda yoki hujum haqida xabar beruvchi va to‘lovni talab qiluvchi kompyuter xabarlarini ko‘rganingizda bilasiz[8].

Adware. Reklama dasturi – bu kompyuteringizda keraksiz reklamalarni ko‘rsatadigan dasturdir. Reklama dasturlari odatda qalqib chiquvchi reklamalarni ko‘rsatadi, brauzeringizning bosh sahifasini o‘zgartirishi, josuslik dasturlarini qo‘shishi va shunchaki reklamalar bilan qurilmangizni bombalashi mumkin. Adware - bu potensial keraksiz dasturlarning qisqaroq nomi. Bu aniq virus emas va u Internetda aylanib yuradigan boshqa ko‘plab muammoli kodlar kabi zararli bo‘lmasligi mumkin. Biroq, ushbu reklama dasturi o‘rnatilgan har qanday mashinadan o‘chirilishi kerak. Reklama dasturi nafaqat kompyuteringizdan har safar foydalanganda juda zerikarli bo‘lishi mumkin, balki qurilmangiz uchun uzoq muddatli muammolarni keltirib chiqarishi mumkin. Reklama dasturi sizning qiziqishlaringizga moslashtirilgandek ko‘rinadigan reklamalarni “maqsadli” qilish uchun veb-sahifalar tarixini to‘plash uchun brauzerdan foydalanadi. Eng zararsiz holatlarda, adware infeksiyasi shunchaki bezovta qiladi. Masalan, reklama dasturlari sizni ko‘rib chiqish tajribangizni sezilarli darajada sekinlashtiradigan va ko‘proq mehnat talab qiladigan qalqib chiquvchi reklamalar bilan bombardimon qiladi. Reklama dasturidan foydalanishning eng keng tarqalgan maqsadi reklamadan pul ishlash uchun siz haqingizda ma’lumot to‘plashdir. Agar kompyuterda o‘rnatilgan bo‘lsa, u reklama dasturi, smartfon yoki planshet kabi mobil qurilmaga o‘rnatilgan bo‘lsa zararli dastur deb ataladi. Reklama dasturi yoki zararli dastur nima bo‘lishidan qat’i nazar, u sizning mashinangizni sekinlashtiradi yoki hatto ishdan chiqishga moyil qiladi[9].

[4] Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.
[5] Schofield, Jack (28 July 2016). "How can I remove a ransomware infection?". The Guardian. Retrieved 28 July 2016.
[6] Mimoso, Michael (28 March 2016). "Petya Ransomware Master File Table Encryption". threatpost.com. Retrieved 28 July 2016.
[7] Justin Luna (21 September 2016). "Mamba ransomware encrypts your hard drive, manipulates the boot process". Neowin. Retrieved 5 November 2016.
[8] www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
[9] us.qnorton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html

ISSN 2181-3187

Mobil qurilmalar va ilovalarni zararli dasturlardan himoya qilish haqida ko‘plar olimlar o‘z fikr mulohazalarni bildirib o‘tgan, xususan Wendy Zamora o‘zining Malvarebytes saytida yozgan postida[10] mobil qurilmalarni himoya qilishning 10 ta yo‘l: ini aytib o‘tgan bo‘lsa, MV Braverman va Karl Frankham o‘zlarining Linkedinda e’lon qilgan maqolasida[11] mobil qurilma elektron pochtasi yoki xabarlaridagi zararli havolalar yoki biriktirmalarni bosishdan qanday saqlanish mumkinligi haqida o‘z fikrlarini bildirib o‘tgan.

Shu bilan birga dunyoga mashhur Kasperskiy kompaniyasi o‘z saytida e’lon qilgan maqolada mobil qurilmalardan foydalanish ortib borishi bilan, ularga bo‘lgan tahdidlar oshishi mumkinligini aytib, har qanday mobil qurilmani zararlash mukinmi degan savolga, Kembrij universiteti tadqiqotchilari barcha Android smartfonlarining 87 foizi kamida bitta muhim zaiflikka duchor bo‘lishini, Zimperium Labs shu yil boshida Android qurilmalarining 95 foizi oddiy matnli xabar orqali buzib kirishi mumkinligini aniqlaganliklarini, xatto Apple ham immunitetga ega emasligini, buning asosi o‘laroq, sentyabr oyida 40 ta ilova rasmiy ilovalar do‘konidan olib tashanganini, chunki ular XcodeGhost, ya’ni Apple qurilmalarini keng ko‘lamli botnetga aylantirish uchun mo‘ljallangan zararli dastur bilan zararlanganligini. Apple kompaniyasining ajoyib himoyasiga qaramay, zararli dastur nafaqat yashirincha o‘tib ketganligini, balki qonuniy ilovalar tepasida joylashgan bo‘lib, uni aniqlashni qiyinlashtirganini aytib o‘tmoqda.Shu bilan birga mobil qurilmalarni himoya qilish bo‘yicha quyidagi tavsiyalarni bermoqda: Xavfsiz Wi – Fi dan foydalanish, elekton pochtani ko‘rish, ilovalarni faqat ishonchli manbalarda yuklab olish, mobil qurilmalarda mavjud antivirus himoyalaridan foydalanish va hokazo[12]**.** Anya Beuzeva MyMemory saytida e’lon qilgan postida mobil zararli dastur hujumlarining oldini olish uchun 5 muhim qadamni sanab o‘tgan, uning so‘zlariga ko‘ra “smartfonlar va boshqa mobil qurilmalar internetga kirishning afzal usuliga aylanib borayotgani sababli, xakerlar ham mobil qurilmalar orqali ko‘proq hujumlar uyushtirayotganini aytish uchun raketa yaratuvchi olim yoki Kremniy vodiysi mutaxassisi bo‘lish shart emas”.

AQSH kiberxavfsizlik va infratuzilma xavfsizligi agentligi (CISA) qanday qilib zararli ilovalardan qochish va ilovalar siz haqingizda to‘playdigan ma'lumotlarni cheklash mumkinligiga to‘xtalib, ilovani o‘rnatishdan oldin, zararli bo‘lishi mumkin bo‘lgan ilovalardan chekinish va ilovalardan xabardor bo‘lish lozimligi, o‘rnatilgan ilovalarda ilova ruxsatlarini ko‘rib chiqish, joylashuv ruxsatlarini cheklash va ilova dasturlarini yangilab turishni maslahat bermoqda. Shu bilan birga keraksiz ilovalarni

[10] https://www.malwarebytes.com/blog/news/2016/09/top-10-ways-to-secure-your-mobile-phone
[11] https://www.linkedin.com/advice/0/how-do-you-avoid-clicking-malicious-links-attachments
[12] https://usa.kaspersky.com/resource-center/threats/mobile-malware

ISSN 2181-3187

o‘chirib, ijtimoiy tarmoq hisoblari bilan ilovalarga kirishda ehtiyot bo‘ling lozimligini uqtirmoqda[13].

Singapur kiberxavfsizlik agentligi (CSA) mobil qurilmalarni zararli dasturlardan himoya qilish bo‘yicha maslahatlari bilan bo‘lishib, shuni ta’kidlamoqdaki, mobil zararli dasturlarni qurilmalarga ishonchsiz veb-saytlarga kirishga olib keladigan havolalarni bosish, ijtimoiy media xabarlari, matnli yoki elektron xatlardagi zararli qo‘shimchalarni, zararli mobil ilovalarni yuklab olish kabi usullar orqali yuklab olish, foydalanuvchilar mobil qurilmalarini zararli dastur infektsiyasidan quyidagi choralarni ko‘rish orqali himoya qilishlari mumkinligini bayon qilmoqda. Ilovalarni faqat rasmiy Play Store (Android) va App Store (iOS) dan yuklab oling; yuklab olishdan oldin ilova va/yoki uning maxfiylik siyosati talab qiladigan xavfsizlik ruxsatnomalariga e'tibor bering; qurilmangizda keraksiz ruxsatlarni so‘raydigan ilovalardan ehtiyot bo‘ling; qurilmaning dasturiy ta'minoti va ilovalarini iloji boricha tezroq so‘nggi versiyalarga yangilang; antivirus/zararli dasturlarga qarshi dasturiy ta'minotni eng so‘nggi zararli dastur imzo fayli bilan yangilab turing va muntazam ravishda virusga qarshi/zararli dasturlarga qarshi skanerdan o‘tkazing; shubhali ijtimoiy media xabarlari, matnli xabarlar va elektron pochta xabarlaridan ehtiyot bo‘ling; har qanday havolani bosishdan yoki qo‘shimchalarni yuklab olishdan oldin har doim xabarning haqiqiyligini tekshiring; foydalanilmayotganda ilovalarni yoping; qurilmani muntazam ravishda yoqing va o‘chiring; android qurilmalaringizda PlayProtect yoqilganligiga ishonch hosil qiling va Google PlayProtect ogohlantirishi so‘ralganda ilovalarni o‘rnatishdan saqlaning.[14]

Yuqoridagi tahlilimizga tayanib aytishimiz mumkinki, ayni vaqtda mobil qurilmalarga bo‘lgan ehtiyoj tobora ortib bormoqda va bu ortishda davom etadi. Shundan kelib chiqib ishonch bilan aytishimiz mumkinki, mobil qurilmalarga zararli dasturlar tahdidi ham ortib boradi. Shuni alohida ta’kidlashimiz lozimki, zararli dasturlar takomillashib, hujum usullari o‘zgarib borgan sayin, ulardan himoyalanishning ham yangi yo‘llari paydo bo‘ladi. Biz ayni maqolamizda aynan yaqin yillarda dunyo miqyosida qo‘llanilayotgan eng ilg‘or himoya usullarini tahlil qilishni maqsad qildik.

Zararli dasturlar mobil qurilmaga qanday yuqadi.

Mobil qurilmaga zararli dasturlar quyidagi yo‘llar bilan kirib kelishi mumkin:

- Shubhali yoki norasmiy manbalardan zararlangan ilovalarni yuklab olish orqali;
- Zararli havolalar yoki elektron pochta qo‘shimchalarini bosish orqali;
- Kerakli xavfsizlik choralari mavjud bo‘lmagan umumiy Wi-Fi tarmoqlaridan foydalanish orqali;
- Qurilmaning operatsion tizimi yoki o‘rnatilgan ilovalardagi zaifliklardan

[13] https://www.cisa.gov/news-events/news/privacy-and-mobile-device-apps
[14] https://www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008

ISSN 2181-3187

foydalanish orqali.

Zararli dasturlarni yuqtirishning oldini olish.

Ilovalarni sertifikatlangan, ishonchli manbalardan yuklab oling. Android uchun Google Play Store va iOS uchun Apple App Store kabi rasmiy ilovalar do‘konlariga ishoning. Ushbu platformalar ilovalarni sinchkovlik bilan tekshiradi va ko‘rib chiqadi, bu esa zararli dastur bilan zararlangan dasturlarga duch kelish ehtimolini kamaytiradi.

Vaziyatga chuqurroq yondashing, ya’ni sharhlarni o‘qing va ruxsat berishdan oldin sinchkovlik bilan tekshiring. Ilovani o‘rnatishdan oldin foydalanuvchi sharhlarini o‘rganing va ilova so‘ragan ruxsatlarni sinchkovlik bilan tekshiring. Agar ilova haddan tashqari yoki asossiz ruxsatlarni so‘rasa, ehtiyot bo‘ling va batafsilroq tekshirib ko‘ring.

Yangilanishlar. Qurilmangizning operatsion tizimi va ilovalarini yangilab turish juda muhim. Ushbu yangilanishlar ko‘pincha zararli dasturlardan foydalanishi mumkin bo‘lgan zaifliklarni oldini olish uchun muhim xavfsizlik yamoqlarini o‘z ichiga oladi.

Imkoni boricha, nufuzli mobil xavfsizlik ilovasini o‘rnating. Zararli dasturlarni muntazam tekshiradigan, real vaqtda himoyani taklif qiluvchi va qo‘shimcha xavfsizlik funksiyalarini, jumladan, fishingga qarshi vositalarni ta’minlovchi nufuzli mobil xavfsizlik ilovalarini o‘rnatish orqali himoyangizni mustahkamlang.

Umumiy Wi-Fi tarmog‘ida ma'lumotlaringizni himoya qilish. Muhim tranzaksiyalarni amalga oshirayotganda ma’lumotlaringizni shifrlash uchun virtual xususiy tarmoqni (VPN) o‘rnating, ayniqsa kiberjinoyatchilar uchun oson nishon sifatida tanilgan umumiy Wi-Fi tarmoqlariga ulanganda.

Hushyorlik va tezkor aniqlash: zararli dastur infektsiyalarini aniqlash. Qattiq profilaktika choralari ko‘rilgan bo‘lsa ham, zararli dastur vaqti-vaqti bilan mobil qurilmangiz himoyasini buzishi mumkin . Shu sababli, erta aniqlash potentsial zararni minimallashtirishning muhim jihati bo‘lib qolmoqda.

Antivirus va zararli dasturlarga qarshi vositalar bilan quvvatlang. Qurilmangizni tahdidlarni vaqti-vaqti bilan tekshiradigan va zararli dasturlarni samarali aniqlash va olib tashlash imkonini beradigan nufuzli antivirus va zararli dasturlardan foydalanish orqali mobil qurilmangiz xavfsizligini mustahkamlang.

Ishlash monitoringi. Zararli dastur infektsiyasining aniq belgilari uchun qurilmangizning ishlashini muntazam ravishda kuzatib boring. Batareyaning noodatiy zaryadsizlanishi, sust ishlashi yoki ma’lumotlardan foydalanishning kutilmagan o‘sishi zararli dastur qurilmangizga kirishga muvaffaq bo‘lganligini ko‘rsatishi mumkin.

Ilova anomaliyalarini kuzatib boring. Xatti-harakatlar uchun o‘rnatilgan ilovalaringizni faol ravishda kuzatib boring. Ilovaning tez-tez ishdan chiqishi, kutilmagan reklama namoyishlari yoki qo‘shimcha ruxsatlarga shubhali so‘rovlar darhol tekshiruvni boshlashi kerak.

ISSN 2181-3187

Qurilma jurnallarini ko‘rib chiqish. Mobil qurilmangiz jurnallari, qaysi hujjat tizimi va ilovalar faoliyati bilan tanishing. Ushbu jurnallarni sinchkovlik bilan tekshirish har qanday noto‘g‘ri faoliyat yoki ilova xatti-harakatlarini aniqlashga yordam beradi.

Zararli dasturlarni zararsizlantirish va yo‘q qilish. Agar mobil qurilmangiz zararli dasturlarning qurboni bo‘lgan deb gumon qilsangiz, tezkor va qat'iy harakat qilish muhim ahamiyatga ega. Zararli dasturlarni qurilmangizdan qanday qilib zararsizlntirish va olib tashlashni batafsilroq ko‘rib chiqing:

Izolyatsiya va o‘chirish.Zararli dasturlardan shubhalansangiz, keyingi zararni oldini olish uchun qurilmangizni darhol internetdan uzing. Qurilmangizni samarali karantin qilish uchun Wi-Fi va mobil ma’lumotlarni o‘chirib qo‘ying.

Shubhali ilovalarni o‘chirish.O‘rnatilgan ilovalar ro‘yxatini ko‘rib chiqing va shubhali yoki notanish ko‘rinadigan ilovalarni o‘chirib tashlang. Bu boshlang‘ich qadamdir.

Keng qamrovli skanerdan o‘tkazish. To‘liq miqyosli tizim tekshiruvini amalga oshirish uchun antivirus yoki zararli dasturlarga qarshi dasturdan foydalaning. Zararlangan fayllarni o‘chirish kabi tavsiya etilgan amallarni bajarganingizga ishonch hosil qiling.

Parollarni o‘zgartirish. Zararli dasturiy ta'minotni olib tashlaganingizdan so‘ng, parolni keng qamrovli ta'mirlashni boshlang, ayniqsa hisob qaydnomasi ma'lumotlari buzilgan deb gumon qilsangiz.

Zaxiradan tiklash. Zararli dasturiy ta'minot infektsiyasi ayniqsa doimiy yoki olib tashlash qiyin bo‘lgan hollarda, qurilmangizni zavod sozlamalariga qaytarish, so‘ngra toza zaxiradan qayta o‘rnatish haqida o‘ylab ko‘ring.

Mutaxassislar bilan maslahatlashishdan tortinmang. Zararli dasturlarni qanday samarali olib tashlash haqida shubhangiz bo‘lsa yoki o‘ta murakkab infektsiyaga duch kelganingizda, mutaxassis bilan maslahatlashing yoki mutaxassis ko‘rsatmalari va yordami uchun qurilmangiz ishlab chiqaruvchisi bilan bog‘lanish tavsiya etiladi.

Xulosa qilib aytadigan bo‘lsak, mobil qurilmalar, shubhasiz, hayotimizning ajralmas qismiga aylangan, ammo ularning zararli dasturlarga moyilligi doimo dolzarb bo‘lib qolmoqda. Mobil qurilmangiz va ilovalaringizni zararli dasturlardan himoya qilish nafaqat asosiy xavfsizlik choralarini amalga oshirishdir. Bu keng qamrovli yondashuvni, jumladan, oldini olish bo‘yicha faol pozitsiyani, hushyor monitoringni va infektsiya sodir bo‘lganda aniq belgilangan javob strategiyasini o‘z ichiga oladi. Ushbu keng qamrovli qo‘llanmada taqdim etilgan kengaytirilgan strategiyalarga rioya qilish orqali siz mobil zararli dasturlar bilan bog‘liq xavflarni sezilarli darajada kamaytirishingiz va xavfsizroq mobil tajribani ta'minlashingiz mumkin. Xabardor bo‘ling, doimo hushyor bo‘ling va tobora ortib borayotganimizda doimo himoyalangan bo‘ling. Maqolamiz asosida O‘zbekiston qonunchiligiga quyidagi takliflarni beramiz:

ISSN 2181-3187

1. Qonun hujjatlarida zararli dastur atamasiga aniq ta’rif berish.
2. Zararli dasturlarni ogoh bo‘lish uchun aholining kibersavodxonligini oshirish dasturini ishlab chiqish.
3. Zararli dastur tahdidlarini tahlil qilib boruvchi alohida markaz tuzish.

Foydalanilgan manbalar

1. https://www.open.edu/openlearn/mod/oucontent/view.php?id=48320&printable=1
2. https://www.open.edu/openlearn/mod/oucontent/view.php?id=48320&printable=1
3. Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.
4. Schofield, Jack (28 July 2016). "How can I remove a ransomware infection?". The Guardian. Retrieved 28 July 2016.
5. Mimoso, Michael (28 March 2016). "Petya Ransomware Master File Table Encryption". threatpost.com. Retrieved 28 July 2016.
6. Justin Luna (21 September 2016). "Mamba ransomware encrypts your hard drive, manipulates the boot process". Neowin. Retrieved 5 November 2016.
7. www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
8. us.qnorton.com/internetsecurity-emerging-threats-what-is-grayware-adware- and-madware.html
9. https://www.malwarebytes.com/blog/news/2016/09/top-10-ways-to-secure- your-mobile-phone
10. https://www.linkedin.com/advice/0/how-do-you-avoid-clicking-malicious-links-attachments
11. https://usa.kaspersky.com/resource-center/threats/mobile-malware
12. https://www.cisa.gov/news-events/news/privacy-and-mobile-device-apps
13. https://www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008