ZARARLI VIRUSLAR KOMPYUTER XAVFSIZLIGI VA HIMOYA CHORALARI

Mirzajonov Murodjon Muzaffar o‘g‘li

Namangan viloyati Ichki Ishlar Boshqarmasi Axborot-texnologiyalari sohasidagi jinoyatlarga qarshi kurashish boshqarmasi tergov guruhi, katta tergovchisi, katta leytenant

KIRISH

Zamonaviy raqamli dunyoda kompyuter viruslari va zararli dasturlar eng katta xavflardan biri hisoblanadi. Ular shaxsiy ma'lumotlarni o'g'irlash, tizimlarni buzish va moliyaviy zararlarga sabab bo'lishi mumkin. Zararli viruslar — bu kompyuter tizimlariga zarar yetkazish, ma'lumotlarni o'g'irlash yoki tizim ishlashini buzish maqsadida yaratilgan dasturiy ta'minotlardir.

Ushbu hujjatda zararli viruslarning turlari, ular qanday tarqalishi, oqibatlari va himoya choralari to'liq ko'rib chiqiladi.

1. Zararli viruslarning asosiy turlari

1.1. Virus (Virus)

Viruslar o'z-o'zidan takrorlanuvchi dasturlar bo'lib, ular boshqa dasturlarga yoki fayllarga birikib, ularni zararlaydi. Viruslar dasturlar ishga tushirilganda faollashadi va tizim bo'ylab tarqaladi. Eng xavfli tomonlaridan biri shundaki, ular foydalanuvchi bilmasdan fayl yoki dastur orqali boshqa kompyuterlarga o'tishi mumkin.

Viruslarning turli shakllari mavjud: fayl viruslari, boot-sektor viruslari, makros viruslari va boshqalar. Ularning barchasi tizimga turlicha zarar yetkazishi mumkin.

1.2. Troyalar (Trojans)

Troyan dasturlari foydali dastur sifatida ko'rinadi, lekin aslida zararli funktsiyalarni bajaradi. Ular odatda foydalanuvchi tomonidan ixtiyoriy ravishda yuklab olinadi va o'rnatiladi. Troyanlar parollarni o'g'irlash, tizimga kirish huquqlarini berish yoki boshqa zararli dasturlarni yuklash uchun ishlatiladi.

Masalan, foydalanuvchi o'yin yoki foydali dastur deb o'ylab yuklab olgan fayl aslida troyan bo'lishi va keyingi fonda maxfiy ma'lumotlarni yuborib turishi mumkin.

1.3. Qurtlar (Worms)

Kompyuter qurtlari o'z-o'zidan tarqaluvchi dasturlar bo'lib, ular tarmoq orqali boshqa kompyuterlarga o'tadi. Viruslardan farqli o'laroq, qurtlar alohida dasturga birikmasdan mustaqil tarqaladi. Ular tizim resurslarini ko'p ishlatib, tarmoqni sekinlashtirishi yoki to'liq to'xtatib qo'yishi mumkin.

Eng mashhur qurt hujumlari orasida 2000-yilda paydo bo'lgan ILOVEYOU qurti va 2017-yildagi WannaCry ransomware qurti bor.

1.4. Ransomware (To'lov talabi)

Ransomware — bu foydalanuvchi fayllarini shifrlash orqali ularga kirishni blokirovka qiluvchi va shifrlash kalitini olish uchun to'lov talabini yuboradigan zararli dastur turi. Bu eng xavfli va moliyaviy jihatdan zararli viruslardan biridir.

Ransomware hujumlari kompaniyalar va tashkilotlar uchun katta zarar keltiradi, chunki ular muhim ma'lumotlarini yo'qotishi yoki katta miqdorda to'lov to'lashi mumkin.

1.5. Spyware (Josuslik dasturlari)

Spyware foydalanuvchi faoliyatini kuzatib, shaxsiy ma'lumotlarni (parollar, bank kartalari ma'lumotlari, shaxsiy xabarlar) o'g'irlaydigan dasturlardir. Ular foydalanuvchi bilmasdan o'rnatiladi va fonda ishlaydi.

Spyware ko'pincha bepul dasturlar bilan birga yoki spam habarlar orqali tarqaladi. Ular foydalanuvchining barcha klaviatura bosishlarini qayd etishi (keylogger) mumkin.

1.6. Adware (Reklama dasturlari)

Adware — bu foydalanuvchiga keraksiz reklamalarni ko'rsatadigan dasturlardir. Garchi ba'zi adware dasturlari qonuniy bo'lsa-da, ko'plari foydalanuvchi roziligisiz o'rnatiladi va tizimni sekinlashtiradi, shuningdek, shaxsiy ma'lumotlarni to'playdi.

2. Zararli viruslar qanday tarqaladi

2.1. Elektron pochta orqali

Eng keng tarqalgan yuqish usullaridan biri — bu spam elektron pochta xabarlari va zararli ilovalar. Hujumchilar foydalanuvchilarni aldab, noma'lum havolalarni bosishga yoki zararli fayllarni yuklashga undaydi. Phishing xabarlari ko'pincha ishonchli manba (bank, davlat muassasasi) nomi ostida yuboriladi.

Masalan, foydalanuvchi bank nomidan kelgan xabar deb o'ylab havolani bosishi mumkin va natijada uning ma'lumotlari o'g'irlanadi yoki kompyuteriga virus yuklanadi.

2.2. Zararli veb-saytlar

Ba'zi veb-saytlar maxsus foydalanuvchilarni aldash va ularga virus yuklash uchun yaratilgan. Bu saytlarga kirganingizda, avtomatik ravishda zararli dastur yuklanishi mumkin (drive-by download). Bunday hujumlar odatda xavfsizlik zaifliklaridan foydalanadi.

Shuningdek, noma'lum saytlardan dastur yoki fayl yuklash xavfli bo'lishi mumkin, chunki ular troyan yoki boshqa zararli dasturlar bo'lishi mumkin.

2.3. USB va tashqi qurilmalar

Zararli dasturlar USB flesh-disklar, tashqi qattiq disklar va boshqa tashqi qurilmalar orqali ham tarqalishi mumkin. Agar yuqtirilgan qurilma kompyuterga ulanganida, virus tizimga o'tishi va tarqala boshlashi mumkin.

Autorun funktsiyasi orqali viruslar avtomatik ishga tushishi mumkin, shuning uchun noma'lum USB qurilmalarni ehtiyotkorlik bilan ishlatish kerak.

2.4. Tarmoq zaifliklaridan foydalanish

Kompyuter qurtlari ko'pincha tarmoq xavfsizligidagi zaifliklardan foydalanib tarqaladi. Agar tizimda yangilanmagan dasturlar yoki xavfsizlik teshiklari bo'lsa, hujumchilar bulardan foydalanib tizimga kirishlari mumkin.

Shuning uchun operatsion tizim va dasturlarni muntazam yangilab turish juda muhimdir.

3. Zararli viruslarning oqibatlari

3.1. Ma'lumotlar yo'qolishi

Viruslar fayllarni o'chirishi, buzishi yoki shifrlashi mumkin. Bu shaxsiy suratlar, hujjatlar, video va boshqa muhim ma'lumotlarning butunlay yo'qolishiga olib kelishi mumkin. Ransomware esa fayllarni shifrlaydi va ularni qaytarish uchun to'lov talab qiladi.

Ma'lumotlar zaxira nusxasini saqlamasangiz, viruslar tufayli yillar davomida yig'ilgan muhim fayllarni yo'qotishingiz mumkin.

3.2. Shaxsiy ma'lumotlarning o'g'irlanishi

Spyware va troyanlar parollar, bank kartalari raqamlari, shaxsiy identifikatsiya ma'lumotlari va boshqa maxfiy ma'lumotlarni o'g'irlashi mumkin. Bu ma'lumotlar keyinchalik kiberjinoiyatchilar tomonidan moliyaviy firibgarlik yoki identifikatsiya o'g'irlashda ishlatilishi mumkin.

Masalan, agar sizning bank kartangiz ma'lumotlari o'g'irlansa, hujumchilar sizning hisobingizdan pul o'g'irlashi mumkin.

3.3. Tizim ishlashining buzilishi

Viruslar kompyuter tizimini sekinlashtirishi, dasturlarning ishdan chiqishiga sabab bo'lishi yoki tizimni butunlay ishdan chiqarishi mumkin. Ba'zi viruslar operatsion tizimning asosiy fayllarini buzadi, natijada kompyuterni qayta o'rnatish kerak bo'ladi.

Qurtlar esa tarmoq kengligini to'ldirish orqali internetni sekinlashtirishi yoki butunlay ishdan chiqarishi mumkin.

3.4. Moliyaviy yo'qotishlar

Ransomware hujumlari to'lov talabini yuboradi, va ko'plab kompaniyalar o'z ma'lumotlarini qaytarish uchun katta miqdorda to'lov to'lashga majbur bo'ladi. Bundan tashqari, tizimni tiklash, ma'lumotlarni qayta tiklash va xavfsizlik tizimlarini yangilash ham qo'shimcha xarajatlar talab qiladi.

4. Himoya choralari va tavsiyalar

4.1. Antivirus dasturlarini o'rnatish

Ishonchli antivirus dasturini o'rnatish va uni muntazam yangilab turish eng asosiy himoya choralaridan biridir. Zamonaviy antivirus dasturlari zararli dasturlarni aniqlash, blokirovka qilish va yo'q qilish qobiliyatiga ega.

Mashhur antivirus dasturlari orasida Kaspersky, Norton, Avast, Bitdefender va boshqalar mavjud. Bepul versiyalar ham bo'lsa-da, to'liq versiyalar ko'proq himoya beradi.

4.2. Operatsion tizim va dasturlarni yangilab turish

Dasturiy ta'minot ishlab chiqaruvchilari muntazam ravishda xavfsizlik zaifliklarini tuzatish uchun yangilanishlar chiqaradi. Operatsion tizim (Windows, macOS, Linux) va barcha dasturlarni (brauzer, Office, PDF o'quvchi) doimiy yangilab turish kerak.

Avtomatik yangilanishlarni yoqib qo'yish tavsiya etiladi, bu xavfsizlik teshiklarini tezda yopishga yordam beradi.

4.3. Noma'lum manbalardan ehtiyot bo'lish

Noma'lum elektron pochta xabarlaridagi havolalar va ilovalarni ochmang. Agar xabar shubhali ko'rinsa yoki kutilmagan bo'lsa, uni o'chiring. Faqat ishonchli veb-saytlardan dastur va fayllarni yuklang.

Phishing hujumlaridan ehtiyot bo'lish uchun har doim yuboruvchi manzilini tekshiring va shubhali havolalarni bosmang.

4.4. Kuchli parollar ishlatish

Barcha hisoblaringiz uchun murakkab va noyob parollar yarating. Parolda katta va kichik harflar, raqamlar va maxsus belgilar bo'lishi kerak. Bir xil parolni turli saytlarda ishlatmang.

Parol menejerlari (1Password, LastPass, Bitwarden) yordamida barcha parollaringizni xavfsiz saqlashingiz mumkin.

4.5. Ikki faktorli autentifikatsiyani yoqish

Ikki faktorli autentifikatsiya (2FA) qo'shimcha xavfsizlik qatlami qo'shadi. Shunchaki parol kiritish bilan emas, balki telefon orqali yuborilgan kod yoki autentifikatsiya ilovasi orqali ham tasdiqlash talab qilinadi.

Ko'pgina xizmatlar (Google, Facebook, Microsoft) 2FA-ni qo'llab-quvvatlaydi va uni yoqish tavsiya etiladi.

4.6. Ma'lumotlarni muntazam zaxiralash

Muhim fayllaringizni muntazam ravishda tashqi qattiq diskka yoki bulut xizmatlariga (Google Drive, Dropbox, OneDrive) zaxiralang. Bu ransomware hujumlari yoki boshqa hodisalar natijasida ma'lumotlar yo'qolishining oldini oladi.

3-2-1 qoidasini qo'llang: 3 nusxa saqlansin (asl + 2 zaxira), 2 xil muhitda (masalan, kompyuter va tashqi disk), 1 tasi internetda (bulut).

4.7. Firewall va xavfsizlik sozlamalarini yoqish

Firewall (xavfsizlik devori) tarmoq trafigini nazorat qiladi va keraksiz ulanishlarni blokirovka qiladi. Ko'pchilik operatsion tizimlarda o'rnatilgan firewall mavjud, uni faollashtirib qo'yish kerak.

Shuningdek, router sozlamalarini tekshiring va noma'lum qurilmalarning tarmoqqa kirishini cheklang.

4.8. Tashqi qurilmalardan ehtiyot bo'lish

Noma'lum USB qurilmalarini ehtiyotkorlik bilan ishlating. Avval antivirus bilan tekshirmay ochish xavfli bo'lishi mumkin. Avtomatik ishga tushirish (autorun) funksiyasini o'chiring.

Xulosa

Zararli viruslar zamonaviy raqamli texnologiyalar davrida jiddiy xavf hisoblanadi. Ular turli yo'llar bilan tarqalishi, ma'lumotlarni yo'qotish, shaxsiy ma'lumotlarni o'g'irlash va moliyaviy zararlarga olib kelishi mumkin. Ammo to'g'ri himoya choralari qo'llash orqali bu xavflarni sezilarli darajada kamaytirish mumkin.

Antivirus dasturlarini o'rnatish, tizimni yangilab turish, kuchli parollar ishlatish, ikki faktorli autentifikatsiya va ma'lumotlarni muntazam zaxiralash — bularning barchasi sizning raqamli xavfsizligingizni ta'minlashga yordam beradi.

Kiberxavfsizlik — bu bir martalik chora emas, balki doimiy jarayon. Texnologiyalar rivojlanib borayotgani kabi, yangi xavflar ham paydo bo'lmoqda. Shuning uchun doimiy ravishda ehtiyot bo'lish, o'rganib turish va eng so'nggi himoya usullarini qo'llash zarur.

Esingizda bo'lsin: kiberxavfsizlik siz bilan boshlanadi. Ehtiyotkorlik va to'g'ri amallar sizning kompyuter va shaxsiy ma'lumotlaringizni himoya qilishning eng yaxshi yo'li hisoblanadi.