INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.2 №5 (2024). May
innovativepublication.uz

Kompyuter viruslari va zararli dasturlar bilan ishlash

Yusufjonov Bahrom Yo‘ldoshovich
ilmiy izlanuvchi, O‘zbekiston davlat jahon tillari universiteti Xalqaro munosabatlar yo‘nalishi 1-kurs talabasi

Annotatsiya: Hammamizga ma’lumki hozirgi biz yashayotgan raqamli dunyoda hayotimizning har bir jabhasi raqamli axborot texnologiyalariga chambarchas bog‘liqdir. Yana shuni aytib o‘tishimiz kerak axborot texnologiyalari rivojlangan sari axborotning yaxlitligiga, uning dalxsizligiga bo‘lgan tahdidlar kuchayib bormoqda, buni esa biz anchagina ko‘payib borayotgan va asosan software tizimlarini shikastlashga qaratilgan viruslar hamda zararli dasturlar misolida ko‘rishimiz mumkin. Kompyuter viruslari va zararli dasturiy ta'minot raqamli xavfsizlikka sezilarli xavf tug'diradi va tizimlar va ma'lumotlarga jiddiy zarar etkazishi mumkin. Ushbu xavflarni tushunish samarali himoya choralarini amalga oshirish uchun juda muhimdir va bugunning dolzarb masalasi bo‘lgan axborot xavfsizligini ta’minlashning asosiy komponentlaridan biridir.

Kalit so‘zlar: kiber xavfsizlik, EHM, worms, trojan, Email attachments, Infected devices, Fishing attacks, operatsion tizim, antivirus dasturlari.

Albatta axborot xavfsizligini ta’minlash uchun birinchi navbatda kompyuter viruslari va umuman olganda raqamli dunyoda virus nimaligini, u qaysi turlarga bo‘linishini, shuningdek qaysi dasturlar kompyuter uchun zarali bo‘lishini bilib olishimiz kerak.Mana shu yerda bir savol tug‘ilishi tabiiy. Xo‘sh nega biz kompyuter viruslari turlarini o‘rganishimiz kerak? Negaki kompyuter viruslari turlarini, ularning kelib chiqishini o‘rganish orqali ularga qarshi samarali himoya chorasini tezroq topishimiz mumkin bo‘ladi

Shu o‘rinda kompyuter virusi o‘zi nima ekanligini bilib olish maqsadga muvofiq bo‘ladi. Kompyuter virusi — EHM ning xavfli „dasturi“. Kompyuter egasini ogoxlantirmay va uning istagiga qarshi uning dasturiga „joylashtiriladi“ va zaryadlangan faylni navbatdagi qo‘yishda ko‘payadi. Kompyuter virusi kompyuterning risoladagi ish me’yorini buzadi, ma’lumotlarni o‘chirib yuboradi, displey (monitor) ekranidagi tasvirni buzadi, hisoblash jarayonini sekinlashtiradi. Kompyuter virusi dasturini ishlab chiquvchilar 20-asr 80-yillari boshida AQShda paydo bo‘ldi, keyin dunyoning barcha mamlakatlariga tarqaldi. Kompyuter virusiga qarshi kurashish uchun maxsus dasturlar ishlab chiqiladi [1]. Lekin yana bir narsani aytib o‘tishimiz kerakki hozirgi kunga kelib viruslar mutatsiyasi ham ancha rivojlanib bormoqda. Bir qancha viruslarning birlashishi natijasida yangidan yangi viruslar vujudga kelmoqda. Kompyuter viruslarining turlari xilma-xildir. Quyidagilar ularga yorqin misol bo‘ladi.

- Troyan viruslari (Trojan horses)
- Chuvalchang viruslar (Worms)
- Boot sektor viruslari (Boot sector viruses)
- Makro viruslar (Macro viruses)
- Operativ xotirada yashovchi viruslar (Memory Resident Viruses)
- Rootkit viruslari (Rootkit viruses)
- O‘zgaruvchan viruslar (Polymorphic viruses)
- Vaqt bombasi viruslari (Time or Logic Bombs)[2]

Bu viruslar asosan kompyuterlarning zararlaydigan qismi, zararlash usullari va qanday qilib kompyuterga kirib olishlari bilan bir-biridan farq qiiladi. Bunday zararli viruslarni yuqtirib olishga to‘xtaladigan bo‘lsak, biz ularni quyidagi 3 turga bo‘lishimiz mumkin: bular **Email attachments, Infected devices** va **Fishing attacks.** Amail attachmentda qurilmalar ko‘pincha zararli viruslari bo‘lgan electron pochta ilovalari orqali zararlanadi, Fishing attackslarda esa soxta web saytlar va electron pochta manzillari orqali

viruslar tarqaladi, oxirgi turida, yani Infected devicesda zararlangan USB-driverlari va tashqi qurilmalar viruslarning asosiy tashuvchisi bo‘ladi. Kompyuter virus bilan zararlanganini o‘z vaqtida aniqlash ham uni himoya qilishning muhim qadamlaridan biridir. Kompyuterning virus bilan zaralanganligini ko‘rsatuvchi bir qancha belgilar mavjud.

- Birinchidan, kompyuter operatsion tizimi faoliyatining sekinlashuvi, kompyuterning odatdagidan ancha sekin ishlashi.
- Ikkinchidan, axborotning yo‘qolishi, ya’ni muhim fayllarning o‘z-o‘zidan g‘oyib bo‘lishi.
- Uchinchidan, turli xil oynalarning bir vaqtda ochilib yopilishi.

Yuqorida ko‘rsatib o‘tilgan belgilarning kompyuterda uchrashi uning viruslar bilan zararlanganligidan dalolat beradi. Bunday holatlarda esa biz antivirus dasturlaridan foydalanishimiz kerak. Hozirgi vaqtda viruslarni yo'qotish uchun ko'pgina usullar ishlab chiqilgan va bu usullar bilan ishlaydigan dasturlarni antiviruslar deb atashadi. Antiviruslarni, qo'llanish usuliga ko'ra, quyidagilarga ajratishimiz mumkin: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar.

Detektorlar — virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo'yicha tezkor xotira va fayllarni ko'rish natijasida ma'lum viruslarni topadi va xabar beradi.

Faglar — yoki doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oldingi holatiga qaytaradi.

Vaktsinalar — yuqoridagilardan farqli ravishda himoyalanayotgan dasturga o'rnatiladi.

Filtrlar — qo'riqlovchi dasturlar ko'rinishida bo'lib, rezident holatda ishlab turadi va viruslarga xos jarayonlar bajarilganda, bu haqda foydalanuvchiga xabar beradi.

Revizorlar (CRC-skaner, Monitor) — eng ishonchli himoyalovchi vosita bo'lib, diskning birinchi holatini xotirasida saqlab, undagi keyingi o'zgarishlarni doimiy ravishda

nazorat qilib boradi(Kaspersky Monitor)[3]. Masalan eng keng tarqalgan antivirus dasturlaridan bir bu Kasperskiydir va bu antivirus dasturi 1.5 milliondan ortiq virus dasturlarini (2009-yil malumoti) aniqlay oladi.

Agarda kompyuter virus bilan zaralangan bo‘lsa, birinchi navbatda uni tizimdan ajratib qo‘yish, ya’ni internet tarmog‘idan uzish lozim, shu yo‘l bilan uni tarqalishini oldini olish mumkin. Keyingi qadam esa bu antivirus dasturlari yordamida uni skanerlash va olib tashlash bilan amalga oshiriladi. Yana bir muhim qadamlardan biri esa bu professional malakali yordamda foydalanishdir. Agarda antivirus dasturlari ham yordam bermasa, oxirgi aytib o‘tilgan chora tadbirni qo‘llab, kiber xavfsizlik mutaxssisiga murojaat qilish lozim. Lekin albatta virusni yuqtirib uni tozalashdan ko‘ra, kompyuter tizimini virus yuqtirishdan ximoyalash anchagina oson. Kompyuterni viruslar bilan zararlanishidan saqlash va axborotlarni ishonchli saqlash uchun quyidagi qoidalarga amal qilish lozim:

- kompyuterni zamonaviy antivirus dasturlar bilan ta’minlash;
- disketalarni ishlatishdan oldin har doim virusga qarshi tekshirish;
- qimmatli axborotlarning nusxasini har doim arxiv fayl ko‘rinishida saqlash;
- operatsion tizimni va dasturlarni doimo yangilab turish;
- shubxali internet saytlari va electron xabarlardan extiyot bo‘lish

Xulosa o‘nida aytishimiz mumkin bugungi kunda axborot xurujlarini qaytatarish unga bo‘lgan taxdidlarni bartaraf etish uchun zararli viruslardan hamda dasturlardan extiyot bo‘lishimiz lozim. Shuningdek yangi virus tahdidlari haqidagi bilimlarimizni muntazam yangilab borishimiz lozim. Yuqorida ta’kidlab o‘tilgan chora tadbirlar orqali muhim fayllar va malumotlarning xavfsizligini ta’minlash yoki eng kamida ularning xavfsizlik darajasini oshirishimiz mumkin. Lekin shuni unutmasligimiz kerakki hozirgi raqamli dunyoda ogohlik bu davrning eng katta talabidir.

Foydalanilgan adabiyotlar ro‘yxati:

1. https://www.wikipedia.uz

2. Terabayt.uz, “Kompyuter viruslari haqida va ularning turlari”, Said Mamurov

3. https://www.texnoman.uz