ISSN 2181-3187

KOMPYUTER VIRUSLARI VA ULARGA QARSHI KURASHISH

Bahramov Muhammadali Eraliyevich
University of Management and Future Technologies
bahromov1997.04.09@gmail.com

Annotatsiya

Ushbu maqolada kompyuter viruslari, ularning turlari, ishlash prinsiplari va xavflari haqida batafsil ma'lumot beriladi. Kompyuter viruslari zamonaviy axborot texnologiyalarining eng katta tahdidlardan biri bo‘lib, ular foydalanuvchilarning shaxsiy ma'lumotlarini o‘g‘irlash, tizimlarni buzish yoki ularni ishlamay qolishiga olib kelishi mumkin. Maqola, viruslarning qanday tarqalishi, qanday ishlashi va ulardan qanday himoyalanish haqida ilmiy va amaliy yondashuvlarni o‘rganadi. Shuningdek, viruslarga qarshi kurashishning zamonaviy usullari va antivirus dasturlarining ahamiyati ham ko‘rib chiqiladi. Maqsad - foydalanuvchilarni kompyuter viruslari haqida xabardor qilish va ularni himoya qilish uchun samarali choralar ko‘rishning ahamiyatini tushuntirishdir.

Kalit so’zlar: Kompyuter viruslari, xavf, antivirus dasturlari, tizim xavfsizligi, ma'lumot o‘g‘irlash, zararlangan fayllar, himoya, kompyuter hujumlari, virus turlari, tizimni buzish, tarqalish, zararli dasturlar, himoya choralar, axborot texnologiyalari, infektsiya, shaxsiy ma'lumotlar, tizim ishlashini bloklash.

Kompyuter viruslari — bu zararli dasturlar bo‘lib, ular kompyuter tizimlariga kirib, ishlashini buzishi, ma'lumotlarni o‘g‘irlashi yoki tizimni ishlamay qolishiga olib kelishi mumkin. Viruslar zamonaviy axborot texnologiyalari sohasida keng tarqalgan xavf hisoblanadi, va ularning keltirib chiqaradigan oqibatlari juda jiddiy bo‘lishi mumkin. Quyida kompyuter viruslarining xavflari va ularning mumkin bo‘lgan oqibatlari haqida batafsil ma'lumot keltirilgan:

1. **Ma'lumotlarni yo‘qotish**

Viruslar kompyuter tizimiga kirib, foydalanuvchining shaxsiy yoki ish ma'lumotlarini yo‘qotishi mumkin. Ba'zi viruslar fayllarni shifrlash orqali foydalanuvchi ma'lumotlariga kirishni bloklaydi, yoki ma'lumotlarni o‘chirib yuboradi. Bu o‘z-o‘zidan katta iqtisodiy va moddiy zarar keltirishi mumkin.

2. **Shaxsiy ma'lumotlarni o‘g‘irlash**

Ba'zi viruslar foydalanuvchilarning shaxsiy ma'lumotlarini (parollar, bank kartalari raqamlari, elektron pochta manzillari va boshqalar) o‘g‘irlab, ular bilan noqonuniy

ISSN 2181-3187

amallarni amalga oshirishi mumkin. Masalan, bank hisoblariga kirib, pul o‘tkazmalari qilish.

3. **Tizim resurslarini isrof qilish**

Viruslar kompyuterning tizim resurslarini (masalan, protsessor quvvatini yoki xotirani) ortiqcha ishlatib, tizimning ishlashini sekinlashtirishi yoki butunlay bloklashi mumkin. Bu ish unumdorligiga salbiy ta'sir ko‘rsatadi.

4. **Tizimga kirish imkoniyatini bloklash (Denial of Service - DoS)**

Ba'zi viruslar kompyuter tizimini ishlashdan to‘xtatish yoki xizmatlarni bloklashga olib keladi. Misol uchun, tizimni band qilish yoki boshqa qurilmalarga kirish imkoniyatini cheklash.

5. **Agar boshqa zararli dasturlar bilan birgalikda ishlasa**

Ba'zi viruslar boshqa zararli dasturlarni, masalan, trojanlar yoki wormlarni o‘rnatish uchun ishlatiladi. Bu o‘z navbatida kompyuter tizimining boshqa qismlariga zarar yetkazishi yoki boshqa qurilmalarga tarqalishi mumkin.

6. **Kompaniyalar uchun moliyaviy zararlar**

Agar virus korxona tizimlariga kirib, muhim ma'lumotlarga zarar yetkazsa yoki ish faoliyatini to‘xtatib qo‘ysa, kompaniya katta moliyaviy zarar ko‘rishi mumkin. Shu bilan birga, bu kompaniyaning obro‘si va mijozlar ishonchini yo‘qotishiga olib kelishi mumkin.

7. **Viruslarning tarqalishi**

Kompyuter viruslari tarmoqlar orqali tez tarqaladi. Bir kompyuterdan boshqasiga o‘tishi, masalan, elektron pochta orqali yoki internetda tarqatilgan zararli linklar orqali bo‘lishi mumkin. Shuning uchun, bitta infektsiyalangan qurilma butun tarmoqni xavf ostiga qo‘yishi mumkin.

8. **Avtomatik o‘zgarishlar va tizim xavfsizligini kamaytirish**

Ba'zi viruslar tizimning xavfsizlik sozlamalarini o‘zgartirib, antivirus dasturlari va xavfsizlikni ta'minlovchi boshqa dasturlarning faoliyatini bloklashadi. Bu foydalanuvchining tizimini qo‘shimcha himoya choralari olishdan mahrum qiladi.

Kompyuter viruslari turli xil shakl va usullarda tarqalishi mumkin. Har bir virus turining o‘ziga xos xususiyatlari va zararli ta'sirlari bor. Quyida kompyuter viruslarining asosiy turlari va ularning tavsiflari keltirilgan:

1. Fayl viruslari (File Viruses)

Fayl viruslari kompyuter tizimidagi bajariladigan fayllarni (EXE, COM, BAT kabi) maqsad qilgan holda tarqaladi. Ular odatda faylni o‘zgartirib, zararli kod qo‘shadi va shu orqali boshqa tizimlarga kirish imkoniyatini oshiradi. Fayl viruslari tizimda ishlashga kirishganida, odatda o‘zgartirilgan fayllar orqali boshqalarga ham yuqadi.

ISSN 2181-3187

2. Boot sektor viruslari (Boot Sector Viruses)

Boot sektor viruslari kompyuterni yoqish jarayonida tizimning "boot sektor"iga kirib, zararli kodni o‘rnatadi. Bu viruslar odatda kompyuterning operatsion tizimini ishga tushirish vaqtida faollashadi. Boot sektor viruslari USB flesh-disklar va boshqa tashqi qurilmalar orqali tarqalishi mumkin.

3. Makro viruslari (Macro Viruses)

Makro viruslari, odatda, Microsoft Word, Excel va boshqa ofis dasturlarida ishlatiladigan makro funksiyalarini suiiste'mol qiladi. Bu viruslar hujjatga qo‘shilgan kod orqali tarqaladi va foydalanuvchi hujjatni ochganida yoki tahrir qilganida ishga tushadi. Makro viruslari tizimga zarar keltirishi yoki foydalanuvchi ma'lumotlarini o‘g‘irlamoqchi bo‘lishi mumkin.

4. Trojanlar (Trojan Horses)

Trojanlar — bu zararli dasturlar bo‘lib, ular foydalanuvchiga foydali yoki zararli ko‘rinishda bo‘lishi mumkin, ammo ichida virus yoki boshqa zararli kodlar bor. Trojanlar tizimga kirib, foydalanuvchining shaxsiy ma'lumotlarini o‘g‘irlaydi yoki boshqa zararli amallarni bajaradi, lekin foydalanuvchi ularni odatiy dasturlar kabi ishlatayotgan bo‘lib ko‘rinadi.

5. Wormlar (Worms)

Wormlar tarmoq orqali tarqaladigan va tizimga o‘rnatiladigan viruslardir. Wormlar boshqa tizimlarga o‘z-o‘zidan tarqaladi va foydalanuvchining aralashuvini talab qilmaydi. Ular tarmoq orqali bir tizimdan boshqasiga ko‘chib, ko‘p hollarda tizimni sekinlashtiradi yoki tarmoqqa zarar yetkazadi.

6. Ransomware (Zarba dasturlari)

Ransomware (zaharlangan dasturlar) viruslari foydalanuvchining ma'lumotlarini shifrlab, undan keyin ma'lum bir pul miqdorini talab qiladi. Foydalanuvchi pul to‘lagan taqdirdagina shifrlangan ma'lumotlarni qayta olish imkoniga ega bo‘ladi. Bu viruslar ko‘pincha elektron pochta yoki zararli veb-saytlar orqali tarqaladi.

7. Adware (Reklama dasturlari)

Adware — bu foydalanuvchining kompyuterida reklama ko‘rsatadigan dasturlardir. Bu dasturlar ko‘pincha zararli bo‘lmasa-da, foydalanuvchi uchun bezovta qilish va tizimni sekinlashtirish kabi noxush oqibatlarga olib kelishi mumkin. Ba'zi adware dasturlari, foydalanuvchi harakatlarini kuzatib, shaxsiy ma'lumotlarni yig‘ish ham mumkin.

8. Spyware (Spyware dasturlari)

Spyware viruslari foydalanuvchining shaxsiy ma'lumotlarini, internetda qidiruv tarixini va boshqa xususiy ma'lumotlarni kuzatadi. Ular odatda foydalanuvchining roziligisiz tizimga o‘rnatiladi va to‘plangan ma'lumotlarni uzatadi. Spyware ko‘pincha reklama va phishing hujumlarini amalga oshirishda ishlatiladi.

ISSN 2181-3187

9. Rootkit'lar (Rootkits)

Rootkit — bu tizimda "root" yoki "administrator" huquqlariga ega bo‘lishga mo‘ljallangan virus. Ular tizimdagi xavfsizlikni o‘zgartirib, antivirus dasturlarining virusni aniqlash imkoniyatlarini cheklaydi. Rootkit tizimga kirganidan so‘ng, boshqa zararli dasturlarni yashirishi mumkin.

10. Fileless viruslar

Fileless viruslar faylga o‘rnatilmasdan, faqat tizimning xotirasida ishlaydi. Ular odatda tizimda mavjud bo‘lgan qonuniy dasturlarni suiiste'mol qilib, zararli kodlarni ishga tushiradi. Fileless viruslar an'anaviy antivirus dasturlari tomonidan aniq bo‘lishi qiyin, chunki ular fayllarda saqlanmaydi.

Kompyuter viruslarining har bir turi o‘ziga xos xususiyatlarga ega bo‘lib, ular har xil usullar bilan tizimga zarar yetkazishi mumkin. Viruslardan himoya qilish uchun doimiy antivirus dasturlari o‘rnatish, tizimni yangilab turish va ehtiyotkorlik bilan internetda harakat qilish zarur.

Xulosa

Kompyuter viruslari zamonaviy texnologiyalar rivojlanishi bilan birga keng tarqalgan va jiddiy xavfga aylangan. Ularning turli turlari, masalan, fayl viruslari, trojanlar, wormlar, ransomware va boshqalar, kompyuter tizimlariga turli usullar bilan zarar yetkazishi mumkin. Viruslar tizimni buzish, ma'lumotlarni o‘g‘irlash, tizim resurslarini isrof qilish yoki foydalanuvchi ma'lumotlariga zarar yetkazish kabi jiddiy oqibatlarga olib kelishi mumkin. Shuningdek, ba'zi viruslar tarqalishida tarmoqlar, elektron pochta yoki zararli veb-saytlar orqali ishlaydi, bu esa butun tarmoq xavfsizligini tahdid ostiga qo‘yadi.

Viruslardan himoya qilish uchun antivirus dasturlaridan foydalanish, tizim yangilanishlarini o‘rnatish, ehtiyotkorlik bilan internetda harakat qilish va foydalanuvchining xavfsizlik bo‘yicha bilimlarini oshirish zarur. Shuningdek, viruslar tarqalishini oldini olish uchun foydalanuvchilarni har doim xabardor qilish va ularga xavfsizlik choralarini qo‘llashni o‘rgatish muhimdir. Tizim xavfsizligini ta'minlash va kompyuter viruslari tomonidan keltirilishi mumkin bo‘lgan zararlarni kamaytirish uchun yuqoridagi choralarga amal qilish muhimdir.

Foydalanilgan adabiyotlar

1. Eugene H. Spafford, "The Protection of Computer Systems"
2. William Stallings, "Computer Security: Principles and Practice"
3. Peter Szor, "The Art of Computer Virus Research and Defense"
4. Cheswick, W. R., & Bellovin, S. M., "Firewalls and Internet Security: Repelling the Wily Hacker"