ISSN 3060-4567

KOMPUTER VIRUSLARI VA ULARNING ZARARLI OQIBATLARI

Dang'ara 1-son Politexnikumi

Xidirova Feruzaxon Bahodirovna

Annotatsiya: *Ushbu maqola kompyuter viruslarining mohiyati, turlari va tarqalish usullarini ko'rib chiqadi. Viruslarning kompyuter tizimiga, ma'lumotlarga va shaxsiy hayotga yetkazishi mumkin bo'lgan zararli oqibatlari tahlil qilinadi. Maqola kompyuter viruslaridan himoyalanish usullarini, jumladan, antivirus dasturlaridan foydalanish, dasturiy ta'minotni yangilab turish va internetda ehtiyotkor bo'lishni tavsiya etadi. Maqsad - foydalanuvchilarni kompyuter viruslarining xavfi haqida xabardor qilish va ularni himoya choralarini ko'rishga undash.*

Kalit so'zlar: *Kompyuter viruslari, zararli dastur , ma'lumot xavfsizligi, antivirus, tazyiq dasturlari (Ransomware), josuslik dasturlari (Spyware), kiberxavfsizlik, ma'lumot yo'qotish, shaxsiy ma'lumotlar.*

Компьютерные вирусы и их вредное воздействие

Абстракт: *В статье рассматриваются природа, типы и способы распространения компьютерных вирусов. Анализируется пагубное воздействие вирусов на компьютерные системы, данные и конфиденциальность. В статье рекомендуются способы защиты от компьютерных вирусов, в том числе использование антивирусного программного обеспечения, регулярное обновление программного обеспечения и соблюдение осторожности в Интернете. Цель — информировать пользователей об опасностях компьютерных вирусов и побуждать их принимать меры защиты.*

Ключевые слова: *компьютерные вирусы, вредоносное ПО, информационная безопасность, антивирус, программы-вымогатели, шпионское ПО, кибербезопасность, потеря данных, персональные данные.*

Computer viruses and their harmful effects

Annotation: *This article examines the nature, types and methods of distribution of computer viruses. The harmful effects that viruses can have on a computer system,*

ISSN 3060-4567

data and personal life are analyzed. The article recommends methods of protection against computer viruses, including the use of antivirus programs, keeping software up to date and being careful on the Internet. The goal is to inform users about the dangers of computer viruses and encourage them to take protective measures.

Keywords: *Computer viruses, malware, information security, antivirus, ransomware, spyware, cybersecurity, data loss, personal data.*

KIRISH. Hozirgi axborot texnologiyalari asrida kompyuterlar hayotimizning ajralmas qismiga aylandi. Ular orqali biz muloqot qilamiz, ishlaymiz, ta'lim olamiz va ko'ngilxushlik qilamiz. Biroq, bu qulayliklar bilan birga xavf ham keladi: kompyuter viruslari.

Kompyuter virusi – bu kompyuter tizimiga zarar yetkazish, ma’lumotlarni o‘g‘irlash yoki o‘chirish, tizim ishini buzish kabi zararli harakatlarni amalga oshirishga mo‘ljallangan dasturdir. Viruslar turli yo‘llar bilan tarqalishi mumkin: internetdan yuklab olingan fayllar, elektron pochta xabarlaridagi ilovalar, tashqi xotira qurilmalari (USB flesh-disklar) va hatto viruslangan veb-saytlarga tashrif buyurish orqali.

Kompyuter viruslarining asosiy turlari:

- Viruslar: Boshqa fayllarga yopishib oladi va ular ishga tushirilganda faollashadi. Ko'pincha executable fayllar (.exe, .com) yoki dokumentlar (.doc, .xls) ichida tarqaladi.
- Qurtlar: Tarmoqlar orqali o'zini nusxalash va tarqatish qobiliyatiga ega. Ular odam aralashuvisiz ham tarqalishi mumkin, masalan, zaif himoyalangan tizimlardan foydalanib.
- Troya otlari: O'zini foydali dastur sifatida ko'rsatadi, lekin aslida zararli funksiyalarni bajaradi. Foydalanuvchilarni aldab o'rnatishga undaydi.
- Tazyiq dasturlari (Ransomware): Kompyuterga kirishni bloklaydi yoki fayllarni shifrlaydi va ularni ochish uchun to'lov talab qiladi. Hozirda eng xavfli turlardan biri hisoblanadi.
- Josuslik dasturlari (Spyware): Foydalanuvchi haqida ma'lumot to'playdi (shaxsiy ma'lumotlar, internetda harakatlar) va uni uchinchi tomonlarga yuboradi.

• Reklama dasturlari (Adware): Keraksiz reklamalarni ko'rsatadi va foydalanuvchini bezovta qiladi. Ba'zan, shaxsiy ma'lumotlarni ham to'plashi mumkin.

• Rootkitlar: Viruslarni yashirish va tizimga chuqur kirib borish uchun ishlatiladi. Ularni aniqlash va o'chirish juda qiyin.

• Botnetlar: Ko'plab kompyuterlarni (botlarni) birlashtirib, markazdan boshqarish imkonini beradi. Ular DDoS hujumlarida, spam tarqatishda va boshqa noqonuniy maqsadlarda ishlatiladi.

Zamonaviy tendensiyalar:

• AI (sun'iy intellekt) dan foydalanish: Xakerlar hujumlarni avtomatlashtirish va yanada samarali qilish uchun sun'iy intellektdan foydalanmoqda.

• Zero-Day Exploits: Dasturiy ta'minotdagi noma'lum zaifliklardan foydalanib hujum qilish.

• DDoS hujumlari (Distributed Denial of Service): Veb-sayt yoki xizmatga haddan tashqari yuk tushirib, uning ishlashini to'xtatish.

• Deepfake Texnologiyalari: Soxta video va audio materiallar yaratish orqali odamlarni aldash.

Viruslarning zararli oqibatlari:

Kompyuter viruslari turli xil zararli oqibatlarga olib kelishi mumkin, jumladan:

Ma’lumotlarni yo‘qotish yoki shikastlash: Viruslar muhim fayllarni o‘chirishi, shifrlashi yoki buzishi mumkin, bu esa ma’lumotlarni yo‘qotishga olib keladi.Shaxsiy ma’lumotlarning o‘g‘irlanishi: Viruslar loginlar, parollar, kredit karta ma’lumotlari va boshqa shaxsiy ma’lumotlarni o‘g‘irlashi mumkin, bu esa shaxsiy hayotga putur yetkazadi va moliyaviy zarar keltiradi. Kompyuterning ishdan chiqishi: Viruslar tizim fayllarini shikastlashi va kompyuterning noto‘g‘ri ishlashiga, hatto ishdan chiqishiga olib kelishi mumkin. Pul yo‘qotish: Tazyiq dasturlari orqali pul talab qilinishi yoki shaxsiy ma’lumotlar o‘g‘irlanishi orqali moliyaviy zarar yetkazilishi mumkin. Maxfiylikning buzilishi: Josuslik dasturlari shaxsiy ma’lumotlarni to‘plashi va uni uchinchi tomonlarga yuborishi mumkin.

Kompyuter viruslaridan himoyalanish uchun bir qator choralar ko‘rish zarur:

• Antivirus dasturini o‘rnatish va muntazam yangilab turish.

- Operatsion tizim va boshqa dasturlarni doimiy ravishda yangilab turish.
- Ishonchsiz manbalardan fayllarni yuklab olmaslik va shubhali elektron pochta xabarlarini ochmaslik.
- Kuchli parollardan foydalanish va ularni hech kim bilan baham ko‘rmaslik.
- Fleshkalarni va boshqa tashqi xotira qurilmalarini tekshirib turish.
- Shubhali veb-saytlarga kirmaslik.
- Internetda ehtiyotkor bo‘lish va shaxsiy ma’lumotlarni faqat ishonchli saytlarda kiritish.

Xulosa:

Axborot texnologiyalari rivojlanishi bilan kompyuter viruslari va kiberhujumlar tobora murakkablashib bormoqda. Ushbu maqolada ko'rib chiqilganidek, viruslarning asosiy turlari va hozirgi zamonaviy tahdidlar kompyuter tizimlari, ma'lumotlar va shaxsiy hayot uchun jiddiy xavf tug'diradi. Xususan, ransomware hujumlari, fishing firibgarliklari, ta'minot zanjiri hujumlari va mobil zararli dasturlar nafaqat moliyaviy zarar yetkazishi, balki biznes jarayonlarini to'xtatib, shaxsiy ma'lumotlarning oshkor bo'lishiga ham olib kelishi mumkin.

Bugungi kunda sun'iy intellekt (AI) va zero-day zaifliklardan foydalanish, shuningdek, deepfake texnologiyalarining rivojlanishi kiberxavfsizlik sohasidagi vaziyatni yanada murakkablashtirmoqda. Bunday sharoitda har bir foydalanuvchi, tashkilot va davlat kiberxavfsizlikka jiddiy e'tibor qaratishi, zamonaviy himoya vositalaridan foydalanishi va xodimlarning kiberxavfsizlik bo'yicha bilimini oshirishi zarur.

Xulosa qilib aytganda, kompyuter viruslari va kiberhujumlarga qarshi kurash - bu doimiy jarayon. Yangi tahdidlar paydo bo'lishi bilan birga, himoya usullari ham takomillashib borishi kerak. Har bir foydalanuvchi va tashkilot kiberxavfsizlikni o'zining ustuvor vazifalaridan biri sifatida qabul qilib, zamonaviy himoya choralarini qo'llashi va kiberhujumlarga qarshi kurashishga tayyor bo'lishi zarur. Faqat shunday yondashuv orqali biz o'z ma'lumotlarimizni, tizimlarimizni va shaxsiy hayotimizni himoya qila olamiz.

ISSN 3060-4567

FOYDALANILGAN ADABIYOTLAR.

1. https://www.kaspersky.com – Kaspersky kompaniyasining rasmiy sayti, viruslar va kiberxavfsizlik haqida yangiliklar va hisobotlar.

2. https://www.symantec.com – Symantec (Norton) antivirus kompaniyasining rasmiysi, tahdidlar haqida ma'lumotlar.

3. Муртазин А. Компьютерная безопасность и антивирусная защита. – Санкт-Петербург: Питер, 2018.

4. Алешин С.В. Информационная безопасность: Учебник для вузов. – Москва: Юрайт, 2020.

5. Mandia, K., Prosise, C., Pepe, M. Incident Response and Computer Forensics. – McGraw-Hill, 2014.

6. Microsoft Security Intelligence Reports. – Microsoft rasmiy saytida chop etilgan hujjatlar.