KOMPYUTER VIRUSLARIDAN HIMOYALANISH YO‘LLARI

Nazarboyev Sardor Raim o‘g‘li
Maxsus fan o‘qituvchisi:
Kubayev Alisher Baxtiyorovich
Maxsus fan o‘qituvchisi:
Rustamova Feruza Isroilovna
Maxsus fan o‘qituvchisi:
Toshkent imkoniyati cheklangan shaxslar uchun ixtisoslashtirilgan 1-son kasb-hunar maktabi

Annotatsiya: *Maqolada kompyuter viruslari, ularning foydalanuvchilarga va kompyuterlarga keltirishi mumkin bo‘lgan zararlari va bu kabi viruslardan qanday himoyalanish usullari keltirilgan.*

Kalit so‘zlar: *alfanumerik belgi, anti-spyware, anti-malware, xavfsizlik devori, heuristic aniqlash, kross-platformali dastur.*

Kompyuter virusi – o‘z-o‘zini nusxalash qobiliyatiga ega bo‘lgan dastur kodi hisoblanadi va odatda, tizimni buzish va ma’lumotlarga zarar yetkazish kabi salbiy ta’sirlarni o‘zida jamlaydi. Viruslar dasturchidan ko‘plab kompyuterlarga nusxalash va hatto, ko‘zda tutilmagan foydalanuvchilarga ham dastur kodini tarqatish maqsadi bilan yaratiladi. Ozidan nusxa olishi virus bo‘lishlikning dastlabki belgilaridan va vazifasi faqat ko‘payish bo‘lgan viruslar ham talaygina. Ularning ko‘pchiligining boshqa ta’sirlari ham bor, musiqalarni qo‘yib yuborish, xabarnomalarni ko‘rsatish, va eng yomon holatda, foydalanuvchilarning qimmatli ma’lumotlarini yo‘q qilish. Ular yaratuvchi dasturchi ko‘zda tutgan barcha amallarni bajarish imkoniyatiga ega. Ba’zi virus yaratuvchilar o‘zlari kutgan darajada mohir emaslar, va natijada, rejalashtirib qilinmagan bo‘lsada, dasturlar to‘qnashuvi kabi kutilmagan natijalar ko‘zga ko‘rinadi

Buning ortida ko‘plab mumkin bo‘lgan sabablar bor, virus yaratuvchisi shaxsiy statusini oshirish uchun yoki ishdan bo‘shatilgan kompaniyadan qasos olish maqsadida, yo‘q qilinishi ko‘zda tutilayotgan ma’lumot uning hayot tarziga sezilarli ta’sir o‘tkazishi mumkin bo‘lgan hollarda yaratilishi mumkin. Virus dasturchilari yaratgan kodlari miqyosi bilan maqtanishni xush ko‘radilar, o‘zlarini kod nomlari bilan chaqiradilar. Tarmoq buzilishini nazorat qilish, masalan, yovuz niyatli kod yaratuvchisiga qudrat hissini beradi.

Viruslar ishga tushiriladigan kodda yashiringan bo‘ladi. Bu shunday ma’no anglatadiki, yuklab olingan har qanday dastur, mashinada qoldirilgan yumshoq disk dastur nusxalanish xavfini yaratadi. Ko‘pchilik odamlar viruslar faqat dastur nusxalarida va virus o‘rnashib qolgan dasturlardagina bo‘lishi mumkin deb ishonadi, lekin aslida bunday emas. 1992 yilda Borland o'zining C++ dasturlash tili dasturi bilan virus chiqardi (original qisqartirish bilan o'ralgan kumush CD) va butun dunyo bo'ylab minglab nusxalari jo'natildi. Bu, ehtimol, virusga qarshi tekshiruvlar yoki antivirus dasturiy ta'minot eskishiga qarshi yangilanishlarning yetishmasligi bilan bog'liq bo‘lishi mumkin. Ba’zi vaqtlarda

ko‘plab shaxsiy kompyuterlar kompakt disklarida nuqsonlar ko‘zga tashlangan, shuning uchun hatto nufuzli manbaalar dasturiy ta’minotlariga ham ishonish qiyin. Bundan tashqari, Internetdan yuklab olinadigan dasturiy ta'minotlarga ham ishonish kerak emas, lekin tez-tez foydalanishga ehtiyoj seziladi. Bu yerda muammolarni oldini oladigan yechim - dasturiy ta’minot va strategiya. Hujum qilinishi va virus dasturlarni o‘rnatish yo‘llari ko‘p ekaniga qaramasdan, kompyuter va tarmoqni kiber tahdidlardan himoyalashga yordam bera oladigan bir qancha usullar bor.

Kuchli kompyuter parollarini yoki ifodalarni yaratish, balki tizim xavfsizligini kengaytirishning eng oson usulidir. 8 dan 64 gacha alfanumerik belgilar va @, #, * va & kabi belgilardan foydalanib murakkab parol yoki ifodalarni yaratish lozim.

imkon bo‘lganda ikki bosqichli tasdiqlashni faollashtirish lozim.

Davriy ravishda yangilash yovuz kuchlarning parollarni yorib kirishlarini oldini olishga yordam berishi mumkin. Zararkunanda dastur hujumi test-va-xatolik usuli, bunda dastur parolni dekodlashga harakat qiladi va nishon kompyuteriga kirish imkoniyatini qo‘lga kiritadi. Parol qanchalik kuchli bo‘lsa, haker uchun uni yorib kirish shunchalik qiyin bo‘ladi.

Antivirus dasturi e.mailga bostirib kirishga harakat qiladigan viruslarni, tizim fayllarini yoki operatsion tizimni faol tekshiradi. Sifatli dastur paketini tanlash, kompaniya nufuzi va mahsulotini, dastur xususiyatlarini (m-n, kunlik yangilanishini) va kompyuterga mosligini yodda tutish lozim.

Viruslar, spyware va malware davomli ravishda rivojlanib bormoqda. Natijada, ba’zan ular tizim himoya usullarini buzib o‘tadi va kompyuter tizimiga yuqtiradi. Biror bir yoki qo‘shimcha zarar yetishidan avval tarmoqdagi yovuz agentlarni aniqlash, karantin e’lon qilish va olib tashlash uchun antivirus, anti-spyware va antimalware dasturlari orqali kunlik tekshiruvlarni bajarish kerak.

Yovuz agentlarning ko‘plab turlari kompyuter ichidagi kontentga zarar yetkaza oladi. Kompyuterga biror zararli voqea sodir bo‘lganda ma’lumotlarni qayta tiklash mumkin ekaniga ishonch hosil qilish uchun davriy zaxira tartibini tashkil qilish lozim. Bulut xizmati yoki shaxsiy tashqi qattiq disk kabi zaxira tanlovlardan foydalanish mumkin. Bulut xizmati ma’lumotlarni tarmoqda saqlashga imkon beradi. Shaxsiy tashqi qattiq disk kompyuterga ulanishi mumkin, shuning uchun yangilangan fayllarni zarurat paydo bo‘lganda nusxasini olishga imkoniyat bor.

Har qanday viruslarni, g‘ayritabiiyliklarni tuzatish uchun doimiy kompyuter tizimlari yangilanishlarini ishga tushirish muhim hisoblanadi. Yangilanishlarga ruxsat berilmasa, tizimda qolib ketuvchi viruslar hakerlar tomonidan ishlatilishi mumkin. Yangi tizim versiyasi e’lon qilingani bilan foydalanuvchi bundan xabardor bo‘lishi lozim.

Xavfsizlik devori kompyuterni o‘rovchi eng muhim jihat va u ruxsatsiz kirishni bloklaydi. Kompyuterni endi ishga tushirayotganda yoki sozlayotganda, operatsion tizimning xavfsizlik devori imkoniyatlaridan foydalanish lozim. Xavfsizlik devori sozlamalarini kompyuter afzalliklariga ko‘ra yangilash mumkin.

Hakerlar e.mailda ko‘pgina yo‘llarda ustunlikni qo‘lga kiritishi mumkin, masalan, emaillarga biriktirilgan kompyuter fayllarida. Tanimaydigan manzilli emaillarni ochish va

o‘qish tavsiya etilmaydi. Ularni zudlik bilan o‘chirib tashlash kerak.

Hatto eng xavfsiz web saytlar ham spyware va malware ni o‘z ichiga oladi. Virusni yuqtirish uchun sichqoncha bir marta chertilsa kifoya. Ko‘pgina soxta web saytlar haqiqiy web saytlarni taqlid qilish uchun niqoblangan. URL larni kiritayotganda saytning nomi, to‘g‘ri yozilganligini tekshirish kerak. To‘satdan paydo bo‘ladiganlarni, reklamalarni, grafiklarni va boshqa saytlarga linklarni bosishni oldin olish zarur.

Antivirus dasturlari va kompyuter himoyasi dasturiy ta’minoti malwarelarni topishga va mumkin bo‘lgan eng katta tezlikda ildizi bilan yo‘q qilib tashlashga yo‘naltirilgan web sahifalarni, fayllarni, dasturiy ta’minotlarni va murojaatlarni baholashga qaratilgan. Ko‘pchiligi faoliyat jarayonidagi kiruvchi tahdidlardan himoya bilan ta’minlaydi. Chunki hozirgi kunda ko‘plab jarayonlar tarmoqda tashkil qilinadi va yangi tahdidlar muntazam ravishda paydo bo‘ladi, himoyali antivirus dasturini o‘rnatish o‘zining dolzarbligini yanada orttirmoqda. Quvonarlisi shundaki, hozirgi kunda tanlab foydalanish uchun bir qancha a’lo darajadagi mahsulotlar bor.

Bu dasturiy mahsulotlar ularning xavfsizlik darajasini aniqlash uchun professional tarzda testdan o‘tkazilishi lozim. Har bir kompaniya o‘zining xususiyatlari ro‘yxatini tuzgan, chunki har qanday dasturiy ta’minotning ba’zi jihatlari qolganlariga nisbatan muhimroq hisoblanadi. Ularning ba’zilari:

- Foydalanuvchi interfeysi (qulay ko‘rinishga ega bo‘lmagan dasturlar, ko‘pincha, xaridorlar tomonidan yaxshi qabul qilinmaydi)
- Tekshirish va muammoni bartaraf qilish tezligi
- Parol himoyasini o‘z ichiga olgan moslashuvchanlik
- Xususiyatlarni hujjatlashtirish va qo‘llanmani tushunish qulayligi
- Konfiguratsiya va foydalanish uchun texnik malaka darajasi
- Texnik yordam sifati va tezligi
- Yangi viruslar bilan kurashish va muammoni hal qila olish tezligi
- Tarmoqni yangilash imkoniyati

Antivirus dasturiy ta’minoti kompyuter dasturlarini va fayllarni malwarening ma’lum ma’lumotlar bazasiga qarshi tekshirish orqali ishga tushishni boshlaydi. Hakerlar tomonidan hissa qo‘shilganligi va yangi viruslar doimiy ravishda yaratilganligi sababli, antiviruslar hali mavjud bo‘lmagan va ehtimoliy tahdidlar uchun ham tekshiradi. Umuman olganda, ko‘plab dasturlar uchta turli xil aniqlashlarni qo‘llashadi: muayyan aniqlash, avvaldan yaratilgan tahdidlarni tekshiradi; umumiy aniqlash, ko‘p uchraydigan kod bazasiga bog‘liq bo‘lgan belgilarni yoki mavjud qism yoki tiplarini qidiradi; va tajriba jarayonidagi(heuristic) aniqlash, shubhali fayl strukturalari orqali aniqlash orqali noma’lum viruslarni tekshirish. Qachonki dastur virusli faylni topganida, odatda uni karantinga qo‘yadi va o‘chirish belgisini beradi, kirib bo‘lmaydigan qiladi va xavfni olib tashlaydi. Kundalik hayot tarzida internetga ulangan qurilmalar bilan va bir paytning o‘zida xavfliroq hamdir. Keng tarqalgan antivirus dasturlarining viruslardan himoyalash imkoniyatlari

1. ESET NOD32, ko‘pincha NOD32 deb yuritiladi. Ikki xil nashrda chiqarilgan, Uy nashri va biznes nashri. Quyidagi xususiyatlarga ega:

- Anti-fishing

- Qurilma nazorati
- Bank ishi va to‘lov himoyasi rivojlantirilgan
- Ota-ona nazorati
- Web kamera nazorati
- Himoya devori
- Tarmoq tekshiruvi rivojlantirilgan
- Tarmoq hujumi himoyasi

2. Kasperskiy . Kasperskiy internet xavfsizligi malware, email spamlari, fishing, haking urunishlari va ma’lumolar o‘g‘irlanishidan himoyani taqdim etadi. Taklif etadigan xizmatlari:

- Ma’lumotlar himoyasi
- Ma’lumotlar zaxirasi
- Web siyosatlar – cheklashlar va foydalanuvchi faoliyatini yozib borish, Parol menejeri
- Ma’lumotlar shifrlanishi, Tarmoq nazorati
- So‘rovlar faoliyati

3. Avast Antivirus - bu Avast tomonidan Microsoft Windows, macOS, Android va iOS uchun ishlab chiqilgan kross-platformali (ya’ni, turli xil kompyuterlar bilan yoki har xil dasturiy ta’minot paketlari bilan ishlay oladigan) internet xavfsizligi ilovalari oilasi. Avast antivirus quyidagi xususiyatlarni o‘zida jamlagan:

- Anti-spam
- Ma’lumotlar qismlarga ajratuvchi
- Aqlli antivirus
- Uy tarmog‘i xavfsizligi
- Aqlli tekshiruv
- Xavfsiz domain nomi tizimi

FOYDALANILGAN ADABIYOTLAR:

1. Raxmonqulova IBM PC shaxsiy kompyuterlarida ishlash. Sharq NMK-S PRINT.
2. N.X.Noraliev.,N.Qilichev Informatika, o`quv qo`llanma,
3. https://www.techradar.com/best/best-antivirus
4. www.researchgate.net
5. www.google.com
6. https://www.eset.com/us/antimalware/
7. https://www.texnoman.uz/post/antiviruslarning-vazifasiga-kora-turlari.html