

KOMPYUTER VIRUSLARI VA ANTIVIRUS DASTURLARI HAQIDA MA'LUMOT.

Andijon Qishloq Xo'jaligi Va Agrotexnologiyalar Instituti

Raqamli Iqtisodiyot Yo'nalishi Talabasi

Turg'unov Ravshanbek To'lg'injon o'g'li

Tuproq Boniteritirovkasi Va Yer Resuslaridan Foydalanish Yo'nalishi 1-Bosqich

Talabasi

Mavlonova Mohlaroy Abdullaxo'ja qizi

Kalit so'zlar: *Kompyuter viruslari. Kompyuter viruslarini sinflarga ajratish*

Annotatsiya: *Kompyuter viruslari bugungi kunda ko'pchilikning eng dolzarb muammosidir. Bu hammani tashvishga solmoqda.*

Virus dasturi kompyuterdagi ma'lumotlar butunligini buzishga yoki ularni o'chirishga mo'ljallangan bo'ladi. Ilk bor virus dasturlari AQShda ishlab chiqarilgan, chunki aynan bu davlatda shaxsiy kompyuterlar keng tarqalgan edi. Ilk bor ishlab chiqarilgan virus dasturlari foydalanuvchini hotirjamligini buzishga va asabiga tegishga qaratilgan edi. Lekin keyinchalik ular zarar yetkazishni o'zining maqsadi sifatida qabul qilib oldi. Hozirgi paytda butun dunyo buyicha 200000 dan ortiq virus dasturlari mavjud. Ular kompyuter viruslari bo'lib, kompyuterdagi ma'lumotlarga zarar etkazadi yoki kompyuterning ishlash samaradorligini tushirib yuboradi.

Kompyuter virusi o'zi nima? Ular ma'naviy qashshoq, hayotdan va boshqalardan alamzada dasturchilar tomonidan g'arazli maqsadlarda yozilgan dastur. Ular odatda, ko'p martalab nusxalanadi va ijrochi fayllarga "yopishib oladi". Ularning "ishga tushishi" oqibatida goh displeyda turli yot yozuvlar paydo bo'lishi, goh disqdagi yozuvlar (fayllar) ni o'chirib yuborishi mumkin. Odatda foydalanuvchiga virus dasturlarining nomigina ma'lum bo'lishi mumkin. Masalan, Black Hole (qora teshik), Black Friday (qora juma), Friday 13 (o'n uchinchi juma), "sekin ta'sir qiluvchi virus" va hokazo. Mazkur viruslar ekranning chap burchagidan qora teshik ochishi yoki 13 sana juma kunlari ishlayotgan fayllarni yo'qotishi, bundan tashqari har 5 minutda kompyuter ishini bir necha yuz marotalab sun'iy sekinlashtirib yuborishi mumkin. Odatda TR-viruslar deb nomlanuvchi viruslar guruhi ajoyib xossaga ega. Zararlangan dasturni ko'rish chog'ida virus dasturi tuzatilgan dastur ichiga "suqilib" kirib oladi va o'zini namoyon etmaydi. Shunga o'xshash pokistoncha viruslar (Brain Ashet) ham zararlangan kompyuterlarda o'z "faoliyatini" ayyorlarcha olib boradi. Keng tarqalgan viruslarni ikki guruhga bo'lish mumkin: -fayllar uchun (SOM, YeXE va DLL ni zararlaydi); -Boot-viruslar (disketlarni boshlang'ich yuklovchi sektorlari yoki MBR (Master Boot Record) qattiq diskning yuklovchi sohasini zararlaydi. Tarmoqqa zarar keltiruvchi alohida viruslar ham mavjud. Ular replikatorlar deb atalib, tarmoqdagi barcha yoki ba'zi abonentlarni zararlaydi. Ulardan eng "taniqlisi" Morrisa nomlidir. 1988 yilda ushbu virus Internet tarmog'idagi 30000 ta kompyuterdan 6000 tasiga zarar keltirib, "karomat" ko'rsatgan.

FAYL VIRUSLARINI SINFLARGA AJRATISH.

Fayl viruslari kompyuterlarda keng tarqalgan viruslar. Ular barcha viruslarning tahminan 80% ini tashkil etadi. Bu toifa kompyuter viruslari juda chidamli bo'lib, o'z vaqtida ehtiyot chorasi ko'rilmasa, haqiqiy epidemiyaga aylanadi. Masalan, RCE-1813 yoki Ierusalem (Quddus), Black Friday (qora juma) va boshqa o'ta xavfli viruslardir. Ko'pchilik tarqalgan fayl viruslari shtammlarga ega, ular baza versiyalaridan uncha farq qilmaydi. Shuning uchun fayl viruslarini quyidagi guruhlarga bo'lish mumkin:

- Vena guruhi. Uning birinchi S-648 deb nomlanuvchi vakili Venada topilgan;
- CASCADE guruhi. RC-1701 deb nomlanuvchi birinchi vakili 1988 yil o'rtalarida topilgan;

- Quddus guruhi. RCE-1813 deb nomlanuvchi uning birinchi vakili 1987 yilning oxirida Quddus universitetida topildi; - TR viruslar guruhi - mazkur viruslar, taxminlarga ko'ra, Bolgariyada ishlab chiqilgan. O'z navbatida bu guruh uch kichik guruhga bo'linadi. VACSINE, "musiqali qayta yuklash" va "o'z-o'zini yeb qo'yuvchilar".

Ohirgi ikkitasini Vankey Doodle ham deb atashadi.

- Datacrime. Bu guruh vakillari joriy yilning 12 oktyabrida faollashadi va A, V, C, D disklarda 8 sektorni ishdan chiqaradilar. - Avenger guruhi. RCE-1800, RCE-1000 deb nomlanuvchi mazkur guruh katta zararlash imkoniyatiga ega. U nafaqat fayllarni bajarish chog'ida, balki uni o'qish va ochish vaqtida ham zararlaydi. Bundan tashqari, bu toifadagi viruslar davriy ravishda sektorlardagi fayl va katologlarni yo'qotadi. Vinchesterga matn xabarlarini yozadi. - Island guruhi (Icelandic). Shu yerda ta'kidlash kerakki, Datacrime va island guruhiga mansub viruslar hozircha bizning mamlakatimizda yo'q.

Boot viruslari fayl viruslaridan tubdan farq qiladi. Boot viruslarining soni fayl viruslariga qaraganda ancha kam va shuningdek, ular sekinroq tarqaladi. Fayl viruslari kabi ko'p tarqalgan Boot viruslari ham shtammlarga ega. Hozirgi vaqtda ushbu viruslarni quyidagi guruhlarga ajratish mumkin:

- Italiya guruhi. "Bxl-1S-a" deb nomlanuvchi uning birinchi vakili 1987 yilning oxirida paydo bo'ldi; - Pokiston guruhi. Bu guruhga Vgat 86 va Brain 88 viruslari kiradi. Birinchi vakili Vgat 86 Pokistonning Lahor shaxrida 1986 yil topilgan. Buzish darajasi bo'yicha viruslarni shartli ravishda ikki turga - "illyuzion" va "vandallar" ga bo'lish mumkin. "Illyuzion" guruh qandaydir yoqimli musiqa sadosi yoki namoyish orqali virusni yuqtiradi. "Vandal" so'zining o'zbekcha lug'aviy ma'nosi - madaniy yodgorliklarni harob etuvchi, xuddi shunday "vandallar" dasturni harob qiladi. Bu toifa viruslar yopiq holatda fayllarni bildirmasdan ishdan chiqaradi. Tabiiyki, ham fayl tizimini, ham yuklash (Boot) sektoriga zarar yetkazuvchi viruslar ham mavjud.

Dasturni dastlabki "sog'lom" holatga keltirish. Bu ish har bir fayldan zararli viruslarni "tishlab olib tashlash" usuli bilan amalga oshiriladi. Yuqorida aytilganlardan ko'rinib turibdiki, virusdan himoyalaniishning bir necha turdagi dasturiy vositalari mavjud: dastur-detektorlar (disketa yoki diskdagi viruslarni "tutadi") va

dastur-faglar (viruslardan davolaydi). Ular har bir foydalanuvchida bo'lishi va kompyuter ishga tushirilishidan oldin doimo sinab ko'rilishi kerak.

Shuni ta'kidlash kerakki, eng qulay detektorlar bir emas, ko'plab keng tarqalgan viruslarni "ushlaydi". Dastur-fayllar zararlangan dasturlarni tiklashni ta'minlaydi. Ish jarayonida faga virus tanasini "tishlaydi" va virus o'zgartirib yuborgan buyruqlar ketma-ketligini tiklaydi. Biz tilga olayotgan kompyuter viruslari fagasi hozirda yaratilib bo'lingan. Hozir turli fagalarni yig'ish bilan odamlar band bo'lishmoqda. Bu, bizningcha, noto'g'ri. Asosiy e'tiborni zararlanishning oldini olishga qaratish lozim. "1 gramm profilaktika 1 kilogramm davolashga teng" maqoli naqadar to'g'ri.

Antivirus dasturlarini ishlatishdagi yo'l qo'yilishi mumkin bo'lgan xatolarga batafsil to'xtab o'tamiz. Antivirus vositalarini qo'llashdagi eng ko'p yo'l qo'yiladigan xato - zararlangan kompyuterda ularni ishlatib yuborishdir. Virus aniqlangach, keyingi hatti-harakat quyidagicha bo'ladi: kompyuterni o'chiring va uni himoyalangan sistemali disket yordamida qayta yuklang (bunday disketa Sizda albatta bo'lishi kerak). Mazkur disketada antivirus dasturlari joylashgan bo'lishi kerak. Antivirus dasturini ishga tushiring. Zararlangan operasion sistemalarda amallarni bajarish va dasturlarni ishga tushirish qo'pol xato va misli ko'rilmagan yo'qotishlarga sabab bo'ladi. Jumladan, bunda hali zararlanmagan dasturlar ham talofat ko'rishi mumkin. Masalan, Sizning kompyuteringiz RCE-1800 virusi bilan zararlangan bo'lsin. Mazkur virusga mo'ljallanmagan faga dasturni extiyotsizlik bilan ishlatish qolgan yuklovchi modullarni ham ishdan chiqaradi.

Yana ko'p uchraydigan xatolardan biri antivirus vositalarini haddan tashqari ishonish. Garchand, bunday dasturlarni juda yuqori darajadagi dasturchilar yaratsalar-da, ular har doim ham ishonchli emas. Har qanday dastur kabi, ular ham xatolardan holi emas. Bu detektorlarga ham, fagalarga ham taaluqli. Shu yerda biz ta'kidlashimiz lozimki, biz faga deb atalayotgan dasturlar aslida "detektor-faga"ning o'zi. Shuning uchun ularning ishida viruslarni aniqlashda ham, ularni davolashda ham xatolar bo'lishi mumkin.

Ishlatilayotgan detektorlar ko'pincha viruslarni payqamay, zararlangan fayllarni o'tkazib yuboradilar. Masalan, juda mashhur McAfee Associates firmasiga tegishli SCAN kompleks detektori bizning mamlakatimizda keng tarqalgan viruslarni payqamay o'tkazib yuboradi va yangi, bir nechta yolg'on ishlanmalar beradi. Shuning uchun bir nechta detektorlarni bir yo'la qo'llash "ovoz berish yo'li bilan" zararli dasturlarning ro'yxatini tuzish mumkin.

Arxivda saqlanayotgan dasturlarga detektorlarni qo'llash samarasiz ekanligini ta'kidlash lozim. Bunda dasturlarni arxivdan ozod etish lozim. Aks holda, detektor mazkur fayllarni tekshirmaydi. Yana faga noo'rin dasturning foydali qismini "tishlashi mumkin". Aynan shu yerda detektor yolg'on axborot bergan bo'ladi. Faga ishlab turgan dasturni ishdan chiqarishi hech gap emas. Yana bir eng katta, yo'l qo'yiladigan xatolardan biri himoyalangan disketaning qo'lma-qo'l yurishi va ishonchsiz disketalarni yuklashdir. Shuning uchun disketalarni doimo himoyalash kerak. Faqat ishonchli disketalardangina foydalanish darkor. Va yana bir yo'l qo'yiladigan xatoga maxsus to'xtalamiz. Bu A disk yuritgichda disketa bo'la turib, kompyuterni qayta yuklashdir. Bunda BIOC aynan disk yuritgichdagi disketadan dasturni yuklaydi, natijada disketadagi boot-virus vinchesterga yuqadi.

Faganing sifati, eng avvalo, u qayta ishlayotgan viruslar soniga bog'liq. Bundan tashqari, interfeys qulayligi ham muhim ahamiyat kasb etadi. Bular faganing hisobotini yaxshilaydi. Odatda, fagalar bir necha viruslarga mo'ljallangan bo'lib, qolganlari uchun samarasiz bo'lishi mumkin.

Virusdan himoyalanish usullarini qo'llash

"Virus-himoya vositalari" muammosi xuddi "hujum quroli - himoya quroli" muammosiga o'xshaydi. Himoya vositalari ko'paygan sari hujum vositalari ham takomillashib, uni ishlatuvchilar rag'batlantirilmokda. Nachora, hayot shunday kurashdan iborat. Shuning uchun aytish darkorki, kompyuter viruslari hali ko'p vaqt dolzarb muammo bo'lib qolaveradi, har ikki tomon ham rivojlana beradi.

Himoyalanishning asosiy texnologik sxemasi. Himoyalanishning bunday sxemasi quyidagi bosqichlardan iborat: - yangi dasturiy mahsulotning dastlabki nazorati; - qattiq diskni bir necha mantiqiy disklarga ajratish; - rezident revizor (taftishchi) dasturlar bilan davriy ravishda axborot butligini tekshirib turish - arxivlashtirish. Yangi kiritilayotgan dasturiy ta'minotni nazorat qilish: Birinchi va juda zarur himoya kiritilayotgan dastur va disketalarni nazorat qilishdir. Go'yoki, samolyotning muvaffaqiyatli parvoz qilishi uchun passajirlar batafsil tekshirilganidek, kompyuterda kiruvchi axborotlarni batafsil tekshirish viruslar yuqishining oldini oladi. Har qanday "firma" disketalariga ham ishonaverish kerak emas.

Ularda ham virus bo'lishi mumkin.

Ko'pchilik mashhur fayl va boot-viruslar mavjudligini kirish nazoratining o'zidayoq aniqlash mumkin. Bu jarayon bor-yo'g'i bir necha daqiqani oladi, xolos. Aks holda ko'p vaqt axborotlarni viruslardan tozalashga ketib qoladi. Kirish nazoratini bir nechta marta saralab, maxsus tanlab olingan detektor va fagalardan o'tkazgan ma'qul. Biz quyidagilarni tavsiya etamiz. SCAN, AIDSTEST, DOCTOR, AV, TP48CLS. Fagalarni detektor rejimida ishlatish zarur.

Karantin rejimi: Agar dasturiy ta'minot "begona qo'ldan" olingan yoki yot tashkilotlardan kelgan bo'lsa, mazkur dasturlarni ishlatishda "karantin muddati"ni belgilash foydali. Bunda har bir dastur uchun qat'iy sinov muddatini joriy etish zarur. Bu muddat oy, haftaning kunlari bo'lishi mumkin.

Nega? Chunki, biz yuqorida ayganimizdek, ba'zi bir viruslar ma'lum oy yoki aynan oying bir kunida o'z "hunarini" ko'rsatadi. Zararlangan dasturlardan tashqari, ba'zida "singan" himoyadagi dasturlar ham xavf tug'diradi (ular ko'proq ofis va o'yin dasturlarida uchraydi). Gap shundaki, dasturning himoyasini olish viruslar faoliyatini kuchaytirib yuboradi. Ayniqsa, "troya" viruslari faollashadi.

Masalan, Ukrainaning Donesk shahrida noqonuniy nusxalangan Formula o'yinlari davriy ravishda SMOS-xotirani o'chirib tashladi.

Qattiq diskni tekshirish

Kompyuterni harid qilgach, uning vinchesterida nima borligini tekshirish darkor. Endigina sotib olingan kompyuter vinchesteridagi barcha dasturlariga xuddi yangidek qarash kerak. Shuning uchun, yangi olingan mashina vinchesterini testdan o'tkazing, shuningdek, hamma disketalarni virusdan detektor-dasturlar bilan tekshiring. Vinchesterni testdan

o'tkazish chog'ida, albatta, yozuvdan saqlangan, toza sistema disketalari yordamida yuklanadi.

Himoyalashning o'ziga xos usullari: Disketaning normal holati - uning yozuvdan himoyalangan holatidir. Himoya faqat axborotni yozish chog'ida olinishi kerak. Faqat yozishdan himoyalangan disketalarni ishlatib, antivirus dasturlari, sistemali disketalarni ko'ngil to'q bo'lishi uchun ehtiyot qilib saqlash joiz. Axborotlarni tiklash: Shuni ta'kidlash kerakki, "zaralangan" axborotlarni eng qiyin vaziyatlarda ham tiklash mumkin. Biroq viruslar "zararlagan" fayllarni tiklash sistema dasturchilaridan yuksak mahorat talab etadi. Ko'pincha qutqarish mumkin bo'lgan fayl yoki ma'lumotlar sistemali bloklarni formatlash jarayonida shikast yeydi, bunda axborotning yo'qolib ketish ehtimoli ham bor. Yu qorida aytganimizdek, dasturni saqlashning eng yaxshi yo'li - uni arxivlab qo'yish. Lekin shunday bo'lsa ham har ish kuni so'ngida dastur va fayllarning joylashishini birma-bir ko'zdan kechirish darkor.

FOYDALANGAN ADABIYOTLAR:

1. O.Abduraxmonov "Development of a structure for implementation of parallel algorithms based on cubic splines in a multiple nuclear processor" International Journal of Engineering and Information Systems //Vol. 5, Issue 5., Pages: 63-66, 2021 y.
2. O.Abduraxmonov "Ko'p yadroli protsessorda kubik bazisli splaynlar asosida parallel algoritmlarni amalga oshirish tuzilmasini ishlab chiqish" Academic Research In Educational Sciences Scientific Journal // Vol.2, Issue 3., Pages: 628-633, 2021 y.
3. O.Abduraxmonov "Some methods of signals digital operation" International journal for advanced research in science & technology // Vol.10, Issue 06., Pages: 1-4, 2020 y. Abduraxmonov Odiljon Qobulovich: Pandemiya sharoitida "Axborot-kommunikatsion texnologiyalari" dan foydalanib, elektron ta'lim shakliga o'tishning o'ziga xos xususiyatlari. "International scientific-online conference on innovation in the modern education system. Washington University in St. Louis
4. Usmanova Mavluda Soyibjon qizi, Karimov Otabek Raximovich, Mamatov Shohruxbek Muhammadjon o'g'li "OLIIY TA'LIMDA RAQAMLI TEXNOLOGIYARDAN FOYDALANISHNING ILMIY METODIK ASOSLARI" "XALQ TA'LIMI XODIMLARINI "UZLUKSIZ KASBIY RIVOJLANTIRISH"GA MOSLASHISH JARAYONINING IJTIMOIIY-PEDAGOGIK MUAMMOLARI" MAVZUSIDAGI ILMIY AMALIY ANJUMANI 2022-yil 31-oktyabr.
5. Usmonova Mavludaxon Soyibjon qizi "TA'LIM MUASSASALARIDA ELEKTRON O'QUV ADABIYOTLARIDAN FOYDALANISH" INTEGRATSIYALASHGAN TA'LIM VA TADQIQOTLAR JURNALI JOURNAL OF INTEGRATED EDUCATION AND RESEARCH MAY 2023
6. Усмонова Мавлудахон Сойибжон қизи, Каримов Отабек Рахимович, Маматов Шохрухбек Муҳаммаджон ўғли "ИҚТИСОДИЁТДА РАҚАМЛИ ТЕХНОЛОГИЯЛАРДАН ФОЙДАЛАНИШ" «Zamonaviy dunyoda innovatsion tadqiqotlar: Nazariya va amaliyot» nomli ilmiy, masofaviy, onlayn konferensiya 2022

7. Usmonova Mavludahon Soyibjon qizi “Library of Programming Languages Python"Easy Delivery Methods Using Modern Information Communication Tools” European Journal of Pedagogical Initiatives and Educational Practices ISSN (E): 2938-3625 Volume 1, Issue 1, April, 2023

8. Usmonova Mavludakhon “Operating Principles and Applications of Blockchain Technology” European Journal of Pedagogical Initiatives and Educational Practices ISSN (E): 2938-3625 Volume 1, Issue 9, December, 2023