O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
URGANCH FILIALI

MAVZU:KOMPYUTERNI VIRUSLARIDAN SAQLASH

Urganch 2015

Reja

1. **Kompyuter viruslaridan himoyalash**
2. **Kompyuter virusi qanday namoyon bo`ladi**
3. **Viruslardan himoyalanishning asosiy vositalari**
4. **Viruslar bilan kurashuvchi ba'zi programmalar (antiviruslar)**
5. **Windows lar uchun Doctor Web**

Kompyuter viruslaridan himoyalash. Kompyuter virusi nima?

Kompyuter virusi - bu maxsus yozilgan programma bo`lib, u boshqa programmalarga qo`shilishi (ya'ni uni zaharlashi) mumkin, shuningdek kompyuterda noma'qul harakatlarni amalga oshirishi mumkin. Ichida virus bo`lgan programma «zararlangan» deyiladi. Bunday programma ishni boshlaganda boshqaruvni avvalo virus amalga oshiradi. Virus boshqa programmalarni topadi va zararlaydi, shuningdek qandaydir buzg`unchi harakatlarni bajaradi (masalan, diskdagi fayllarni va shu fayllar joylashgan jadvalni ishdan chiqaradi (buzadi), operativ xotirani bo`lar-bo`lmas «axlat» bilan to`ldiradi va h.z.). Virus o`zini yashirish maqsadida programmani zararlantirish harakatlari har doim ham bajarilavermaydi. Ular faqat muayyan sharoitda amalga oshadi. Virus kerakli harakatlarni bajarib bo`lgandan so`ng, u boshqaruvni o`sha programmaga beradi (virus shu programmaning ichida yotadi) va u oldingidek ishlayveradi. Shu bilan bir qatorda virus bilan zararlangan programma xuddi viruslanmagan programma kabi faoliyat ko`rsatadi.

Mavjud bo`lgan viruslarning ko`pchiligi yadro sistemali fayllarni afzal ko`radilar, chunki ko`p zamonaviy kompyuterlarda fayllar sistemasi bir xil nomlanadi. Masalan, viruslar aksariyat hollarda, Command.com fayliga birlashadi va Dir komandasi bilan boshqa disk va direktoriyalarga tarqaladi. Ko`p hollarda sistemaning zararlanishi kiritish-chiqarish jarayoniga murojaat qilganda ro`y beradi.

Aslini olganda, viruslar sistemalarga birikib ketish uchun har qanday yo`llarni ishlatishadi, shuning uchun ham zararlanmaydigan sistemalar yo`qdir.

Personal kompyuterlarga viruslar kirib ketishining asosiy yo`li bo`lib zararlangan disketalar xizmat qiladi. Viruslar borgan sayin beshafqat va hech narsadan qo`rqmaydigan bo`lib borayapti, hatto eng yetuk viruslarga qarshi programmalar ham ular bilan kurashishga ba'zan ojizlik qilayaptilar. Shunday viruslar mavjudki, ular energiyaga bog`liq bo`lmagan xotiraga yashirinib olib, sistemani tozalashda juda katta qiyinchiliklar tug`diradilar. Hatto haqiqiy firma belgisiga ega bo`lgan, siqilgan dastur ham virusdan holi ekanligiga hech kim kafillik bera olmaydi. Viruslarni CD-ROM disklarning shtampovka jarayonida ham o`rnashganlik hollari mavjuddir.

Virus asosan 4 ta fazaga ega:

- uxlash fazasi;
- ko`payish fazasi;
- ishga kirishish fazasi;
- vayron qilish fazasi.

Virus ixtirochisi asta-sekinlik bilan foydalanuvchining ishonchini qozonish maqsadida, uxlash fazasini ishlatishi mumkin, chunki bunda virus ko`paymaydi va ma'lumotlarni buzmaydi. Ko`payish fazasida programmaning ishga tushishi bilan u namoyon bo`la boshlaydi. Ishga kirish fazasi virus programmadagi belgilangan vaqt, oy, yil yoki nusxa ko`chirishning belgilangan sonlaridan keyin

ro`y beradigan voqelik bilan bog`liqdir. Va nihoyat, vayron qilish fazasida ommaviy zararlash amalga oshiriladi.

Ko`payish jarayonida viruslar o`zlarining xayoliy nusxalarini boshqa programmalarga uzatadi yoki diskning ma'lum sohalariga joylashib oladi. So`ngra asl virusning o`zi bo`lib qoladi va ko`payish jarayonini davom ettiradilar, ya'ni yangi virtual nusxalarni ko`chiradilar.

Viruslarning ko`p turlari shunday yaratilganki, ular zararlangan programmani ishlatganda rezident bo`lib qolaveradi, ya'ni DOSni yuklashdan oldin kompyuter xotirasida vaqti-vaqti bilan boshqa programmalarni zararlab boradilar va noma'qul harakatlarni amalga oshiradilar.

Viruslarning harakati juda tez amalga oshadi, hamda hech qanday xabar bermaydi. Shu sababli, foydalanuvchi kompyuterdagi noxush o`zgarishlarni o`zi sezishi lozim.

Virus programmalarni yozish unchalik qiyin ish emas, bu programmalarni o`rganayotgan talaba ham uddalay oladigan vazifadir, shuning uchun dunyoda kundan-kunga turli xil yangi viruslar yaratilmoqda.

Kompyuter virusi qanday namoyon bo`ladi

Kompyuter zararlanganda, bir qancha Qaroyib hodisalar yuz beradi:

- ba'zi bir programmalar ishlamaydi yoki yomon ishlay boshlaydi;
- ekranga boshqa xabarlar yoki simvollar chiqa boshlaydi;
- kompyuter ishlashi sekinlashadi;
- ba'zi bir fayllar buziladi yoki ularning hajmi ortiqcha har xil yozuvlarni qo`shish hisobiga o`zgaradi, kattalashadi;
- operativ xotiraning bo`sh joyi qisqaradi;
- sistemali disketadan programmalarni yuklash qiyinlashadi yoki umuman yuklanmaydi va h.k.

Shuni ta'kidlash kerakki, programmalar va hujjatlar matnlari, berilganlar bazasining axborot fayllari, jadvallar va boshqa shunga o`xshash fayllar zararlanmaydi. Ular faqat buzilishi mumkin.

Virus bilan quyidagi turdagi fayllar zararlanishi mumkin:

- Bajariluvchi fayllar: **COM** va **EXE** ko`rinishidagi fayllar. Fayllarni zararlaydigan viruslar **fayl viruslari** deyiladi. Bajariluvchi fayllaridagi viruslar shu fayl tegishli bo`lgan programma ishlaganda o`z faoliyatini boshlaydi;

- Operatsion sistemaning yuklovchisi va qattiq diskning asosiy yuklovchisi yozuvlaridan iborat fayllar. Bu sohalarni zararlaydigan viruslar **yuklovchi** yoki **but viruslari** deyiladi. Bunday viruslar kompyuter yuklanishi bilan ishlay boshlaydi va u rezidentlik holatiga o`tadi, ya'ni doim kompyuter xotirasida saqlanadi. Tarqalish mexanizmi - kompyuterga qo`yiladigan disketalarning yuklovchi yozuvlarining zararlanishi. Bularda joylashgan viruslar shu qurilmalar, qurilmalar drayverlari, ya'ni har xil qurilmalar ishini ta'minlovchi programmalarga murojaat qila boshlaganda ishga tushadi.

**Diskdagi fayl sistemani o`zgartiradigan viruslar**Odatda bunday viruslar **DIR** deb ataladi. Bu viruslar diskning biror-bir sohasida fayllarning oxiri sifatida yashirinadilar. Ular ko`rsatgichlar boshini yozuv oxiriga olib o`tib

qo`yadi va **NDD** (Norton Disk Doctor) bilan tekshirganda diskning buzilganligi ma'lum bo`ladi.

Ko`rinmas va o`zi differensiallanuvchi viruslar Ko`p viruslar o`zini sezdirmaslik uchun sistemada DOS ga murojaat qila boshlaganda fayllarni xuddi oldingi holatidek ishlashini ta'minlaydilar. Ko`rinmas viruslar shunday tarzda harakat qiladi.

O`zi differensiallanuvchi viruslar esa, o`zini formasini takomil-lashtiradi. Ko`p viruclar boshqalar uning ishlash mexanizmini sezib qol-masliklari uchun o`zining katta qismini kodlangan holda saqlaydi. Bu albatta bunday viruslarni topishda qiyinchiliklar tug`diradi.

BOOT -viruslar Ba'zida disketadan hech narsa ko`chirmasdan ham, undan qandaydir programmani yuklamay turib virus bilan zararlanish mumkin. Masalan, **STONE** yoki **MARS** kabi viruslar mavjudki, ular kompyuterni yoqishingiz bilan yoki qayta yuklanganingizda, ichida disketa qolib ketgan bo`lsa, zarar yetkazishi aniq. Bunday viruslar **BOOT** - viruslar deyiladi. **BOOT** Sector-yuklanuvchi soha degan so`zdan kelib chiqqan. Kompyuter yoqilishi bilan disketa orqali yuklanishga harakat qiladi, agar kompyuterda yuklanish disketasi bo`lmasa, buning uddasidan chiqa olmaydi. Lekin disketa qanday bo`lishidan qat'i nazar, **BOOT** viruslar kompyuterni bemalol zararlaydi, shuning uchun ehtiyotkorlik talab qilinadi.

Viruslardan himoyalanishning asosiy vositalari

Eng yaxshi himoya turi - viruslarni qay tarzda ta'sir etishini bilishdir. Viruslar oddiy programmalar bo`lib, biror g`aroyib kuchga ega emaslar.

Kompyuter viruslar bilan zararlanishi uchun undagi biror-bir zararlangan programma ishlashni talab qilinadi. Shuning uchun kompyuterning birlamchi zararlanishi quyidagi hollarda ro`y beradi:

- kompyuterdagi virus bilan zararlangan programmalar yuklanishi (**COM, BAT** yoki **EXE** fayllar) yoki moduli zararlangan programmaning ishlatilishi;
- kompyuterga virusli disketning yuklanishi;
- kompyuterga zararlangan OS yoki qurilmalarning zararlangan drayverlarining o`rnatilishi.

Viruslardan quyidagi usullar bilan himoyalanish mumkin:

- o`qilayotganda disketani, albatta, virus borligiga tekshirish;
- axborot nusxalarini ko`chirish, shuningdek disklar va axborotni saqlash uchun ishlatiladigan umumiy qoidalardan foydalanish, disklarni jismoniy zararlanishdan, programmalarni esa buzilishdan saqlash;
- axborotdan noqonuniy foydalanishni cheklash, xususan, programma va ma'lumotlarning viruslar ta'sirida o`zgarishidan, noto`g`ri ishlayotgan programmalar va foydalanuvchilarning noto`g`ri harakatlaridan himoya qilish;
- viruslar bilan zararlanish ehtimolini kamaytiruvchi chora-tadbirlar;
- viruslar bilan kurashuvchi maxsus programmalardan foydalanish.

Viruslar bilan kurashuvchi ba'zi programmalar (antiviruslar)

Antiviruslarni quyidagicha guruhlash mumkin:

- **detektor** va **doktor**-viruslar bilan zararlangan fayllar va zararlantiruvchi virus turini aniqlaydigan programmalar (**Aids, doktor Web, Virus Scan, NU VS**). Bu turdagi antiviruslar fayllarda viruslarning bayt kombinatsiyalari mavjudligini tekshirib, mos bo`lgan axborotni ekranga chiqarib beradi. Ba'zi detektor programmalar viruslarning yangi turlariga moslasha oladi, buning uchun shu viruslarga mos bo`lgan baytlar kombinatsiyasini belgilab berish kerak. Doktorning vazifasi zararlangan fayllar va disk sohalarini tekshirib, ularni dastlabki holatiga qaytarishdir. Tiklanmagan fayllar, odatda, ishlatib bo`lmaydigan holga tushadi yoki yo`q qilib yuboriladi.

- **vaksina** programmalar yoki **immunizatorlar** disk yoki programmalarni shunday o`zgartiradiki, bu narsa programmalarning ishida namoyon bo`lmaydi, lekin vaksinatsiya ishlatilganda virus programma va disklarni zararlagan deb hisoblaydi.

Windows lar uchun Doctor Web

Bu programma 32 bitli Windows turkumidagi operatsion sistemalar uchun mo`ljallangan bo`lib, qisqacha **DrWeb32W** deb ataladi.

DrWeb32W funksional jihatdan DOS ning **DrWeb** antivirusiga o`xshash. Lekin **DrWeb** ning 4.0 versiyasidan boshlab antivirus programma ishlashining arxitekturasi va algoritmiga sezilarli o`zgartirishlar kiritilgan. Bu esa o`z navbatida yangi antiviruslar yaratilishiga asos bo`ldi. **DrWeb 4.0** antivirusining asosiy yangiligi modul prinsiplarining qo`llanilganidir, ya'ni viruslar bazasi alohida faylda tashkil etilgan bo`lib, u asosiy programma ishga tushgandan so`ng qo`shimcha fayl sifatida yuklanadi. Natijada operativ xotira yetishmovchiligining oldi olinadi. **DrWeb32** antivirus programmasida programma biror muhitda (masalan, Windows 95/98/NT) ishlaydigan qobiq programma va muhitga bog`liq bo`lmagan yadrodan tashkil topadi. Programmalarni bunday tashkil etish quyidagi afzalliklarga ega:

- bitta virus bazasining faylidan DOS ning **DrWeb** programmasi uchun ham, Windows 95/98/NT, OS/2, Novell Netware uchun ham foydalanish mumkin;
- programmaning yadrosini boshqa qobiq programmalar va amaliy dasturlarga ulash mumkin;
- qobiq programmalar, yadrolar va virus bazalarini **Internet** tarmog`i orqali avtomatik kengaytirish hamda yangilash imkonini beradi.

DrWeb32 ning yana boshqa yangiliklaridan biri uning test qilinadigan obyektlarni ixtiyoriy diskdagi kataloglar ro`yxatidan (hatto alohida fayllarni ham) tanlash imkoniyatining mavjudligidir.

DrWeb32 antivirus programmasini ishga tushirganda (Windows ning ish stolidan, **PUSK** menysining

Quyida asboblar panelining, meny bo`limlari va bandlarining asosiy funksiyalari berilgan.

Asboblar paneli va funksiyalari

Zararlangan fayllar ro`yxatini chiqarish holatiga o`tish.

Tekshiriladigan sohani tanlovchi daraxt holatiga o`tish.

Virusga tekshirish natijalarining ma'lumotlarini chiqarish.
Zararlangan fayllar haqidagi ma'lumotlarni saqlovchi ro`yxatni tozalash.
DrWeb bazasini **Internet** orqali to`ldirish.
Antivirus programmaning ishlash parametrlarini o`rnatish.
Chiqish (ishni tugallash).

File (Fayl) menysi

-Davolashni boshlash
-Ishni to`xtatish
-ro`yxatni tozalash
-bazani to`ldirish
-ishni tugallash

View (Ko`rish) menysi

- zararlangan fayllar ro`yxati
- obyektni tanlash
-statistika

Options (Opsiya) menysi

- holat parametrlarini o`zgartirish
- holat parametrlarini saqlash
- holat parametrlarini tiklash

Help (Yordam) menysi

- mavzular bo`yicha yordam
- programma haqida ma'lumot