KOMPYUTER VIRUSLARI VA ANTIVIRUS DASTURLARI HAQIDA MA'LUMOT

Suleymenova Rushana Asomidinovna.

Annotatsiya: Ushbu maqola informatika va axborat texnologiyalari fanidan.Kompyuter viruslari va antiviruslar dasturlari haqida tushuncha. Kompyuter viruslari bugungi kunda ko'pchilikning eng dolzarb muammosidir Bu hammani tashvishga solmoqda

Kompyuter viruslari. Kompyuter viruslarini sinflarga ajratish

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 nomlisidir. 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) cektoriga zarar yetkazuvchi viruslar ham mavjud.

Kompyuter viruslaridan himoyalanish usullarini sinflashtirish

1. Kompyuter viruslaridan himoyalanish usullarini sinflashtirish.

Dastlabki nazorat:

Kelayotgan dasturlarni detektor dasturlari bilan tekshirish.

Profilaktika:

"Yozishdan himoyalangan" disketalar bilan ishlash, yozish uchun disketadan foydalanishni minimallashtirish, ilgarigi va amaldagi disketalarni alohida saqlash, dasturlarni vinchesterda arxivlangan holda saqlash.

Taftish (Reviziya):

Yangi dasturlarni maxsus dasturlar yordamida tekshirish.

Karantin:

Har qanday yangi dastur yangi karantin muddatini o'tashi lozim. Ular mutaxassislar tomonidan viruslarga tekshirilgan bo'lishi kerak.

Filtrlashtirish:

FluSbot Plus, MaceVaccine, ANTIWS2 turdagi dasturlar orqali ehtimoldagi viruslarni tutish.

Terapiya: (davolash).

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 himoyalanishning 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, koplab 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 himoyalanmagan 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 oyning 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.

Yuqorida 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.

Antivirus dasturlari

Kompyuterdagi ma'lumotlar va dasturlar ma'lum virus dasturi tomonidan o'chirilib yuborilishi yoki shikastlanishi mumkin. Virus-dasturlari dasturchilar tomonidan tajriba uchun yoki yomon niyatlarda yaratilib, asosan ular quyidagi vositalar orqali Sizning kompyuteringizga kirishi mumkin:

- noma'lum disketadagi ma'lumotlarni o'qish natijasida (hujjat, o'yin va boshqalar);
- internet tarmog'idan ba'zi xil dasturlarni yuklash natijasida;
- elektron-pochta orqali;
- lokal tarmoq orqali;
- noqonuniy ko'chirilgan va tarqatilayotgan dasturlardan foydalanish oqibatida;

Virus dasturlari asosan Assembler dasturlash tilida tuziladi va ular salbiy ta'siri bo'yicha bir nechta guruhga bo'linadi:

1. Sodda viruslar - operativ xotirani band qilib, kompyuterning ishlashi sekinlashtiradi.
2. Maxsus "stels" viruslari, ular joylashishini o'zgartirib turadi va ularni topish ancha murakkab.
3. Ma'lumotlarga o'zgartirish kiritadigan viruslar.
4. Ma'lumotlarni o'chiradigan viruslar.
5. Foydalanuvchining ayrim bir (mahfiy) ma'lumotlarini Internet tarmog'i orqali virusni yaratgan shaxsga yuboradigan viruslar.

Kompyuterdagi ma'lumotlarni viruslardan himoya etish uchun antivirus dasturlar ishlab chiqarilgan.

Antivirus dasturlar AQSh, Kanada, Rossiyaning bir qator firmalari tomonidan ishlab chiqarilmokda.

Antivirus dasturlar rezident va norezident turlarga bo'linadi: rezident antivirus dasturi kompyuter yoqilganidan o'chirilguncha qadar operativ xotira, aktiv (joriy) dasturlarni, fayllarni virusga tekshirib turadi. Rezident antivirus dasturi o'zining ishini foydalanuvchiga bildirmasdan olib boradi, faqat ayrim hollarda foydalanuvchidan virusi mavjud faylni davolashga ruxsat so'raydi. Norezident antivirus dasturlar esa faqat foydalanuvchining o'zi ko'rsatgan joylarni va belgilangan vaqtda tekshiradi va davolaydi. Hozirgi kunda quyidagi antivirus dasturlar keng tarqalgan:

1. DrWeb for DOS;
2. DrWeb for Windows;
3. Antiviral Tool Kit Pro;
4. AVP Platinium;

5. Norton Antivirus;

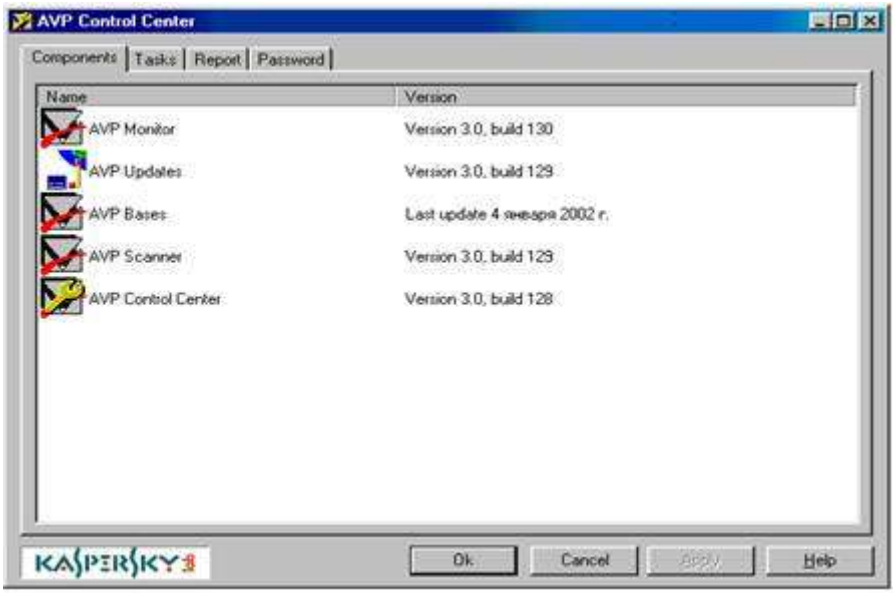
6. McAfee;

7. Aidstest;

Doctor Web, AVP, Aidstest antivirus dasturlari Rossiyaning "Kasperskiy" laboratoriyasi tomonidan ishlab chiqarilgan va u MDH davlatlarida ko'p uchraydigan viruslardan xabari bor. Norton Antivirus mashhur Symantec firmasi tomonidan ishlab chiqarilgan bo'lib, u topa oladigan viruslar soni 100000 dan ortiq. AVP dasturi virusdan himoyalaydigan eng ishonchli antivirus dasturi hisoblanadi. DrWeb dasturining rezident tekshiruv dasturi Spider - Windows rejimida tekshiruvni olib boradi. Bitta kompyuterda bir nechta turdagi antivirus dasturlar o'rnatmagan ma'qul, chunki ularning virusni topish usullari (algoritmlari) har xil hamda ular ham ?zlarini viruslar kabi tutadilar va bu holda ular o'zaro "kelisha olmay qolishlari" mumkin.

AVP antivirus dasturlar majmuasi (kompleksi)

Antiviruslar ham dastur bo'lib, virus tomonidan shikastlanishi mumkin. Buning oldini olish uchun antivirus dasturi himoyaga ega bo'ladi, ya'ni unda maxsus alohida modul bo'lib, u antivirusni viruslardan himoyalashga qaratilgan bo'ladi.



Amerika Qo'shma Shtatlarida antivirus dasturlaridan Symentec kompaniyasining Norton Antivirus va Network Associates kompaniyasinig McAfee dasturlari keng tarqalgan.

Rossiya, O'zbekistonda yuqorida ko'rsatilgan antivirus dasturlar bilan birgalikda Rossiya Federasiyasida ishlab chiqarilgan Doctor Web va AVP antivirus dasturlar kompleksi qo'llaniladi.

2005 yilning yakuni bo'yicha Kasperskiy laboratoriyasining AVP antivirus kompleksi eng yaxshi dastur sifatida tan olingan. U modullardan iborat bo'lib, har bir modulni yangilash imkoni mavjud, ya'ni dasturni butunlay o'zgartirmasdan yangi versiyasiga almashtirish mumkin.

AVP kompleksi quyidagi modullardan tashkil topgan:

- AVP Control Center - AVP ning boshqarish markazi.
- AVP Scanner (AVP Skaner) - tashqi xotirani viruslardan tozalash uchun xizmat qiladi.
- AVP Monitor (AVP Monitor) - kompyuterga tarmoq orqali yoki boshqa usullar bilan kirib kelayotgan ma'lumotlardagi va birinchi navbatda kompyuterning tezkor xotirasidagi viruslarni topish uchun xizmat qiladi.
- AVP Updates (AVP yangilash) - dasturni yangi viruslarning namunalari bilan to'ldirish uchun xizmat qiladi.

AVP Control Center

AVP Control Center - boshqaruv moduli bo'lib antivirus kompleksining ishlash rejimlari, tekshiruv parametrlari, usullari, tekshiruvni boshlash vaqti, yangilash vaqtini belgilab beradi. Odatda, AVP kompleksi o'rnatilganidan keyin AVP boshqaruv paneli Windows bilan birgalikda ishga tushadi. Bu holda masalalar satrining o'ng burchagida uning belgisi paydo bo'ladi.

Uni ishga tushirish uchun Pusk/Programmi/AntiViral Toolkit Pro/AVP Control Center ni tanlash kerak. Natijada ekranda uning oynasi hosil bo'ladi.

AVP Control Center oynasi quyidagi bo'limlardan iborat:

- Components - antivirus kompleksiga kiruvchi modullar ro'yxati, versiyalari va oxirgi yangilanish sanasi

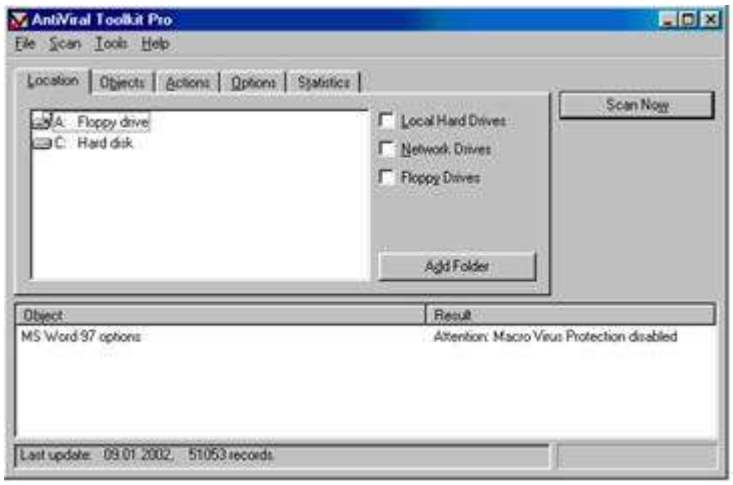
- Tasks - bajariladigan vazifalar ro'yxati;

- Report - hisobotlar bo'limi;

- Password - AVP Control Center dasturini yuklashga va chiqib ketishga parol o'rnatish. Kerakli o'zgartirishlar kiritilganidan keyin OK tugmasi chertiladi. O'zgartirishlarni bekor qilib chiqish uchun "Cancel" tugmasi bosiladi.

AVP Scanner moduli

Bu modul foydalanuvchi ko'rsatgan joylarni va ko'rsatilgan vaqtda tekshirish va zarurat tug'ilsa, davolash uchun mo'ljallangan, u avtomatik tarzda AVP Control Center tomonidan yoki foydalanuvchi tomonidan ishga tushishi mumkin. AVP Scanner modulini ishga tushirish uchun quyidagilarni bajarish kerak bo'ladi: "Pusk" / "Programmi"/ "AntiViral Toolkit Pro"/ AVP Scanner tanlanadi. Natijada ekranda quyidagi oyna hosil bo'ladi:



U yuklanish jarayonida operativ xotirani virusga tekshiradi va lozim b?lsa yangilanish kerakligini ta'kidlaydi. Uning oynasi quyidagi kismlardan iborat:

- Location - tekshiriladigan disk va katolog ko'rsatish;
- Objects - tekshiriladigan ob'ektlarni - fayllar turini ko'rsatish;
- Actions - virus topilganida bajariladigan amalni ko'rsatish;
- Options - tekshiruvni olib borish tartibi va parametrlarini ko'rsatish;
- Statstics - hisobot va statistika oynasi.

Location bo'limi

Local Hard Drives - kompyuterning qattiq disklari tekshirilishi kerakligini ko'rsatish;

Network Drives - tarmoq qattiq disklari tekshirilishi kerakligini ko'rsatish;

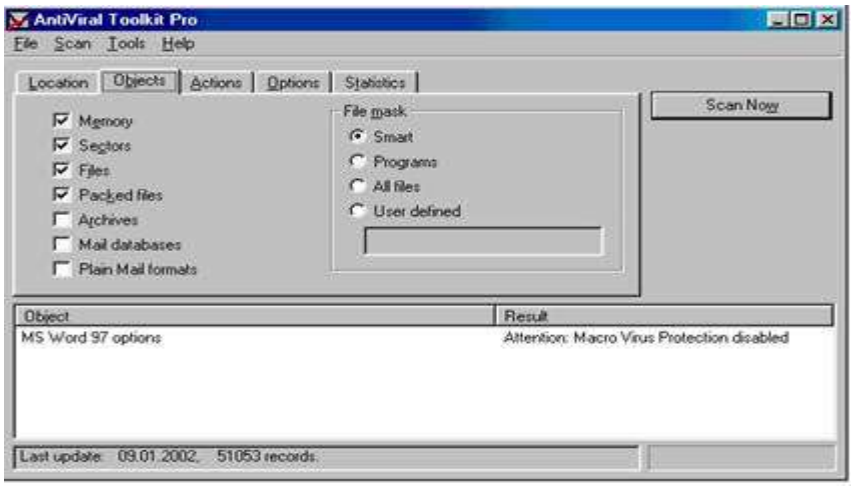
Floppy Drives - disketa tekshirilishi kerakligini ko'rsatish;

Add Folder - joriy katlogni tekshirish lozim bo'lgan kataloglarga qo'shish;

Scan Now - tekshiruvni boshlash;

Object - topilgan xato va virusli fayllarni ko'rsatish bo'limi.

Objects bo'limi



Memory - xotirani tekshirish;

Sectors - qattiq disk yoki disketaning yuklanish sektorini tekshirish;

Files - fayllarni tekshirish;

Packed Files - siqilgan fayllarni tekshirish;

Archives - arxiv fayllarini tekshirish;

Mail databases - elektron pochta fayllarini tekshirish

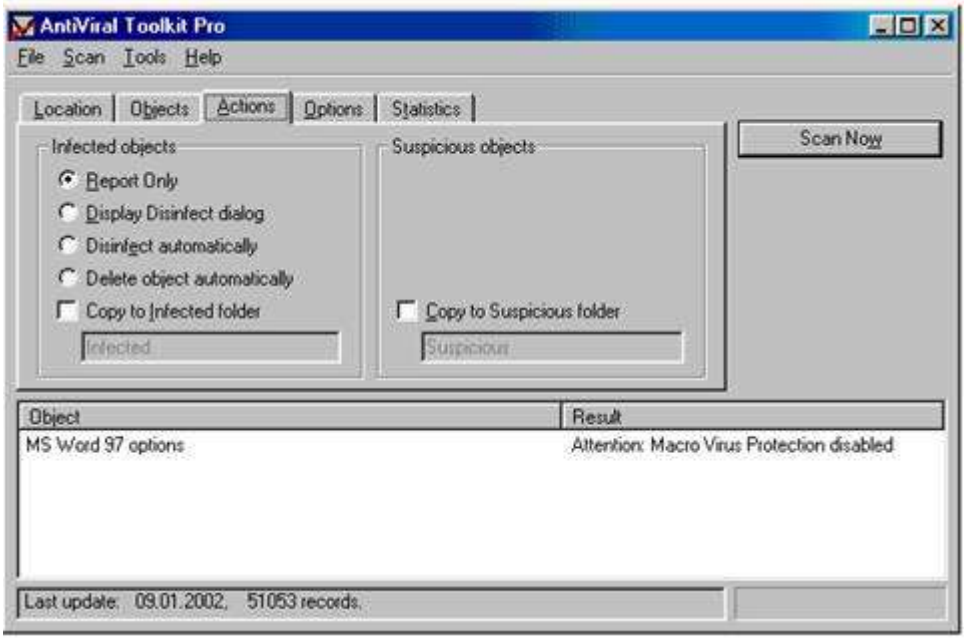
Smart - tekshiruvni yuzaki o'tkazish;

Programs - faqat dastur fayllarini tekshirish;

All files - barcha fayllarni tekshirish;

User defined - foydalanuvchi ko'rsatgan turdagi fayllarni tekshirish.

Actions bo'limi



Report Only - topilgan virus to'g'risida faqat hisobot berish.

Display Disinfect dialog - aniqlangan virus faylini davolash to'g'risida so'rov oynasini chiqarish;

Disinfect automatically - avtomatik tarzda davolash;

Delete object automatically - aniqlangan virusli fayllarni avtomatik tarzda o'chirish;

Copy to Infected Folder - topilgan virusli fayllarni ko'rsatilgan katalogga ko'chirish.

Хулоса

Kompyuter virusi 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. 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. Shuni ta'kidlash kerakki, eng qulay detektorlar bir emas, koplab 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.

Foydalanilgan saytlar

- www.google.co.uz
- www.ref.uz
- www.ziyo.uz