20-mavzu. Kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlari.

Kompyuter virusining ko‘p ta’riflari mavjud. Birinchi ta’rifni 1984-yili Fred Koen bergan: "Kompyuter virusi - boshqa dasturlarni, ularga o‘zini yoki o ‘zgartirilgan nusxasini kiritish orqali, ulami modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko‘payish qobiliyatini saqlaydi". Virusning o‘z-o‘zidan ko‘- payishi va hisoblash jarayonini modifikatsiyalash qobiliyati bu ta’- rifdagi tayanch tushunchalar hisoblanadi. Kompyuter virusining iishbu xususiyatlari tirik tabiat organizmlarida biologik viruslaming parazitlanishiga o ‘hshash.

Hozirda kompyuter virusi deganda quyidagi xususiyatlarga ega bo‘lgan dasturiy kod tushuniladi:

- asliga mos kelishi shart boim agan, ammo aslining xususiyatlariga (o‘z-o‘zini tiklash) ega b oigan nusxalarni yaratish qobiliyati;

- hisoblash tizim ining bajariluvchi obyektlariga yaratiluvchi nusxalaming kiritilishini ta’minlovchi mexanizmlaming mavjudligi.

Ta’kidlash lozim ki, bu xususiyatlar zaruriy, ammo yetarli emas. K o‘rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta’sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to id in sh lozim.

Viruslarni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

- yashash makoni;

- operatsion tizim;

- ishlash algoritmi xususiyati;

- destruktiv imkoniyatlari.

Kompyuter viruslarini yashash makoni, boshqacha aytganda, viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo‘yicha

turkumlash asosiy va keng tarqalgan turkumlash hisoblanadi (7.1- rasm).

7.1-rasm. Yashash makoni b o ‘yicha kompyuter viruslarining turkumlanishi.

F ayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko‘p tarqalgan viruslar xili), yoki fayl-yo‘ldoshlarni (kompanon viruslar) yaratadi yoki fay Hi tizimlarni (link-viruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o'zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (MasterBootRecord) bo‘lgan sektorga yozadi.

Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.

M akroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan, MicroSoft Word, MicroSoft Excel va h. kabi om m aviy muharrirlarning fayl-hujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o'zin i tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. B a'- zida tarmoq viruslarini "qurt" xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo‘yicha tarqaladi), IRCqurtlarga (chatlar, InternetR-elayChat) bo‘linadi.

Kompyuter viruslarining ko‘pgina kombinatsiyalangan xillari ham mavjud, masalan - tarmoqli makrovirus tahrirlanuvchi hujjatlarni zaxarlaydi hamda o'zin in g nusxalarini elektron pochta orqali tarqatadi. Boshqa bir misol sifatida fayl-yuklama viruslarini ko‘rsatish mumkinki, ular fayllarni hamda disklarning yuklanadigan sektorini zaharlaydi

Viruslarning hay of davri. Har qanday dasturdagidek, kompyuter viruslari hayot davrining ikkita asosiy bosqichini - saqlanish va bajarilish bosqichlarini ajratish mumkin.

Saqlanish bosqichi virusning diskda u kiritilgan obyekt bilan birgalikda shundaygina saqlanish davriga to‘g ‘ri keladi. Bu bosqichda virus virusga qarshi dastur ta’minotiga zaif bo‘ladi, chunki u faol emas va himoyalanish ucliun operatsion tizimni nazorat qila olmaydi.

Kompyuter viruslarining *bajarilish davri,* odatda, beshta bosqichni o‘z ichiga oladi:

1. Virusni xotiraga yuklash.

2. Qurbonni qidirish.

3. Topilgan qurbonni zaharlash.

4. Destruktiv funksiyalarni bajarish.

5. Boshqarishni virus dastur-eltuvchisiga o ‘tkazish.

Virusni xo tira g a y u k fttsh . Virusni-^cotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi obyekt bilan bir vaqtda amalga oshiriladi. M asalan, agar foydalanuvchi virus bo‘lgan dasturiy faylni ishga tushirsa, ravshanki, virus kodi ushbu fayl qismi sifatida xotiraga yuklanadi. Oddiy holda, virusni yuklash jarayonidiskdan operativ xotiraga nusxalash bo‘lib, so'ngra boshqarish virus badani kodiga uzatiladi. B u harakatlar operatsion tizim tomonidan

bajariladi, virusning o‘zi passiv holatda bo‘ladi. Murakkabroq vazifalarda virus boshqarishni olganidan so‘ng o‘zining ishlashi uchun q o ‘shimcha harakadami bajarishi muinkin. Bu bilan bog‘liq ikkita jih a tk o ‘riladi.

Birinchisi viruslarni aniqlash muolajasining maksimal murakkablashishi bilan bog‘liq. Saqlanish bosqichida ba'zi viruslar himoyalanishni ta’minlash maqsadida yetarlicha murakkab algoritmdan foydalanadi. Bunday murakkabiashishga virus asosiy qismini shifrlashni kiritish mumkin. Ammo faqat shifrlashni ishlatish chala chora hisoblanadi, chunki yuklamsh bosqichida rasshifrovkani ta’minlovch i virus qismi ochiq ko‘rinishda saqlanishi lozim. Bunday holatdan qutilish uchun viruslarni ishlab chiquvchilar rasshifrovka qiluvch i kodni "mutatsiyalash" mexanizmidan foydalanadi. Bu usulning m ohiyati shundan iboratki, obyektga virus nusxasi kiritilishida uning rasshifrovka qiluvchiga taalluqli qismi shunday modifikatsiyalanadiki, original bilan matnli farqlanish pay do boMadi, ammo ish natijasi o ‘zgarmaydi.

Kodni mutatsiyalash mexanizmidan foydalanuvchi viruslar *polin to rf viru slar* nomini oigan. Polimorf viruslar (polymorphic)-qiyin aniqlanadigan viruslar bo‘lib, signaturalarga ega emas, ya’ni tarkibida birorta ham kodining doimiy qismi yo'q. Polimorfízm faylli, yuklamali va makroviruslarda uchraydi

Stels-algoritmlardan foydalanilganda, viruslar c ‘zlarini tizimda to‘la yoki qisman bekitishlari mumkin. Stels-algoritmlaridan foydalanadigan viruslar - *stels-viruslar* (Stealth) deb yuritiladi Stels viruslar operatsion tizimning shikastlangan fay!larga murojaatini ushlab qolish y o ‘li bilan o'zini yashash makonidaligini yashiradi va operatsion tizimni axborotni shikastlanmagan qismiga yo‘naltiradi.

Ikkinchi jihat *rezidem viruslar* deb ataluvchi viruslar bilan b o g ‘liq. Virus va u kiritilgan obyekt operatsion tizim uchun bir butun. bo‘lganligi sababli, yuklanishdan so‘ng ular tabiiy, yagona adres malconida joylashadi. Obyekt ishi tugaganidan so'ng u operativ xotiradan bo‘shaladi. Bunda bir vaqtning o‘zida virus ham bo‘shalib saqlanishning passiv bosqichiga o‘tadi. Ammo, ba’zi viruslar xili xotirada saqlanish va virus eltuvchi ishi tugashidan so‘ng faol qolish qobiliyatiga ega. Bunday viruslar rezident nomini oigan. Rezident viruslar, odatda, faqat operatsion tizimga ruxsat etilgan imtiyozli

rejimlardan foydalanib, yashash makonini zaharlaydi va ma’lum sharoitlarda zararkunandalik vazifasini bajaradi. Rezident viruslar xotirada joylashadi va kompyuter o'chirilishigacha yoki operatsion tizim qayta yuklanishigacha faol holda boiadi.

Rezident bo 'Imagan viruslar faqat faollashgan vaqtlarida xotiraga tushib, zaharlash va zararkunandalik vazifalarini bajaradi. Keyin bu viruslar xotirani butunlay tark etib, yashash makonida qoladi.

Ta’kidlash lozimki, viruslarni rezident va rezident bo‘lmaganlarga ajratis’n faqat fayl viruslariga taalluqli. Yuklanuchi va makroviruslar rezident viruslarga tegishli.

Qurbonni qidirish. Qurbonni qidirish usuli bo‘yicha viruslar ikkita sinfga bo‘linadi. Birinchi sinfga operatsion tizim funksiyalaridan foydalanib, faol qidirishni amalga oshiruvchi viruslar kiradi. Ikkinchi sinfga qidirishning passiv mexanizmlarini amalga oshiruvchi, ya’ni dasturiy fayllarga tuzoq qo‘yuvchi viruslar taalluqli.

Topilgan qurbonni zahartaslu Oddiy holda zaharlash deganda, qurbon sifatida tanlangan obyektda virus kodining o ‘z-o‘zini nusxalashi tushuniladi.

Avval fayl viruslarining zaharlash xususiyatlarini ko‘raylik. Bunda ikkita sinf viruslari farqlanadi. Birinchi sinf viruslari o'zining kodini dasturiy faylga bevosita kiritmaydi, balki fayl nomini o'zgartirib, virus badani bo‘lgan yangi fay Ini yaratadi. Ikkinchi sinfga qurbon fayllariga bevosita kiruvchi viruslar taalluqli. Bu viruslar kiritilish joylari bilan xarakterlanadi. Quyidagi variantlar bo‘lishi mumkin:

1. Fayl boshiga kiritish. Ushbu usul MS-DOSning com-fayllari uchun eng qulay hisoblanadi, chunki ushbu formatda xizmatchi sarlavhalar ko'zda tutilgan.

2. Fayl oxiriga kiritish. Bu usul eng ko‘p tarqalgan bo'lib, viruslar kodiga boshqarishni uzatish dasturining birinchi komandasi *(com)* yoki fayl sarlavhasini *(exe)* modifikatsiyalash orqali ta’minlanadi.

3. F ayl o ‘rtasiga kiritish. Odatda, bu usuldan viruslar strukturasi oldindan ma’lum fayllarga (masalan, *Command.com* fayli) yoki tarkibida bir xil qiymatli bavtlar ketma-kethgi bo'lgan, uzunligi virus joylashishiga yetarli fayllarga tatbiqan foydalaniladi.

Yuklama viruslar uchun zaharlash bosqichining xususiyatlari ular kiritiluvchi obyektlar - qayishqoq va qattiq disklarning yuklanish sektorlarining sifati va qattiq diskning bosh yuklama yozuvi (MBR) orqali aniqlanadi. Asosiy muammo-ushbu obyekt oicham - larining chegaralanganligi. Shu sababli, viruslar o ‘zlarining qurbon

joyida sig'magan qismini diskda saqlashi hamda zaharlangan yuklovchi original kodini tashishi lozim.

Makroviruslar uchun zaharlash jarayoni tanlangan hujjat-qurbonda virus kodini saqlashdan iborat. Ba’zi axborotni ishlash dasurlari uchun buni amalga oshirish oson emas, chunki hujjat fayllari formatining makroprogrammalarni saqlashi ko'zda tutilmagan bo‘- lishi mumkin.

D estruktiv fu n ksiy a la rn i bajarish. Destruktiv imkoniyatlari bo‘yicha beziyon, xavfsiz, xavfli va juda xavfli viruslar farqlanadi.

Beziyon \irttslar - o‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi viruslar. Ular tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydi xolos.

Xavfsiz viruslar - tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq viruslar, bo‘sh xotirani kamavtirsa-da, dastur va ma’lumotlarga ziyon yetkazmaydi.

Xavfli viruslar - kompyuter ishlashida jiddiy nuqsonlarga sabab boiuvchi viru

Dinamik — (bir martalik) parol- bir marta ishlatilganidan so‘ng boshqa umuman ishlatilmaydigan parol. Amalda odatda doimiy parolga yoki tayanch iboraga asoslanuvchi muntazam o‘zgarib turuvchi qiymat ishlatiladi.

“So’rov-javob ” tizimi - taraflaming biri noyob va oldindan bilib bo‘1maydigan “so‘rov” qiymatini ikkinchi tarafga jo‘natish or- qali autentifikatsiyani boshlab beradi, ikkinchi taraf esa so‘rov va sir yordamida hisoblangan javobni jo‘natadi. Ikkala tarafga bitta sir ma’1um bo‘1gani sababli, birinchi taraf ikkinchi taraf javobini tekshirishi mumkin.

Sertifikatlar va raqamli imzolar - agar autentifikatsiya uchun sertifikatlar ishlatilsa, bu sertifıkatlarda raqamli imzoning ishlatilishi talab etiladi. Sertifıkatlar foydalanuvchi tashkilotining mas’ul shaxsi, sertifıkatlar serveri yoki tashqi ishonchli tashkilot tomonidan beriladi. Internet doirasida ochiq kalit sertifıkatlarini tarqatish uchun ochiq kalitlami boshqaruvchi qator tijorat infrastrukturalari PKI (Public Key Inf astrusture) paydo bo‘1di. Foydalanuvchilar turli daraja sertifikatlarini olishlari mumkin.

Autentifikatsiya jarayonlarini xavfsizlikning ta’minlanish dara- jasi bo‘yicha ham turkumlash mumkin. Ushbu yondashishga binoan autentifikatsiya jarayonlari quyidagi turlarga bo‘1inadi:

- parollar va raqamli sertifikatlardan foydalanuvchi autentif- ikatsiya;
- kriptografik usullar va vositalar asosidagi qat’iy autentifı- katsiya;
- nullik bilim bilan isbotlash xususiyatiga ega bo‘1gan autentifi- katsiya jarayonlari (protokollari);
- foydalanuvchilami biometrik autentifikatsiyasi.

Xavfsizlik nuqtayi nazaridan yuqorida keltirilganlaming har biri o‘ziga xos masalalami yechishga imkon beradi. Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi. Shu bilan bir qatorda ta’kid1ash lozimki, nullik bilim bilan isbotlash xususiyatiga ega bo‘1gan autentifikatsiyaga qiziqish amaliy xarak- terga nisbatan ko‘proq nazariy xarakterga ega. Balkim, yaqin kela- jakda ulardan axborot almashinuvini himoyalashda faol foyda- lanishlari mumkin.

Autentifikatsiya protokollariga bo‘1adigan asosiy hujumlar quyidagilar:

- *maskaraJ* (impersonation). Foydalanuvchi o‘zini boshqa shaxs deb ko‘rsatishga urinib, u shaxs tarafidan harakatlarning imkoniyatlariga va imtiyozlariga ega bo‘lishni mo‘lja11aydi;

- autentifikatsiya almashinuvi *tarafini almashtirib qo’yish* (interleaving attack). Niyati buzuq odam ushbu hujum mobaynida ikki taraf orasidagi autenfikatsion almashinish jarayonida tralikni modifikatsiyalash niyatida qatnashadi. Almashtirib qo‘yishning qu- yidagi xili mavjud: ikkita foydalanuvchi o‘rtasidagi autentifikatsiya muvaffaqiyatli o‘tib, ulanish o‘rnati1ganidan so‘ng buzg‘unclıi foy- dalanuvchilardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;

- *takroriy uz-atish* (replay attack). Foydalanuvchilaming biri tom.onidan autentifikatsiya ma’1umotlari takroran uzatiladi;
- *uzatishni qaytarfsh* (reflection attak). Oldingi hujum variant- laridan biri bo‘lib, hujum mobaynida niyati buzuq protokolning ush- bu sessiya doirasida ushlab qolingan axborotni orqaga qaytaradi.
- *majburiy kechikish* (forsed delay). Niyati buzuq qandaydir ma’1umotni ushlab qolib, biror vaqtdan so‘ng uzatadi.
- *matn tanlashli hujum* (chosen text attack). Niyati buzuqautentifikatsiya trafigini ushlab qolib, uzoq muddatli kriptografik kalitlar xususidagi axborotni olishga urinadi.

Yuqorida keltirilgan hujumlarni bartaraf qilish qchun auten- tifikatsiya protokollarini qurishda quyidagi usullardan foydalaniladi:

- “so‘rov-javob”, vaqt belgilari, tasodifiy sonlar, indcntifi- katorlar, raqamli imzolar kabi mexanizmlardan foydalanish;
- autentifikatsiya natijasini foydalanuvchilarning tizim doirasi- dagi keyingi harakatlariga bog‘1ash. Bunday yondashishga misol tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyingi o‘zaro aloqalarida ishlatiluvchi maxfly seans kalitlarini almashishni ko‘rsatish mumkin;
- aloqaning o‘rnati1gan seansi doirasida autentifikatsiya muo- lajasini vaqti-vaqti bilan bajarib turish va h.

“So‘rov-javob” mexanizmi quyidagicha. Agar foydalanuvchi d foydalanuvchi U dan oladigan xabari yolg‘on emasligiga ishonch hosil qilishni istasa, u foydalanuvchi U uchun yuboradigan xabarga

oldindan bilib bo‘lmaydigan element — A so‘rovini (masalan, qandaydir tasodifiy sonni) qo‘shadi. Foydalanuvchi V javob berishda bu amal ustida ma’1um amalni (masalan, qandaydir *f(X)* funksiyani hisoblash) bajarishi lozim. Buni oldindan bajarib bo‘1- maydi, chunki so‘rovda qanday tasodifiy son kelishi foyda- lanuvchi K ga ma’1um emas. Foydalanuvchi K harakati natijasini olgan foydalanuvchi *A* foydalanuvchi U ning haqiqiy ekanligiga ishonch hosil qilishi mumkin. Ushbu usulning kamchiligi - so‘rov va javob o‘rtasidagi qonuniyatni aniqlash mumkinligi.

Vaqtni belgilash mexanizmi har bir xabar uchun vaqtni qayd-

lashni ko‘zda tutadi. Bunda tarmoqning har bir foydalanuvchisi kel-gan xabaming qanchalik eskirganini aniqlashi va uni qabul qil- maslik qaroriga kelishi mumkin, chunki u yo1g‘on bo‘1ishi mumkin. Vaqtni belgilashdan foydalanishda seansning haqiqiy ekanligini tasdiqlash uchun *kechikishning joiz vaqt oralig’i* muammosi paydo bo‘1adi. Chunki, “vaqt tamg‘asi”li xabar, umuman, bir lahzada uza-tilishi mumkin emas. Undan tashqari, qabul qiluvchi va jo‘natuv- chining soatlari mutlaqo sinxronlangan bo‘1ishi mumkin emas.

Autentifikatsiya protokollarini taqqoslashda va tanlashda quyi-dagi xarakteristikalarni hisobga olish zarur:

- *o’zaro autentifikatsiyaning mavjudligi.* Ushbu xususiyat autentifikatsion almashinuv taraflari o‘rtasida ikkiyoqlama autentifi- katsiyaning zarurligini aks ettiradi;
- *hisoblash samaradorligi.* Protokolni bajarishda zarur bo‘1- gan amallar soni;
- *kommunikatsion samaradorlik.* Ushbu xususiyat autentifi- katsiyani bajarish uchun zarur bo‘1gan xabar soni va uzunligini aksettiradi;
- *uchinchi tarafning mavjudligi.* Uchinchi tarafga misol tari- qasida simmetrik kalitlarni taqsimlovchi ishonchli serveri yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko‘rsatish mumkin;
- *xavfsizlik kafolati asosi.* Misol sifatida nullik bilim bilan isbotlash xususiyatiga ega bo‘1gan protokollami ko‘rsatish mumkin;
- *sirni saqlash.* Jiddiy kalitli axborotni saqlash usuli ko‘zda tutiladi.