Kompyuter virusları və antivirus proqramları

Səid Həmidov
ADPU-nun dosenti
E-mail: hamidovsaid@mail.ru

Rəyçilər: t.e.ü.f.d., dos. A.M. Quliyev,
t.e.ü.f.d. Ç.M. Həmzəyev

Açar sözlər: proqramçı, virus, proqram, rezident, elektron poçt, internet, antivirus, mühafizəçi, detektor, revizor, skaner

Ключевые слова: программист, вирус, программа, резидент, электронная почта, интернет, антивирус, защитник, детектор, ревизор, сканер

Key words: programmer, virus, program, resident, e-mail, Internet, antivirus, keeper, detektor, revizor, scanner

Kompyuter virusu peşəkar proqramçılar tərəfindən yaradılmış çoxalma qabiliyyətinə malik kompüterin işini əngəlləyən proqramdır. Bu günə qədər 50000-dən artıq kompüter virusunun növləri məlumdur. Kompyuter viruslarının yaranma tarixi dəqiq məlum olmasa da. İlk kompyuter viruslarının meydana gəlməsi 1986-cı ilə təsadüf edir. Viruslar 3 məqsəqlə yaradılır: intiqam, kommersiya, özünü təsdiq. Virusun aşkar edilməməsi üçün o çox kiçik həcmə malik olmalıdır. Odur ki, virus proqramları çox zaman Asembler proqram dilində yazılır.

Kompyuter virusları yalnız proqram vasitəsilə fəaliyyət göstərir. Onlar bir qayda olaraq, fayllarla birləşir və onun tərkibinə daxil olur. Belə olan halda fayl virusa yoluxmuş hesab edilir. Kompyuter virusunun aktivləşməsi üçün virusa yoluxmuş faylı icra etmək kifayətdir. Bundan sonra kompüter virusu müstəqil surətdə fəaliyyət göstərir.

Bəzi viruslar yoluxmuş fayl icra edildikdən sonra rezident virusa çevrilərək əməliyyat yaddaşında özünə yer alır. Digər növ viruslar isə aktivləşdikdən sonra kompüterə ciddi əngəllər törədir. Bunlara misal olaraq kompyuterdə işləmək üçün istifadəçiyə mane olan lazımsız effektləri və sərt diskdəki informasiyanın itməsini göstərmək olar.

Kompyuter viruslarının əksər hissəsi icraedici proqramları yoluxdurur. Son zamanlar elektron poçt və İnternet şəbəkəsi vasitəsilə yayılan viruslar xüsusilə əksəriyyət təşkil edir.

Kompyuteri viruslarına yoluxmanın əsas mənbələri aşağıdakılardır:

- tərkibində virusa yoluxmuş fayl olan xarici yaddaş qurğuları,
- kompyuter şəbəkələri, o cümlədən elektron poçt və internet,
- əvvəlki istifadəçi tərəfində əməliyyat yaddaşında ilişib qalmış virus.

Kompyuterin virusa yoluxmasının ilkin əlaməti aşağıdakılardır:

- əməliyyat yaddaşının həcminin kiçilməsi,
- kompyuterin yüklənməsinin və iş prosesinin ləngiməsi,
- səbəbsiz olaraq faylları da dəyişikliyin yaranmasıdır,
- əməliyyat sistemi yükləyərkən səhv haqqında məlumatı ekrana çıxması,
- faylların əmrə tabe olmaması,
- ekrana lazımsız vizual və audio effektlərin çıxması,

Kompyuter virusu aktiv fazada olduqda aşağıdakılar baş verir:

- fayllar silinir,
- sərt disk formatlanır,
- əməliyyat sistemi yüklənmir.

Kompyuterin virusa yoluxmasının qarşısını almaq üçün aşağıdakı tədbirləri həyata keçirilmək lazımdır:

- informasiyanın kompüterdən kənarda xarici yaddaş qurğusunda saxlanılması,
- kompyuterdə antivirus proqramına malik olmaq,
- təsadüfi, mənbəyi bilinməyən proqramlarla işləməməli,
- əgər kompüter arxasında, digərləri işləyibsə kompyuterin qarşısında oturan zaman onu söndürüb yenidən yandırmalı.

Adətən kompyuter viruslarından qorunma vasitəsi kimi antivirus proqramlarından istifadə edilir. Antivirus virusları tapan və onları zərərsizləşdirən proqramdır.

Qeyd etmək lazımdır ki, kompüter virusları öz inkişafına görə antivirus proqramlarını qabaqlayır. Buna görə də mütəmadi olaraq antivirus proqramından istifadə etmək də 100% təhlükəsizliyə təminat vermir. Antivirus proqramları yalnız tanınmış virusları tapır, onları zərərsizləşdirə bilir. Yeni virusla çıxdıqda isə onlara bir növ gücü çatmır. Buna görə də antivirus proqramının yeniləməyi tələb olunur. Buna baxmayaraq, müasir antivirus proqram paketləri öz daxilində xüsusi proqram modulları saxlayır. Bu modullar evristik analiz apararaq faylın tərkibində olan koda görə kompüter viruslarını tapır. Bu da kompyuterin virusa yoluxmasının qabağını almağa imkan yaradır.

Antivirus proqramları funksiyalarından asılı olaraq aşağıdakı tiplərə bölünür: Həkim proqramları: tapır, silir və ya müalicə edir: Dr. Solomon, Norton AntiVirus, Doctor Web, Aidstest, AVP, Anti Viral Toolkit Pro Scaner, Kaspersky Personal, Nod 32, Avast

Mühafizəçi proqramlar: Əməliyyat yaddaşında yerləşir, yalnız tapır: AntiViral Toolkit Pro Manitor.

Detektor proqramlar: yalnız onlara məlum virusları tapır.

Revizor proqramlar: sistemin ilkin vəziyyəti ilə yükləmədən sonrakı vəziyyəti müqayisə edilir. Faylların cəminin fərqi yoxlanılır.

Viruslarla mübarizə proqramlarının bir neçə növü var — skanerlər (başqa adı: faqlar, polifaqlar), disk müfəttişləri (CRC-skanerlər), rezident monitorlar və immunizatorlar.

Skanerlər. Antivirus skanerlərin iş prinsipi faylların və sistem yaddaşının yoxlanmasına və onlarda məlum və ya yeni (skanerə məlum olmayan) virusların axtarışına əsaslanır. Məlum virusların axtarışı üçün «maska»lardan istifadə edilir. Virusun maskası konkret virus üçün spesifik olan müəyyən sabit kodlar ardıcıllığıdır. Bir çox skanerlərdə həmçinin «evristik skanlama» alqoritmlərindən istifadə edilir, yəni yoxlanan obyektdə əmrlər ardıcıllığı analiz edilir, müəyyən statistika toplanır və hər bir yoxlanan obyekt üçün qərar qəbul edilir.

Disk müfəttişləri. Disk müfəttişlərinin (CRC-skanerlərin) iş prinsipi diskdə olan fayllar və sistem sektorları üçün CRC-cəmlərin (nəzarət cəmlərinin) hesablanmasına əsaslanıb.

Rezident monitorlar. Rezident monitorlar — daim operativ yaddaşda yerləşən və disklə və operativ yaddaşla aparılan əməliyyatlara nəzarət edən proqramlardır.Məhz bu proqramlar əvvəlki ikisindən fərqli olaraq sistemin real yoluxma anına kimi virusu aşkarlamağa imkan verir.

İmmunizatorlar. İmmunizatorların iki növü var: yoluxma barədə məlumat verən immunizatorlar və hər hansı növ virusa yoluxmanın qarşısını alan immunizatorlar.

Onlardan birincisi adətən faylların sonuna yazılır və hər dəfə fayl işlədikdə onun dəyişməsini yoxlayır. Bu immunizatorların bir nöqsanı var — stels-virusla yoluxma barədə

məlumat verməyə qabil deyil. Buna görə bu immunizatorlar hazırda praktikada istifadə edilmir. İkinci növ immunizator sistemi hər hansı müəyyən növ virusla yoluxmaqdan mühafizə edir. Diskdə fayllar elə modifikasiya edilir ki, virus onları artıq yoluxmuş fayl kimi qəbul edir. Rezident virusdan mühafizə üçün kompüterin yaddaşına virusu imitasiya edən proqram yüklənir. Virus işə düşdükdə onunla rastlaşır və hesab edir ki, sistem artıq yoluxub.

Anti-Virus proqramlarının yoxlanılması prosesini həyata keçirən AV-Comparatives-in məlumatlarına istinadən ən yaxşı Anti-Virusproqramlarını nəzərdən keçirək.

Add-Aware Free Antivirus. Pulsuz antivirus proqramı olan Ad-Awareinternet üzərindən cihaza zərər verəcək proqramlara qarşı çox təsirli bir antivirus proqramıdır. Sizə internet, e-mail və şəbəkə qoruması təqdim etməsinin yanında anlıq qoruma da təmin etməkdədir.

Avast Free Antivirus. İnternet qoruması, e-poçt nəzarəti, oyun rejimi və başqa funksiyaları özündə birləşdirən Avast pulsuz antivirus proqramıdır, lakin digər məşhur antivirus proqramları kimi bəzi funksiyaları yalnız ödənişli versiyasında aktivdir.

*AVG Free Antivirus.*AVG antivirus proqramı etibarlı olmayan əlaqələri, endirmələri və e-poçt faylları sürətli şəkildə gözdən keçirməyə imkan verir.

Software Updater xüsusiyyətiylə yenilikləri avtomatik olaraq edərək səhvləri düzəldir və təhlükəsizlik açıqlarına bağlayır.

Avira Free Antivirus. Avira proqramı tamamilə ödənişsiz antivirus proqramıdır. Web qoruması, e-poçt qoruması və s. xüsusiyyətləri pulsuz şəkildə istifadə etmək olar

Bitdefender Antivirus Free. Bu proqram kompüterinizin sürətini aşağı salmadan qoruma təmin edir. Bütün web, e-poçt və mesajlaşma məlumatlarını hər saat yoxlayır və virus aşkar etdikdə onu məhv edir.

ESET NOD32 Antivirus. Antivirus olaraq uzun müddətdir hamı tərəfindən tanınmasıyla diqqəti çəkir və öz işini layiqincə yerinə yetirir. Kompyuterdə hər saat yoxlama apararaq aşkar etdiyi virusları birbaşa məhv edir.

Kaspersky Anti-Virus Kaspersky antivirus proqramı bir çox zərərli proqramlara qarşı tədbirlər alır və onları təsirsiz hala gətirir. Mükafat almış çox az antivirus proqramlarından biridir.

Məqalənin aktuallığı. Aktuallıq ondan ibarətdir ki, məqalə kompyuter təhlükəsizliyinin təmin edilməsinə həsr olunmuşdur.

Məqalənin elmi yeniliyi. Kompyuter viruslarından qorunmaq üçün üsul və vasitələrdən istifadə edilməsi və antivirus proqramlarının köməyi ilə kompyuterin təhlükəsizliyinin təmin olunması ilə bağlı tövsiyələri məqalənin aktuallığı hesab etmək olar.

Məqalənin praktik əhəmiyyəti və tətbiqi. Bu, məqalədə bəhs edilən üsul və vasitələrdən istifadə etməklə kompyuter viruslarından qorunmanın təmin edilməsidir.

Ədəbiyyat

1. Ю. Родичев. «Нормативная база и стандарты в области информационной безопасности» (2017).

2. Е. Баранова, А. Бабаш. «Информационная безопасность и защита информации» 3-е изд. (2016).

3. В. Бондарев. «Введение в информационную безопасность автоматизированных систем» (2016).

4. С. Нестеров «Основы информационной безопасности» (2016).

5. А. Бирюков «Информационная безопасность: защита и нападение» 2-е изд. (2017).

С. Гамидов

Компьютерные вирусы и антивирусные программы

Резюме

В статье затронуты следующие вопросы:

- история создания и цель компьютерных вирусов;
- действие и классификация компьютерных вирусов;
- источники компьютерных вирусов;
- ранние признаки заражения компьютером вирусами;
- защита информации от компьютерных вирусов;
- классификация антивирусных программ;

S. Gamidov

Computer viruses and antivirus programs

Summary

The article covers the following questions:

- the history of creation and purpose of computer viruses;
- action and classification of computer viruses;
- sources of computer viruses;
- early signs of computer virus infection;
- protection of information from computer viruses;
- classification of antivirus programs.

Redaksiyaya daxil olub: 22.04.2019