Virusla mübarizə

Səkinə İmran qızı Səfiyeva
Azərbaycan Dövlət Pedaqoji Universitetinin
baş müəlilimi
E-mail: sakinasafiyeva@gmail.com

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

Açar sözlər: virus, antivirus, proqram, fayl, sistem, skaner, monitor
Ключевые слова: вирус, антивирус, программное обеспечение, файл, система, сканер, монитор
Key words: virus, antivirus, software, file, system, scanner, monitor

Virusla mübarizə aparmaq üçün xüsusi proqram təminatından – antivirusdan istifadə edilir. İndiki zamanda antivirusların müxtəlif növlərinə rast gəlmək mümkündür və onlar aşağıdakı funksiyaları yerinə yetirirlər:

- **Proqramlar-detektorlar** operativ yaddaşda və fayllarda virus üçün xarakterik olan kodların (siqnaturların) axtarışını həyata keçirirlər. Virus tapıldıqda uyğun məlumatı bildirirlər;
- **Proqramlar-doktorlar** və ya faqi. Bunlar da virusa yoluxmuş faylları axtarıb tapır və onları "müalicə" edirlər, yəni faylı əvvəlki vəziyyətinə qaytarırlar. Faqların arasında yarımfaqlardan da istifadə olunur. Yarımfaqlar və yaxud proqramlar-doktorların təyinatı ondan ibarətdir ki, onlar böyük sayda virusları tapmaqla yanaşı onları məhv də edirlər;
- **Yoxlayıcılar (və ya müfəttişlər)** obyektin yoluxmamışdan qabaqkı vəziyyətini yadda saxlayır və mütamadi olaraq cari vəziyyəti başlanğıc vəziyyətlə müqayisə edirlər;
- **Proqramlar-süzgəclər və ya rezidentlər** (yaxud da daim işləyənlər) kompüter işləyən zaman onda baş vermiş şübhəli fəaliyyəti (viruslara xarakterik olan fəaliyyəti) aşkar etmək üçündür.
- **Vaksinlər rezident proqramlardır,** faylların virusa yoluxmasının qarşısını alırlar. Müasir antivirus proqramları çoxfunksiyalı proqram kompleksidir, əsas vəzifələri virusu tapmaq, müalicə etmək (yəni kanarlaşdırmaq), həmçinin onun kompüterə daxil olmasına maneçilik etməkdir. Müasir antivirus proqramları iki rejimdə işləyir. Monitor rejimində antivirus daim işləyir, sistemin fayla müraciətini izləyir, prosesə daxil olmaqla bu faylların yoluxma predmetini yoxlayır.

Deməli, virusun fayla düşməsi üçün etdiyi birinci cəhd antivirus tərəfindən bloklanır (qıfıllanır) və bu barədə xəbərdarlıq olunur. Kompüter monitor rejimində işləyəndə kompüterin işində ləngimə baş verir, çünki hesablama resurslarının bir hissəsi işlərini antivirusa həsr edirlər, bununla yanaşı fayla və bəzi obyektlərə istənilən müraciət skanerləmə proseduru ilə həyata keçirilir. Digər tərəfdən əgər kompüterdə yoluxmuş fayllar varsa və o fayllar aktivlik göstərmirsə, onda onlara müraciət baş vermir, onlar nəzərdən kanarda qalırlar. Skaner rejimində antivirus proqramı verilmiş sahədə (müəyyən kataloqda, sərt diskin bölmələrində və ya informasiya saxlayan bütün qurğularda) bütün faylları yoxlayır və yoluxmanı kanarlaşdırır (və ya skanerin sazlanmasından asılı olaraq onlar barədə məlumat verir). Verilənlərin kompüterdə yoxlanılması müəyyən qədər vaxt aparır (bəzən bir neçə saat). Bununla yanaşı, bəzi hallarda virus sistemə skanerə əməliyyatı tamamlandıqdan sonra da düşə bilər. Sistemin etibarlı müdafiə edilməsi üçün hər iki rejimdən istifadəni məsləhət bilirlər. Monitor rejimində antivirus proqramının daim işləməsi nəzərə alınmaqla yoxlamanı mütamadi olaraq həftədə bir dəfə (bü-

tün verilənləri yoxlamaqla), skaner rejimində isə yoxlamanı axşamlar həyata keçirməyi məsləhət bilirlər. Antivirusun öz "qurbanları"nı necə aşkar etməsi üsullarına baxaq. Siqnatura əsaslanan aşkaretmə. Əgər antivirus sistemə virusun soxulmasını aşkar edirsə, onda antivurus faylı (və ya şəbəkədən gələn paketi) nəzərdən keçirir, sonra isə məşhur hücumların və ya virusların adları olan siqnatur lüğətə müraciət edir. Seçim edildikdən sonra antivirus fəaliyyətə başlayır. Siqnaturun yaradılması əl ilə, bir neçə faylın korporativ araşdırmalar yolu ilə yerinə yetirilir. Siqnaturun avtomatik generasiya edilməsi (adətən polimorf viruslar olan mühitdə) hələlik tutarlı səviyyədə nəticə verməmişdir. Hər bir müasir antivirus proqramı geniş (bir neçə yüz minlərlə) mütamadi yenilənən siqnatur bazasına malikdir. Yoluxmanın siqnaturlar vasitəsilə müəyyən edilməsi ona əsaslanır ki, yeni virus (hələlik siqnaturu bazada olmayan) çox asanlıqla antivirus müdafiəsini yarıb keçə bilər. Odur ki, siqnaturu yaradanda və onu istifadəçiyə təqdim edəndə bu 11-dən 97 saata kimi vaxt aparır (istehsalçıdan asılı olarq). Nəzəri olaraq hesablanmışdır ki, virus İnternetə elə hücum təşkil edər ki, onu 30 saniyədən az müddət ərzində zəbt edər.

Proqramın özünü şübhəli aparmasının aşkar edilməsi üsulu. Antivirus proqramı bütün işləyən proqramların özünü necə aparmasını izləyir və virusa xarakter olan halların (məsələn, verilənlərin exe-fayla yazılmasını) aşkarlanmasına cəhd edir. Təcrübə göstərir ki, bu üsul bəzi hallarda baş vermiş hadisəyə reaksiya verə bilmir (yalana uyur), nəticədə istifadəçi edilən xəbardarlığa reaksiya vermir. Üsulun müxtəlif növləri vardır. Proqramın emulyasiya olunması, yəni proqram işə salınmazdan öncə antivirus onun özünü aparmasını (şübhəli halları izləmək məqsədi ilə) imitasiya etməyə çalışır.

AÇIQLAMA: Emulyasiya (ingiliscə emulation) hesablama texnikasında proqramlar, aparat vasitələri və ya onların birləşməsi (ahəngi, uyğunluğu) kompleksidir və bir hesablama sistemi (qonaq) funksiyasının digərinə (birincidən fərqli, hesablama sisteminə - hosta) kopiyalanması (və ya emulyasiyası) üçün nəzərdə tutulmuşdur.

Kompüterdə virus əlamətləri aşkarlandıqda nə etmək lazım olduğunu şagirdlərə başa salmaq lazımdır. İlk addım olaraq yerinə yetirdikləri işlərin nəticələrini xarici daşıyıcılarda (CD və ya DVD-diskdə, fləş kartda və s.) saxlasınlar. Sonra:

- Kompüteri lokal şəbəkədən və İnternetdən ayırın;
- əməliyyat sistemi kompüterə düşmüş virus nəticəsində sərt diskdən yüklənmirsə, onda onu CD diskdən yükləməyə çalışın;
- antivirus proqmını başladın.

Virusla mübarizə tədbirləri

Virusla mübarizə aparmaq üçün xüsusi proqram təminatından – **antivirus**dan istifadə edilir.

Antivirus proqramları hansı funksiyaları yerinə yetirir?

İndiki zamanda antivirusların müxtəlif növlərinə rast gəlmək mümkündür və onlar aşağıdakı funksiyaları yerinə yetirirlər:

1. Proqramlar-detektorlar operativ yaddaşda və fayllarda virus üçün xarakterik olan kodların axtarışını həyata keçirirlər. Virus tapıldıqda uyğun məlumatı bildirirlər;

2. Proqramlar-doktorlar və ya faqi. Bunlar da virusa yoluxmuş faylları axtarıb tapır və onları "müalicə" edirlər, yəni faylı əvvəlki vəziyyətinə qaytarırlar. Faqların arasında yarımfaqlardan da istifadə olunur. Yarımfaqlar və yaxud proqramlar-doktorların təyinatı ondan ibarətdir ki, onlar böyük sayda virusları tapmaqla yanaşı onları məhv də edirlər;

3. Yoxlayıcılar (və ya müfəttişlər) obyektin yoluxmamışdan qabaqkı vəziyyətini yadda saxlayır və mütamadi olaraq cari vəziyyəti başlanğıc vəziyyətlə müqayisə edirlər;

4. Proqramlar-süzgəclər və ya rezidentlər kompüter işləyən zaman onda baş vermiş şübhəli fəaliyyəti aşkar etmək üçündür.

5. Vaksinlər rezident proqramlardır, faylların virusa yoluxmasının qarşısını alırlar.

6. Müasir **antivirus** proqramları çoxfunksiyalı proqram kompleksidir, əsas vəzifələri virusu tapmaq, müalicə etmək, həmçinin onun kompüterə daxil olmasına maneçilik göstərməkdir.

Müasir antivirus proqramları neçə rejimdə işləyir?

Müasir antivirus proqramları iki rejimdə işləyir.

Monitor rejimində antivirus daim işləyir, sistemin fayla müraciətini izləyir, prosesə daxil olmaqla bu faylların yoluxma predmetini yoxlayır. Deməli, virusun fayla düşməsi üçün etdiyi birinci cəhd antivirus tərəfindən bloklanır və bu barədə xəbərdarlıq olunur.

Kompüter **monitor** rejimində işləyəndə kompüterin işində ləngimə baş verir, çünki hesablama resurslarının bir hissəsi işlərini **antivirusa** həsr edirlər, bununla yanaşı fayla və bəzi obyektlərə istənilən müraciət skanerləmə proseduru ilə həyata keçirilir. Digər tərəfdən, əgər kompüterdə yoluxmuş fayllar varsa və o fayllar aktivlik göstərmirsə, onda onlara müraciət baş vermir, onlar nəzərdən kanarda qalırlar.

Skaner rejimində **antivirus** proqramı verilmiş sahədə bütün faylları yoxlayır və yoluxmanı kanarlaşdırır. Verilənlərin kompüterdə yoxlanılması müəyyən qədər vaxt aparır. Bununla yanaşı, bəzi hallarda virus sistemə skanerə əməliyyatı tamamlandıqdan sonra da düşə bilər.

Sistemin etibarlı müdafiə edilməsi üçün hər iki rejimdən istifadəni məsləhət bilirlər.

Monitor rejimində antivirus proqramının daim işləməsi nəzərə alınmaqla yoxlamanı mütamadi olaraq həftədə bir dəfə, **skaner** rejimində isə yoxlamanı axşamlar həyata keçirməyi məsləhət bilirlər.

Antivirus öz "qurbanları"nı necə aşkar edir?

Antivirusun öz "qurbanları"nı necə aşkar etməsi üsullarına baxaq.

Siqnatura əsaslanan aşkaretmə. Əgər antivirus sistemə virusun soxulmasını aşkar edirsə, onda antivirus faylı nəzərdən keçirir, sonra isə məşhur hücumların və ya virusların adları olan siqnatur lüğətə müraciət edir. Seçim edildikdən sonra antivirus fəaliyyətə başlayır.

Siqnaturun yaradılması əl ilə, bir neçə faylın korporativ araşdırmalar yolu ilə yerinə yetirilir. Siqnaturun avtomatik generasiya edilməsi hələlik tutarlı səviyyədə nəticə verməmişdir.

Hər bir müasir antivirus proqramı geniş mütamadi yenilənən siqnatur bazasına malikdir. Yoluxmanın siqnaturlar vasitəsilə müəyyən edilməsi ona əsaslanır ki, yeni virus çox asanlıqla antivirus müdafiəsini yarıb keçə bilər. Odur ki, siqnaturu yaradanda və onu istifadəçiyə təqdim edəndə bu 11-dən 97 saata kimi vaxt aparır.

Nəzəri olaraq hesablanmışdır ki, virus İnternetə elə hücum təşkil edər ki, onu 30 saniyədən az müddət ərzində zəbt edər.

Proqramın özünü şübhəli aparmasının aşkar edilməsi üsulu.

Antivirus proqramı bütün işləyən proqramların özünü necə aparmasını izləyir və virusa xarakter olan halların aşkarlanmasına cəhd göstərir. Təcrübə göstərir ki, bu üsul bəzi hallarda baş vermiş hadisəyə reaksiya verə bilmir, nəticədə istifadəçi edilən xəbardarlığa reaksiya vermir.

Bu üsulun müxtəlif növləri vardır.

Proqramın **emulyasiya** olunması, yəni proqram işə salınmazdan öncə antivirus onun özünü aparmasını imitasiya etməyə çalışır.

"Ağ siyahı" üsulu. Öncədən təhlükəsiz kod kimi administrator tərəfindən qeyd olunan kompüter kodları kombinasiyasının qabağı alınır.

Evristik skanerə üsulu. Üsul siqnatura və evristikaya əsaslanır. Üsulun əsas məqsədi siqnaturdan istifadə etməklə skanerləmə bacarığını artırmaq və modifikasiya edilmiş virus versiyalarını aydınlaşdırmaqdır. Modifikasiya edilmiş virus versiyalarını aydınlaşdıranda siqnaturun naməlum proqram cismi ilə uyğunluğu ən azı **100%** olması nəzərə alınmalıdır.

Beləliklə, biz öyrəndik ki, virusun fəaliyyət ssenarisi təxminən bu cürdür.

- Kompüterdə yoluxdurulması mümkün olan bütün proqramlar.
- Özünü proqramın əvvəlinə və sonuna yazmaq.
- Əgər virusun hücuma keçəcəyi gün yetişmişsə, dagıdıcı işlər görmək.

- Kompüterin sərt diskində hər hansı kiçik sahəni "şifrələmək"

XXI əsrin əvvəllərində virusların başilica fəaliyyəti düşdüyü kompüterdən hər hansı informasiyanı oğurlamağa və həmin kompüterə kənar şəxslərin daxil olmasını təmin etməyə yönəlmişdir.

Şagirdlərin nəzərinə çatdırılır ki, kompüter viruslarından qorunma üç səviyyədə ola bilər.

Birinci sıviyyədə virusların kompüterə girməsinin qarşısı alınır.

İkinci səviyyədə virus hücumlarının qarşısı alınır.

Üçüncü səviyyədə virus hücumlarının təsiri minimuma endirilir.

Virus hücumlarının qarşısını almaq üçün antivirus proqramlarından istifadə olunur. Bu gün Symantec Norton Antivus, Kasperiski antivirusu, DrVeb, Mc VirusScan, Panda Titanium antivirus kimi antivirus proqramları daha çox işlədilir. Şagirdlərə başa salınır ki, sadaladığımız proqramlar, əsasən kommerasiya məhsuludur.

Lakin fərdi kompüterdə istifadəçi havayı olan antivirus proqramlarından istifadəyə üstünlük verir.

Onların içərisində **avast!** daha əlverişlidir. Bu proqramı WWW.avast.com saytından əldə emək olar.

Məqalənin aktuallığı. Virusla mübarizə aparmaq üçün xüsusi proqram təminatından – antivirusdan istifadə edilir. Müasir dövrdə antivirusların müxtəlif növlərinə rast gəlmək mümkündür ki, onlar da müxtəlif funksiyaları yerinə yetirirlər. Bu və digər məsələlərin təhlili və öyrənilməsi baxımından məqalə aktual hesab edilməlidir.

Məqalənin elmi yeniliyi. Məqalədə antivirusların müxtəlif növlərinin yerinə yetirdiyi funksiyaların təhlili verilir, proqramın özünü şübhəli aparmasının aşkar edilməsi üsulu nəzərdən keçirilir və kompüterdə virus əlamətləri aşkarlandıqda nə etmək lazım olduğunun yolları göstərilir.

Məqalənin praktik əhəmiyyəti və tətbiqi. Məqalədən ali, orta ixtisas və ümumtəhsil məktəblərinin müəllimləri, tələbə və magistrantlar istifadə edə bilərlər.

Ədəbiyyat

1. İnternet materialları.
2. İ.Sadıqov, R.Mahmudzadə, N.İsayeva. İnformatika-10. Bakı, 2014.
3. İnformasiya təhlükəsizliyi. Dərslik. B., 2015.

С.И. Сафиева

Борьба с вирусом

Резюме

Для борьбы с вирусом используется специальное антивирусное программное обеспечение. Современное антивирусное программное обеспечение - это многофункциональный программный комплекс, основной задачей которого является обнаружение, лечение (т.е. излечение) вируса и предотвращение его доступа к компьютеру.

S.I. Safiyeva

Fight the virus

Summary

Special antivirus software is used to fight the virus. Modern antivirus software is a multifunctional software complex whose main task is to detect, treat (if censure) the virus and prevent its access to the computer.

Redaksiyaya daxil olub: 13.10.2020