UOT 002.6

SƏADƏT MƏMMƏDOVA

KOMPÜTER VİRUSLARI VƏ ONLARDAN QORUNMA YOLLARI

Təqdim olunan işdə, girişdə müasir kompüterlərin ən böyük və qorxulu düşməni olan kompüter virusları və bu virusların meydana gəlməsinin qısa tarixi haqqında geniş məlumat verilir. Göstərilir ki, Windows əməliyyat sistemi yaranandan və İnternetdən istifadə genişlənəndən sonra kompüter virusları ilə mübarizə daha da kəskin şəkil alır. Bunun üçün müasir antivirus proqramları hazırlanır. Hazırda dünyada antivirus proqram təminatının işlənib hazırlanması ilə bağlı bir neçə kompaniya məşğul olur. Qeyd olunur ki, bunlara baxmayaraq kompüter virusları ilə universal və daha etibarlı mübarizə vasitəsi hələ ki yoxdur.

Açar sözlər: *kompüter virusları, antivirus proqramlar, ziyanverici proqram təminatı, internet, mobil viruslar.*

Heç kimə sirr deyil ki, hər bir müasir kompüterin ən böyük və qorxulu düşməni viruslardır. Virus ingilis sözü olub, tərcüməsi manea, əngəl deməkdir. Virus üçün fərdi kompüterin hansı məqsədlə istifadə edilməsi, internetə və ya lokal şəbəkəyə qoşulub-qoşulmamasının fərqi yoxdur. Kompüter virusu nədir? Əslində, bu ad altında bir-neçə növ ziyanverici proqramlar gizlənir ki, bunların da hər birinin özünəməxsus kompüterə daxil olmaq metodikası vardır. Bu gün 50 minə yaxın kompüter virusu məlumdur. Bu kiçik ziyanverici proqramlar aşağıdakı 3 qayda ilə yaşayırlar:

– Çoxalmaq;

– Gizlənmək;

– Pozmaq.

Kompüter virusu kompüterdəki fayla və ya proqrama əlavə edilmiş, bir kompüterdən digərinə keçməklə yayılan proqramdır. Viruslar kompüterə düşməklə onun işinə maneçilik edir, kompüterdə yerinə yetirilən əməliyyatları ləngidir, kompüterin əməliyyat sistemini tamamilə korlayır. Virusların yayılmasında əsas rolu kompüterlərdə istifadə edilən fləş qurğuları, bir istifadəçinin digərinə məktub göndərdiyi zaman istifadə etdiyi e-mail, istifadəçilər arasında piratlıq (oğurluq) yolu ilə birindən digərinə ötürülən, çox istifadə edilən virus yoluxmuş proqramlar oynayır [2, 3].

Kompüter viruslarının təsnifatı. Viruslar daxili quruluşuna görə destruktiv və qeyri-destruktiv kimi təsnif olunurlar. Destruktiv (latıncadan tərcümədə normal strukturun pozulması, dağıdılması mənasını verir) viruslar yerinə yetirdiyi funksiyaya görə aşağıdakı kimi təsnif olunurlar:

1. Verilənləri məhv edən viruslar. Bu tip viruslara "Chernobyl və ya Spacefiller" (1999-cu il) və "Klez.E" (2002-ci il) virusların nümunə göstərmək olar.

2. Casus viruslar. Virusun daxili istifadəçisi klaviatura üzərindəki istənilən düyməni sıxdıqda informasiyanı oğurlayır və verilənləri xüsusi fayla yazaraq virusun müəllifinə göndərir.

3. Kripto-viruslar. Sərt diskdə olan informasiyanı açıq açar alqoritmi ilə şifrələdikdən sonra istifadəçiyə təqdim edir.

Bir qayda olaraq, virus öz həyat dövrünün 4 mərhələsinin birində ola bilir.

– Birinci mərhələ sistemin zəif yerinin təyin edilməsidir. Zəif yer həm təşkilati-hüquqi, həm də proqram-aparat təminatı ilə bağlı ola bilər.

– İkinci mərhələ sistemin zəif yerindən virus hücumu üçün istifadə edilməsidir. Bu mərhələdə virus hostlardan birini yoluxdurur.

– Üçüncü mərhələ virusun işə başlamasıdır. Bu mərhələdə hədəf kompüterin arzuolunmaz davranışlara başlamasıdır.

– Dördüncü mərhələ virusun kompüter mühitində yayılmasıdır. Bu mərhələdə növbəti kompüterin zəif yeri təyin edilir və yuxarıdakı mərhələlər növbəti kompüterdə həyata keçirilir.

Hostinq (ingiliscə hosting) informasiyanı daim şəbəkəyə qoşulmuş serverdə (adətən İnternetdə) yerləşdirmək üçün nəzərdə tutulan xidmətlərin təqdim olunma resurslarıdır. Adətən hostinq sayta göstərilən xidmət paketinə daxil olur və serverdə yerləşmiş sayt fayllarına minimum xidmət göstərir [4].

Kompüter viruslarının meydana gəlməsinin qısa tarixi: Təəssüf ki, tarix kompüter ziyanvericilərinin yaradılması barədə olan çox faktı üzə çıxarmamışdır. Lakin, buna baxmayaraq bəzi faktlar məlumdur. Ziyanverici proqramların bu növünün tarixi nə az, nə çox 50 il əvvələ, yəni keçən əsrin 60-cı illərinin sonuna gedib çıxır. İlk kompüter viruslarının yaradılması 1960-cı illərin sonlarına təsadüf edir. 1960-cı illərin sonu, 1970-ci illərin əvvəlində periodik olaraq maynfreymlərdə "dovşan" (the rabbit) adlandırılan proqramlar meydana çıxdı. Bu proqramlar özlərini klonlaşdırıb, sistem resurslarını zəbt edərək onların məhsuldarlığını aşağı salırdı. 1977-ci ildə, ilk Apple fərdi kompüterlərinin istehsal olunması və infrastruktur şəbəkəsinin inkişafı ilə əlaqədar olaraq yeni viruslar əsrinin başlanğıcı qoyulur. Növbəti mərhələ 1970-ci illərin əvvəlində BBN şirkətinin əməkdaşı Bob Tomas tərəfindən özü yerini dəyişən Creeper proqramı yaradıldı. Bu zaman Reaper adlı daha bir proqram hazırlandı ki, bu da ilk antivirus proqramı idi. Reaper kompüterdən-kompüterə keçərək Creeper-in fəaliyyətdə olan nüsxəsini tapıb məhv edirdi.1970-ci ildə daha bir əhəmiyyətli hadisə baş verdi. May ayında Venture jurnalında Gregory Benford-un fantastik "The Scarred Man (Üzü çapıqlı adam)" hekayəsi çap edildi. Həmin hekayədə Virus və Vaccine adlı iki obraz var idi. Bu obrazlardan biri virus, digəri antivirus proqramının ilk təsvirləri idi. İki ildən sonra David Gerrold-un "When Harlie Was One (Xarli bir yaşında olanda)" adlı fantastik romanında sistemi zəbt edən qurda bənzər proqram təsvir edilmişdi. "Qurd" termini ilk dəfə 1975-ci ildə Jhon Brunner-in "The Shockwave Rider (Sarsıdıcı dalğada)" adlı romanında istifadə olunmuşdu.

"Kompüter virusu" termini ilk dəfə 1973-cü ildə Westworld adlı fantastik filmdə istifadə edilmişdi. Bu söz birləşməsi müasir adamların adət etdiyi mənada, yəni "kompüter sisteminə soxulan ziyanverici proqram" kimi işlədilmişdi. Nəhayət, 1977-ci il aprelin 20-də kütləvi istifadə üçün kompüter istehsal edildi və bu hadisə özütörəyən proqramların özünü reallaşdırması şəraitini əhəmiyyətli dərəcədə yaxşılaşdırdı. 1981-ci ildə 15 yaşlı məktəbli Richard Skrenta Apple II fərdi kompüteri üçün ilk yükləmə virusunu hazırlayır. Virus çoxda böyük olmayan şeirdən ibarət idi və fərdi kompüter istifadəçisini salamlamaqla özünü büruzə verirdi. Virus DOS əməliyyat sisteminə yoluxmaqla yayılırdı. Proqram virusa yoluxmamış disketə rast gələn kimi özünü həmin disketə köçürürdü. Bu virusun təsirindən ilk zərər görənlər Richardın dostları və tanışları, həmçinin, onun riyaziyyat müəllimi olmuşdur.

1986-cı ildə IBM PC üçün ilk "The Brain" virusu yaradılır. Məhz 1987-ci ildə üç böyük kompüter virusu epidemiyası baş verdi. Əmcad Fərux Əlvi və Basit Fərux Əlvi qardaşlarının yaratdığı, birinci kompüter epidemiyasına səbəb olan "Brain" virusu 1987-ci ildə aşkar edilir. McAfee-nin açıqlamasına görə təkcə ABŞ-da Brain virusu 18 mindən çox kompüterə yoluxmuşdur.1988-ci ilin may ayının 13-də eyni zamanda bir neçə universitetdə və firmada "Jerusalem" adlanan virus aşkar edildi. Həmin gün kompüterə yüklənən fayllar məhv edilmişdi. Bu, həqiqi epidemiyaya səbəb olan ilk MS-DOS viruslardan biri idi [6].

1958-ci ildə ABŞ prezidenti Duayt David Eyzenhauerin təşəbbüsü ilə yeni dövlət struk-

turu, strukturun tərkibində isə gələcək problemlərin həlli üçün *ARPA (Advanced Research Projects Agency)* agentliyi yaradıldı. Agentlik qarşısında duran əsas məsələ müdafiə sahəsində yeni və perspektiv elmi layihələrlə bağlı məsələlərin həll edilməsi idi. Tək məqsədi var idi – hərbi işlərdə Sovet dövləti Amerika Birləşmiş Ştatlarını ötüb keçməməli. Buna səbəb dünyada ilk hesablama şəbəkəsinin 1956-1960-cı illərdə keçmiş sovetlər məkanında, Qazaxıstanda akademik Lebedevin və Bursovun rəhbərliyi ilə yaradılması idi. Şəbəkəyə "Diana I" və "Diana II" adı verilmişdir. O dövrdə əsas məsələ agentlik tərəfindən kompüterlər arasında verilənlərin mübadiləsini həyata keçirən elektron şəbəkənin yaradılması idi. Şəbəkə ARPANET adlandırıldı (Net-ingiliscə "şəbəkə" mənasını verir). ARPANET şəbəkəsinin yaradılmasına 1966-cı ildən başlanılır. Tədqiqatlar Boston şəhərində yerləşən, Joseph Carl Robnett Licklider-in rəhbərlik etdiyi BBN firmasına həvalə olunur. Layihənin yerinə yetirilməsində Kaliforniya ştatının üç universiteti və Yuta ştatının bir universiteti iştirak edir. Bir-birindən 600 kilometr məsafədə yerləşən iki kompüter arasında ilk əlaqə seansı 1969-cu il, oktyabr ayının 29-da baş tutur. Bir terminaldan digər terminala ilk ötürülən informasiya "LOGİN" sözü olur. Sonrakı illərdə şəbəkəyə daha 4 universitet qoşulur. Daha sonra şəbəkənin imkanlarından (1971-ci il) daha 15 universitet istifadə etməyə başlayır. 1973-cü ildə şəbəkəyə Böyük Britaniya və Norveç universitetləri də qoşulur. Beləliklə, şəbəkə ümumdünya statusu alır.

1990-cı ildə ARPANET şəbəkəsi öz işini dayandırır, çünki şəbəkə qarşısında qoyulmuş məsələ artıq öz həllini tapmışdı. Şəbəkənin işini onun bazası əsasında yaradılmış yeni şəbəkə – İNTERNET şəbəkəsi davam etdirir. 1989-cu ildə ilk "troya atı" AIDS virusu meydana gəldi. Virus sərt diskdə olan informasiyanı əlçatmaz edirdi və ekrana təkcə "Hansısa ünvana 189 dollarlıq çek göndərin" ifadəsi çıxırdı [1, 4].

1989-cu ildə həm də antivirus proqram təminatına əks təsir göstərən "The Dark Averger" adlı ilk virus yaradılır. Bu virus antivirus proqramının kompüteri yoxladığı müddət ərzində yeni faylları yoluxdururdu. 1990-cı ilin əvvəlində "Chameleon" adlandırılan ilk polimorf virus meydana gəldi. Bu texnologiya tez bir zamanda stels-texnologiya (Stealin) və zirehləmə (Armored) ilə uzlaşdırılmaqla yeni viruslara antivirus paketlərə müqavimət göstərə bilmək imkanı verirdi. 1990-cı ilin ikinci yarısında "Frodo və Whale" adlı iki stels-virus yaradıldı. Bu virusların hər ikisində həddən artıq mürəkkəb olan stels alqoritmlərdən istifadə edilmişdi. Stels-virus (ingiliscə stealth virus – gözə görünməyən virus) sistemdə öz varlığını tam və ya hissə-hissə gizlədir. Buna görə də Stels-alqoritmlərin istifadə olunması viruslara imkan verir ki, onlar sistemdə özlərini bütünlüklə və ya hissə-hissə gizlətsinlər. Ən çox stels-alqoritm yoluxmuş obyektlərdə "oxu/yaz" əmri yerinə yetirildikdə yayılır. 1991-ci ilin əvvəlində *Tequila* adlı yükləmə virusu kütləvi epidemiyaya səbəb oldu. 1991-ci ildə öz bədəninin şəklini dəyişə bilən polimorf viruslar meydana çıxdı. Windows 95 əməliyyat sistemi praktiki olaraq belə hücuma hazır olduğunu bildirdi və firma Windows 95 əməliyyat sisteminin beta-versiyasını 160 testediciyə payladı. Polimorfizm (yunanca πολυ - çoxlu + μορφή - forma, xarici görünüş) kompüter viruslarının skan-sətir (və ya evristika) vasitəsilə aşkarlanmasını çətinləşdirən texnikadır. Belə texnikadan istifadə edən virus polimorf adlanır [7, 8].

Daha sonra Microsoft Word sənədlərini yoluxduran ilk makrovirus aşkar edildi. Bu, artıq sadəcə qeyri-adi şəkildə icra edilən fayl deyil, xüsusi ssenari idi. Bir ay ərzində "Concept" adlı makrovirus bütün Yer kürəsini dolaşaraq dünyada onlarla şirkətin mətn redaktorunu iflic etmişdi. Bugün Concept virusunun 100-ə yaxın modifikasiyası mövcuddur. 1987-ci ildə amerikalı proqramçı Ralf Berqer viruslarla mübarizə metodları haqqında kitab yazır. 1989-cu ildə məxfi dövlət Elmi Tədqiqat İnstitutunun əməkdaşı olan Eugene Kaspersky-nin kompüterinə

"Cascade" virusu düşür. Kaspersky virusu aradan qaldırmaq üçün həyatında birinci dəfə antivirus proqramı yazır. Windows əməliyyat sistemi yarananda və İnternetdən istifadə genişlənəndən sonra kompüter virusları ilə mübarizə daha da kəskin şəkil alır. Hazırda dünyada antivirus proqram təminatının işlənib hazırlanması ilə 60-a qədər kompaniya məşğul olur. Microsoft Security Essentials pulsuz antivirusdur [9, 10].

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 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;

– **Revizorlar (və ya müfəttişlər)** obyektin yoluxmamışdan qabaqkı vəziyyətini yadda saxlayır və mütəmadi olaraq cari vəziyyəti başlanğıc vəziyyətlə müqayisə edirlər;

– **Proqram-süzgəclər və ya rezidentlər (yaxud da daim işləyənlər)** kompüter işləyən zaman onda baş vermiş şübhəli fəaliyyəti aşkar etmək üçündür.

– **Vaksinlər** rezident proqramlardır, faylların virusa yoluxmasının qarşısını alırlar.

Müasir antivirus proqramları çoxfunksiyalı proqram kompleksidir, əsas vəzifələri virusu tapmaq, kənarlaşdırmaq, həmçinin, onun kompüterə daxil olmasına maneçilik törətməkdir. Müasir antivirus proqramları iki rejimdə işləyir.

– **Monitor rejimində** antivirus daim işləyir, sistemin fayla müraciətini izləyir, prosesə daxil olmaqla bu faylların yoluxma predmetini yoxlayır. İlk olaraq, virus fayla düşmək üçün cəhd etdikdə antivirus tərəfindən bloklanır və bununla əlaqədar olaraq xəbərdarlıq edilir. Əlavə olaraq kompüterdə yoluxmuş fayllar, və əgər bu fayllar aktiv deyillərsə, onda onlar nəzərdən kənarda qalırlar.

–**Skaner rejimində** antivirus proqramı verilmiş sahədə bütün faylları yoxlayır və yoluxmanı kənarlaşdırır. Verilənlərin kompüterdə yoxlanılması müəyyən qədər vaxt aparır (bəzən bir neçə saat). Bununla yanaşı bəzi hallarda virus sistemə skan əməliyyatı tamamlandıqdan sonra da düşə bilər [3, 5].

Məsləhət olunur ki, sistemin etibarlı müdafiə edilməsi üçün hər iki rejimdən istifadə edilsin. Monitor rejimində antivirus proqramının daim işləməsi nəzərə alınmaqla yoxlamanı mütəmadi olaraq həftədə bir dəfə (bütün verilənləri yoxlamaqla), skaner rejimində isə yoxlamanı axşamlar həyata keçirmək tövsiyə edilir.

Antivirusun öz "qurbanları"nı necə aşkar etməsi üsullarından əsas ikisinə nəzər yetirək.

Siqnatura əsaslanan aşkaretmə. Əgər antivirus sistemə virusun soxulmasını aşkar edirsə, onda antivirus faylı nəzərdən keçirir, sonra isə məşhur 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.

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 xəbərdarlığa 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.

Ağ siyahı üsulu. Öncədən təhlükəsiz kod kimi administrator tərəfindən qeyd olunan kompüter kodları kombinasiyasının qabağı alınır (təhlükə yaratmayanlar nəzərə alınmır).

Evristik skanerə üsulu. Üsul siqnatura və evristikaya əsaslanır. Üsulun əsas məqsədi siqnaturdan istifadə etməklə skanerlərə 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 [2].

Hələ ki, viruslarla universal və etibarlı mübarizə vasitəsi yoxdur.

ƏDƏBİYYAT

1. Əlizadə M.N., Seyidzadə E.V., Salmanova M.Ə. İnformatika (Mövzular, suallar və testlər), Bakı, 2012,
2. Abbasov Ə.M., Əlizadə M.N., Seyidzadə E.V., Musayev İ.K. İnformatika və kompüterləşmənin əsasları. Yeni işlənmiş nəşri, Bakı: Poliqal, 2012, 932 s.
3. Rüstəmov Ə.M. İnformatika. Bakı, 2012, 522 s.
4. Rüstəmov Ə.M. İnformatika – izahlı terminlər lüğəti (Azərbaycanca, rusca və ingiliscə izahlı lüğət), Bakı, 2011, 568 s.
5. Kərimov S.Q., Həbibullayev S.B., İbrahimzadə T.İ. İnformatika. Dərslik, Bakı, 2011, 534 s.
6. Qurbanov İ.Ə., Qurbanov A.İ., Asadullayev R.A. İnformatika. Bakı, 2012, 420 s.
7. Advanced Encryption Standard (AES) Development Effort. February, 2001.
8. CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department of Defense System Evaluation Criteria in Specific Environments.
9. Datapro Reports on Information Security, vol. 1-3, 1990-1993.
10. DoD 5200.28-STD. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC) 1985.

AMEA Naxçıvan Bölməsi
E-mail: saadatmammadova1994@gmail.com

Saadat Mammadova

COMPUTER VIRUSES AND WAYS OF PROTECTION

The presented case provides a comprehensive overview of computer viruses, the largest and most dangerous enemy of modern computers, and a brief history of the origin of these viruses. It is shown that, after the creation of the Windows operating system and the increased use of the Internet, the fight against computer viruses becomes even more acute. Modern antivirus programs are being developed for this purpose. Currently, several companies around the world are developing antivirus software. It is noted, however, that there is still no universal and more reliable means of fighting computer viruses.

Keywords: *computer viruses, antivirus programs, malware (malicious software), Internet, mobile viruses.*

Саадат Мамедова

КОМПЬЮТЕРНЫЕ ВИРУСЫ И СПОСОБЫ ЗАЩИТЫ

Представленная статья содержит исчерпывающий обзор компьютерных вирусов, самого большого и самого опасного врага современных компьютеров, а также краткую историю происхождения этих вирусов. Показано, что после создания операционной системы Windows и более широкого использования Интернета борьба с компьютерными вирусами становится еще более острой. Для этого разрабатываются современные антивирусные программы. В настоящее время несколько компаний по всему миру разрабатывают антивирусное программное обеспечение. Однако отмечается, что до сих пор не существует универсальных и более надежных средств борьбы с компьютерными вирусами.

Ключевые слова: *компьютерные вирусы, антивирусные программы, вредоносные программное обеспечение, интернет, мобильные вирусы.*

(Riyaziyyat elmləri üzrə fəlsəfə doktoru Vüqar Salmanov tərəfindən təqdim edilmişdir)

Daxilolma tarixi: **İlkin variant** **07.04.2020**
Son variant **02.06.2020**