Шукан А.

Киберқылмыстар барысында қолданылатын зиянкес бағдарламалар мен вирус түрлерінің сипаттамасы

Мақалада қоғамдағы ақпараттық қауіпсіздікке қарсы шабуыл жасаушы бағдарламалар мен вирустардың түрлері көрсетілген. Олардың әрқайсысына сипаттама беріледі. Сонымен бірге әлемдегі ақпараттық желілерде жасалатын қылмыстарға жол ашушы, вирустық бағдарламаларға байланысты зерттеу жасаушы лабороторияларды есептері де келтірілген. Есептерде Қазақстанға қатысты мәліметтерге талдау жасалған. Мақала қазіргі кездегі заңтану ғылымындағы ең өзекті мәслелердің бірін қарастырады.

Түйін сөздер: ақпараттық желілер, зиянкес бағдарламалар, вирус түрлері, ақпараттық жүйе, киберқылмыстар.

Shukan A.

Descriptions of malware and viruses, which are made with the help of cybercrime

The article describes the types of viruses and programs that are used to attack information ofnetworks and systems. The characteristics of each of them are given here as well.However, laboratory researches presented in this article giving necessary information of spreading viral programsin the world. There is an analysis of the necessaryresearches for Kazakhstan. The author considers thatit is one of the most urgent problems of modern society.

Key words: information networks, malware, types of viruses, information system, cybercrime.

Шукан А.

Описания вредоносных программ и вирусов, с помощью которых совершаются киберпреступления

В статье дано описание программ и видов вирусов, используемых для атаки на информационные сети и системы. Дана характеристика каждой из них. Вместе с тем представлены данные исследований лаборатории о получивших распространение в мире вирусных программах. Имеется анализ необходимых сведений по Казахстану. Автор рассматривает одну из самых актуальных проблем современного общества.

Ключевые слова: информационные сети, вредоносные программы, типы вирусов, информационная система, киберпреступления.

ӘОЖ 34:002

Шукан А.

Қазақстан гуманитарлық заң университеті,
Қазақстан Республикасы, Астана қ.
E-mail: alia_shukan@mail.ru

КИБЕРҚЫЛМЫСТАР БАРЫСЫНДА ҚОЛДАНЫЛАТЫН ЗИЯНКЕС БАҒДАРЛАМАЛАР МЕН ВИРУС ТҮРЛЕРІНІҢ СИПАТТАМАСЫ

Ақпараттық технология саласындағы қылмыстарда басты назар аударатын жағдай оның аса жылдам дамуы мен тез түрленіп, өзгеруі болып табылады.

Киберқылмыскердің негізгі мақсаты да әр түрлі процестерді басқаратын, ақпараттық жүйе және онда таралатын ақпаратты алу болып табылады. Шын өмірдегі қарапайым қылмыскерге қарағанда киберқылмыскер дәстүрлі – суық қаруды және пистолет секілді қаруларды қолданбайды. Оның арсеналында – ақпараттық қару, желіге ену, бағдарламалық қамтамасыз етуді бұзу және модификациялау, ақпаратты рұқсатсыз алу және ақпараттық жүйенің жұмысын уақытша тоқтатуға қолданылатын барлық құралдар енеді. Киберқылмыскердің қаруына келесілерді кіргізуге болады: ақпараттық вирустар, бағдарламалық белгілер, ақпараттық жүйелерге рұқсатсыз кіруге мүмкіндік туғызатын шабуылдың әр түрі. Қазіргі заманғы ақпараттық қылмыскерлерде тек дәстүрлі құралдар ғана емес, сонымен қатар қазіргі ақпараттық қарулар және құралдар бар; бұл мәселе баяғыдан бері мемлекеттің шекарасынан өтіп халықаралық мәнге ие болды.

Әлемде ақпараттық технологиялар желісі адамзат өміріне тығыз кіріккен қазіргі уақытта, аталған құбылысты қылмыскерлер де өз пайдасына жаратуда. Сондықтан біз мақалада ақпараттық технологиялар саласындағы шабуылдар жасау барысында ең көп қолданылатын қару түрі зиянкес бағдарламалар немесе вирустар түрлеріне тоқталып өтуді жөн көрдік.

Зиянкес бағдарламалар – ақпараттық технология арқылы жасалатын шабуылдардың және қылмыстық әрекеттердің ең негізгі әрекет ету құралы болып есептеледі. Вирустар, құрттар және троя вирустары. Аталған зиянкес бағдарламаларды пайдалану арқылы қылмыскерлер логиндері, жеке есепшоттар туралы мәліметтерді немесе мемлекеттік әскери құпияларды ұрлау мүмкіндігіне ие болады [1].

Зиянкес бағдарламаларды төмендегідей түрлерге бөліп көрсетуге болады:

1. Трояндық бағдарламалар немесе троян аты (Trojans) – кез-келген қолданбалы бағдарламаның ішіне жасырын салып жіберетін зиянкес бағдарлама, бағдарламаны орнатқанда ол да компьютерге жасырын орнығып алып, өзінің мынадай

зымиян мақсаттарын іске асыра бастайды – ақпараттық технология құралдарына нақты зиян келтіру: құпия мәліметтерді ұрлау, бұзу немесе жою, ақпараттық технология құралдарын істен шығару немесе оны басқа зиянкестік мақсаттарда пайдалану.

2. Зомби (Zombie) – ақпараттық технология құралдарына интернеттен жұғатын вирус, ол бір ақпараттық құралдан екінші ақпараттық құралға вирустық және хакерлік шабуыл жасауға қолданады. Осы зомби-вирустар арқылы зиянкестер сіздің ақпараттық технология құралыңызды сырттан толық басқара алады, сөйтіп оны өздерінің дұшпандық мақсаттарында қолдануға дайындайды. Осы вирус жұққан зомби АТ құралдар үлкен желілерге бірігеді де, олардан бір мезгілде орасан зор спам хабарламалар, вирустар және зиянды бағдарламалар таратылады. Олардың бәрі бір сәтте, мысалы, бір банктің сервер-компьютеріне жіберілсе, сервер «булығып, тығындалып» істен шығады. Мұндай хакерлік шабуылды dDoS-шабуыл деп атайды.

3. Тыңшы бағдарламалар (Spyware) – ақпараттық технология құралына рұқсатсыз, жасырын келіп орналасып алатын бағдарлама, оның бірден-бір мақсаты АТ құралын толық өз басшылығына қаратып, үздіксіз аңдып, жеке құпия ақпараттарды ұрлау немесе жою. Бұл бағдарламалар ақпараттық технологиялар құралдарына көбіне желілік құрттар, трояндар немесе жарнамалық бағдарламалар (adware) арқылы кіріп алады.

4. Тыңшы бағдарламалар (фишинг) Фишинг (Phishing) – құпия қаржылық ақпаратты ұрлауға бағытталған пошта хабарламалары. Мұндай хатта интернет-банктің немесе басқа да қаржылық ұйымның ресми сайтының жалған көшірмесіне сілтеме орналасады. Қолданушы ол сілтемені басып, жалған сайтқа кіргенін білмейді, сондықтан алаяқтарға ойланбай өзінің паролін, кредит картасының нөмірін, есепшот нөмірін және т.б. жеке деректерін бере салады. Тыңшы бағдарламалар (фарминг) Фарминг – бұл фишингтің жасырын түрі. Қолданушы интернет-банктің немесе басқа коммерциялық ұйымның ресми сайтына кіруге әрекет жасаған кезде оны жалған сайтқа бағыттап жібереді, ал оның ресми сайттың айнымас көшірмесі екенін ажырату өте-өте қиын. Сол жерден енгізілген ақпараттың бәрін алаяқтар алып отыра береді. Алаяқтардың негізгі мақсаты жеке қаржылық құпия ақпараттарды ұрлау. Тек, жалған сайттардың қақпанына адамдарды алдап түсіру үшін алаяқтар электрондық поштадан басқа, әлдеқайда құйтырқы әдістерді қолданады.

5. Мобилді вирустар – ұялы телефондарға жұғатын вирустар. Олар SMS және MMS хабарламалар мен Bluetooth каналдары арқылы таралады. Бұл вирустардың да мақсаты ұялы телефон иесінің жеке құпия мәліметтерін ұрлау және пайдалану, бөтен телефондарға халықаралық және ақылы қоңыраулар соққызу немесе SMS, MMS-тер жөнелттіру арқылы пайда түсіру. Бұл вирустардың ең көп таралғандары: Cabir, Comwar, Brador, Viver.

6. Файлдық вирустар Файлдық вирустар әр түрлі жолдармен командалық файлдарға кіріп алады, олар орындалатын *.exe,*.com кеңейтілімдегі файлдар және осы файлдар іске қосылған кезде бірге белсенді күйге көшеді. зақымдаған файл орындала бастағаннан вирус та онымен бірге ақпараттық технология құралдары жадысына орналасып, сол жерден өзінің зиянкестік әрекеттерін іске асырады. Мысалы, басқа да файлдарға жұға береді. Ол тек компьютер өшкенде немесе операциялық жүйе қайта жүктелгенде ғана өзінен-өзі жойылып кетеді. Бірақ файлдық вирустар берілгендер файлын зақымдай алмайды.

7. Жүктемелі вирустар. Жүктемелі вирустар өзін-өзі қатты дисктің жүктеу секторына (нөлдік секторға) жазып қоя алады.

Операциялық жүйені ақпараттық технология жедел жадысына енгізгенде бұл вирустар сол жерге орналасып алады. Одан әрі жүктемелі вирустар да файлдық вирустар сияқты әрекет ете бастайды. Командалық файлдарға жұғып, олармен бірге қосылып, зиянкестік әрекеттерін жүзеге асырады, одан әрі қарай жұғады.

8. Макро вирустар Макро-вирустар Word құжаттары мен Excel электрондық кестелерін зақымдайды. Макро-вирустар деген сол офистік бағдарламаларда қолданылатын макрокомандалар арқылы жазылатын бағдарламалар (макростар). Зақымданған құжат өзі жасалған қолданбалы бағдарламада ашылған кезде макровирус компьютер жадына орналасып алады да, басқа да құжаттарға жұға береді. Жұғу қаупі тек офистік бағдарлама жабылғанда ғана тоқтайды.

9. Желілік вирустар – ақпараттық технология құралдары желісі арқылы таралады және файлдық сервер-мұрағаттардан файлдарды алған кезде жұғады. Желілік вирустардың электрондық пошта және интернет арқылы таралатын түрлері бар. Желілік вирустардың түрлері өте көп. «Пошталық» вирустар Интернет – құрттар Пошта хабарламаларына салынған файлдарда

болады. Сол файлдарды ашқан кезде компьютерге жұғады. Пошта хабарламаларына салынған файлдар арқылы ақпараттық технология құралдары желіде таралады. Скрипт – вирустар ақпараттық технология құралдарына интернеттен сайт беттерін браузер арқылы жүктеген кезде жұғатын зиянкес бағдарламалар. (Sophos ұйымы сонымен қатар интернеттегі зиянкес бағдарламалар көп жағдайда PDF форматында болатынын да ескерткен).

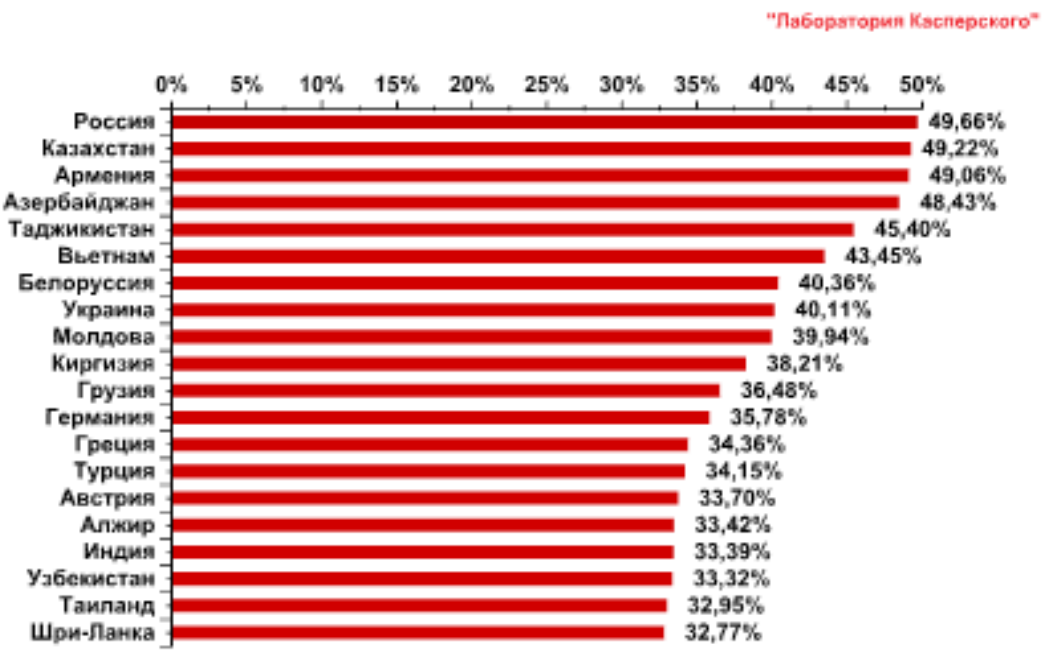
Зиянкес бағдарламалар индустриясы қарқынды даму үстінде. Мысалы, «Symantec» компаниясы 2013 жылдың сәуір айынан маусым айы аралығында 450 000 мың жаңа антивирус кодтарын ойластырғанына қарамастан, жаңа вирустар мен вирустар жұқтырған бағдарламалар санының күннен күнге артып бара жатқанын жариялаған [2].

Қазіргі кезеңде вирустардың таралуына басты және негізгі себебі интернет болып табылады. «Sophos» (1985 жылы Ұлыбританияда және АҚШ-та құрылған вирустардан және спам шабуылдардан қорғау, сүзу үшін құрылған халықаралық ұйым) мәліметтеріне қарағанда, интернет қолданушыларды компьютер немесе ақпараттық технология құралдарына вирустық шабуыл жасайтын сайттарға алдап шақыру әдісі нәтижесінде, көптеген вирустық шабуылдар іске асыруда. Олардың берген есебінен Қазақстандағы ақпараттық технология құралдарын пайдаланушылардың бұл шабуыл түрінен үлкен қауіп астында екендігін 2-кесте көруге болады.

2-кесте – 2014 жылдың бірінші жартысындағы интернет арқылы вирустық шабуылға ұшыраушы алғашқы 10 елдің тізімі

Мемлекеттердің атауы	Вирустық шабуылдардың пайыздық көрсеткіші
Азербайжан	56,29%
Қазақстан	55,62%
Армения	54,92%
Ресей	54,50%
Тәжікстан	53,54%
Вьетнам	50,34%
Молдавия	47,20%
Белоруссия	47,08%
Украина	45,66%
Қырғызстан	44,04%

Бұл келтірілген кестедегі мәліметтер 2014 жылдың бірінші жартысына «Sophos» антивирустық ұйымы берген мәліметтер болса, 2014 жылдың екінші жартысына жасалған талдау бойынша вирустық шабуыл бойынша «Kasper» анти вирустық ұйымының есебіне назар аударсақ (2-сурет).



2-сурет – 2014 жылдың екінші жартысында интернет арқылы белсенді вирустық шабуылға ұшыраушы алғашқы 10 елдің тізімі

«Sophos» ұйымы берген келесі мәліметке назар аударсақ, әлемдегі вирус жұқтырудан алғашқы орындағы мемлекеттер болып соңғы екі жылда мына елдер есептеледі: Үндістан (59,2%), Қытай (46,7%), Қазақстан (46%), Азербайжан (44,1%), Ресей (41,5%) [49].

Жоғарыдағы келтірілген ресми мәліметтерден біз, ақпараттық технология құралдарын оның желісі мен жүйесін пайдаланушы Қазақстанның мемлекеттік мекемелері, банктік жүйесі, жеке тұлғалардың барлығына үлкен вирустық шабуыл қаупі туып тұрғандығын байқаймыз. Себебі вирустық бағдарламалар арқылы барлық мәліметтер ұрланады, өзгертіледі, өшіріледі, жарияланады. Сондықтан отандық заңгерлер мен құқықтанушылар бұл мәселеге аса назар аударуы қажет. Себебі вирустық шабуылдар арқылы жасалатын алаяқтық, ұрлық сияқты заңға қайшы әрекеттер классикалық жолмен жасалатын алаяқтық пен ұрлықтан гөрі орасан зор зардаптарға әкелетіні белгілі жағдай. Мәселен, 2014 ж. мәліметтер бойынша вирустық шабуылдардан келген шығын 92 млн доллар болған [3].

Қазақстан заңнамасына вирустық шабуылдарға байланысты заң нормаларын қайта қарастыру қажет. Жоғарыда берілген антивирустық ұйымдар есептерінде көрсетілген фактілер казақстандық электрондық ресурстардың аса үлкен қауіп астында екенін айқын көрсетеді. Әрі вирустық шабуылдардан келетін шығын да орасан зор болуы мүмкін. Сондықтан берілетін жаза аса қатал болуы қажет. Сонымен қатар вирустық шабуылдардың шетелдік сайттар арқылы жасалуы заңгерлердің ұлттық заңнаманы ғана емес аталған салаға қатысты халықаралық заңнамаларды қарастыру қажеттігін көрсетеді. Сонымен қатар вирустық шабуылдар мен спам шабуылдардың шетелдік сайттар арқылы келетінін ескерсек, Қазақстанға Еуропа Киберқылмысқа қарсы Қауіпсіздік Конвенция (Халықаралық және Еуропалық киберқылмыстармен күрес Конвенциясы. Будапешт, 23 қараша 2001 жылы қабылданды. Аталған конвенция әлемдік деңгейде ақпараттық технология саласындағы қылмыстармен күресумен айналысады) заңдарын ратификациялау мәселесін қарастыру қажет деп есептейміз. Қазір бұл мәселе соншалықты қауіпті көрінбесе де алдағы уақытта елімізді орасан шығынға ұшыратуы әбден мүмкін деп есептеймін.

Әдебиеттер

1 Мехмет Ниязи. Интернет қылмыстар және жеке өмір құқығының бұзылуы. – Анкара, 2013. – 7 б.
2 Бекназаров А. Ақпараттық қауіп туралы есеп. 2103. https:// www. securelist
3 Касперский фирмасының ақпараттық қауіпсіздікке байланысты есебі. 2013.http://ria.ru/Kaspersky_Equation_Group_17022015

References

1 Mehmet Niyazi. Internet criminal violation of the right to life and personal. – Ankara, 2013. – 7 p.
2 A. Beknazarov. The report on the threat information. 2103. https:// www. securelist.
3 Report related to information security firm Kaspersky72013.http://ria.ru/Kaspersky_Equation_Group_17022015