DOI:10.26104/IVK.2023.45.557

ИЗВЕСТИЯ ВУЗОВ КЫРГЫЗСТАНА, № 1, 2023

Турдубаева Ж.А., Сайдаматов Ш.М.

МААЛЫМАТ КООПСУЗДУГУНДАГЫ ВИРУСТАР ЖАНА АНТИВИРУСТУК ПРОГРАММАЛАР

Турдубаева Ж.А., Сайдаматов Ш.М.

ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Zh. Turdubaeva, Sh. Saidamatov

VIRUSES AND ANTI-VIRUS PROGRAMS IN INFORMATION SECURITY

УДК: 004.49:738.5

Азыркы шарттарда компьютердик тармактар, программалоо жана интернет тармагындагы технологиялардын тынымсыз өнүгүүсүндө прогресстин караңгы тарабы да өсүүнү токтотпойт: вирустук программалык камсыздоо. Жөнөкөй колдонуучулар компьютер иштеткенде такыр көңүл бурушпайт, ал тургай антивирустук программалар да орнотулбаганын билишпейт. Ошондуктан, вирустарга каршы күрөштүн бардык аспектилерин изилдөө керек: жугуунун алдын алуу, зыяндуу программаларды аныктоо ыкмалары, аларды жок кылуу, ошондой эле кесепеттерди жоюу. Компьютердик вирустар менен күрөшүү боюнча жетиштүү билимге ээ болгондор, бул тармакта билими жок колдонуучуларга эффективдүү маалымат берүүгө жана компьютердик дүйнөдө да кездешүүчү вирустун чыгышынан сактануугa болот. Бул үчүн биз бул тема боюнча негизги илимий булактарды жана статистикалык маалыматтарды изилдөө жүргүздүк. Натыйжада, бул макалада вирустар жөнүндө негизги түшүнүктөр берилген жана алардын классификациясы, аныктоо жана жок кылуу ыкмалары көрсөтүлөт.

Негизги сөздөр: *вирустар, антивирустар, интернет, компьютерлер, компьютердик тармактар, операциондук система, коопсуздук, маалыматтык коопсуздук, браузерлер, глобалдык тармактар.*

В нынешних условиях беспрерывного развития технологий в области программирования, компьютерных сетей и сети Интернет не перестает расти и темная сторона прогресса: вирусное программное обеспечение. Рядовые пользователи зачастую не обращают внимания, когда они попадают на их компьютеры, и даже не имеют установленных антивирусных программ. Следовательно, необходимо исследовать все аспекты борьбы с вирусами: предотвращение заражения, методы обнаружения вредоносных программ, их уничтожение, а также ликвидация последствий. При достаточном объеме знаний о том, как сражаться с компьютерными вирусами, станет возможно эффективно информировать пользователей, не разбирающихся в данной сфере, и избегать вспышек вирусов, которые происходят и в компьютерном мире. Для этого мы провели исследование основных научных источников по данной тематике и статистических данных. Как итог, в данной работе даются основные представления о вирусах и проводится анализ методов их классификации, обнаружения и уничтожения.

Ключевые слова: *вирусы, антивирусы, интернет, компьютеры, компьютерные сети, операционная система, безопасность, информационная безопасность, браузеры, глобальные сети.*

It is an open secret that no technology can be evolved without its dark side and all the disadvantages bring developed too. That is precisely why computer viruses are not surprising to anybody. However, it is genuinely astonishing that there are still a lot of people worldwide who are not aware of this dangerous phenomenon. They tend not to have anti-virus software installed and regard their computer malfunctions as something ordinary without any alarm. Therefore, our goal is to reconsider both methods of viruses' classification, detection, annihilation and how anti-virus software works itself. With that task completed, we have made a relatively recent and relevant analysis to help average computer users understand what a computer virus is and how to fight it.

Key words: *viruses, anti-viruses, internet, computers, computer networks, security, information security, software, browsers, global networks.*

Компьютерлер пайда болгондон убактан бери ушул күнгө чейин компьютерлердин иштөөсүндөгү маалыматтын бузулууларынын, анын ичинде жашыруун маалыматтардын сыртка чыгып кетишинин негизги себептеринин бири вирустар болуп саналат. Ошол эле учурда компьютердик вирустар эволюцияга жана көптөгөн жаңы формаларга ээ болууга жетишти.

Анткен менен антивирустук программалардын эволюциясы токтобойт. Зыяндуу аракеттерди аныктоо жана алдын алуу ыкмалары өнүгүп келе жатат. Вирустар менен иштөөдөн тышкары кеңири функцияларды камсыз кылган көпчүлүк программалардын акы төлөнүүчү версиялары да бар: мисалы, брандмауэр, VPN ж.б.

Бардык артыкчылыктарга карабастан, учурдагы коопсуздук программалар көптөгөн кемчиликтерге ээ. Натыйжада, вирустук программалар менен күрөшүү маселеси ачык бойдон калууда.

Компьютердик вирустарды аныктоо ыкмалары. Вирус менен күрөшүүнүн жана андан кийин компьютерди калыбына келтирүүнүн биринчи кадамы, албетте, бул зыяндуу программаны аныктоо. Кээ бир учурларда бул жөнөкөй эле иш болуп саналат, колдонуучу компьютери вируска кабылганын түшүнүүсү зарыл. Мисалы, интернет-браузер айрым веб-сайттарга кире албай калышы мүмкүн, башкы бет дайыма өзгөрүп турат же браузердин өзү адаттагыдан жайыраак иштеп калат. Ошондой эле, колдонуучулар көбүнчө төмөнкү белгилерди байкашат:

- Жай иштөө же компьютер катып калуу.
- Иш тактада же браузерде дайыма калкып чыкма эскертүүлөр.
- Компьютер күтүлбөгөн жерден өчүп күйөт.
- Тутум файлдары бузулуп ачылбай калышы.

DOI:10.26104/IVK.2023.45.557

Бирок, операциялык тутумдун же браузердин иштөөсүндөгү каталар анчалык деле ачык-айкын эмес жана колдонуучу өзүнө керектүү бардык иштерди тынч аткарган учурлар да болот, бирок компьютерде вирустар бар. Ошондуктан мезгил-мезгили менен бардык мазмунду вирустарды, аныктоо ыкмаларын колдонгон антивирустук программалар менен сканерлеп туруу зарыл.

Аларды эки негизги топко бөлүүгө болот [1]:

1. Вирустарды «сөздүк» аркылуу аныктоо - бул абдан жөнөкөй жолу. Антивирус жөн гана бардык файлдарды жана программаларды сканерлейт жана аларды учурдагы вирустарды камтыган сөздүк менен салыштырат. Эгерде салыштыруу учурда дал келүү болсо, антивирус зыянкечти жок кылат же карантинге салат. Албетте, бул ыкма өз милдетин аткаруу үчүн, сөздүктү жаңылоо жана ага жаңы зыяндуу программаларды кошуу керек. Бүгүнкү күндө алардын саны абдан көп болгондуктан, бардык вирустар сиздин антивирусуңуздун сөздүгүнө кирбейт. Бирок көпчүлүк учурда бул жетиштүү, анткени көпчүлүк антивирустар аныктоо үчүн сөздүк ыкмасын колдонушат.

2. Программалардын жүрүм-туруму боюнча вирустарды аныктоо. Бул принципте иштеген антивирустар программалар кандай иш алып барарын жана кандай аракеттерди аткарарын көзөмөлдөп турушат. Негизинен, программалардын бардык шектүү иш-аракеттери аткарылуучу файлга жаңы маалыматтарды жазуудан келип чыккан, бирок азыр кадимки программалар көп учурда ушундай кылышат. Натыйжада, антивирус зыянсыз файлды зыяндуу деп кайра ката кетиргенде, колдонуучу көптөгөн жалган эскертүүлөрдү алат. Бул ыкма азыраак колдонулуп жатканы таң калыштуу эмес.

Компьютердик вирустардын классификациясы

Зыяндуулугу боюнча	Зыянсыз – мындай программалар жөн гана тармакка жайылып, бир компьютерден экинчисине өтүүгө жөндөмдүү, бирок системага карата эч кандай кыйратуучу функцияларды аткарбайт [3]. • Жумшак - компьютердин эс тутумун ашыкча жүктөй турган үндөрдү, сүрөттөрдү жаратуучу зыяндуу программалар. • Коркунучтуу - системага зыян келтире турган программалар. • Өтө коркунучтуу – эс тутумдун ар кандай сегменттеринде жана секторлорунда жайгашкан маалыматтарды жок кыла турган вирустар, ПКдин механикалык бөлүктөрүнүн бузулушуна алып келет.
Жашоо чөйрөсү боюнча	Файл - аткарылуучу файлдардын бузулушу, жашоо чөйрөсү тиешелүүлүгүнө жараша COM жана EXE файлдары болуп саналат [3]. • Жүктөө - катуу дисктердин жүктөө секторлоруна же жүктөөчү секторлорго зыян. • Тармак - компьютердик тармактардын жана системалардын бузулушу. • Макро - Microsoft Office файлдарынын женилүүсү.
Жугуу ыкмасы боюнча	Резиденттик вирустар – бул вирус жуккан программа аткарылгандан кийин оперативдүү эсте кала турган вирустар. Кайта жүктөгөндөн кийин системалар аппараттан өчүрүлөт, эгерде программанын коду autorun функциясын камтыбаса, бул шартта система кайра жуктуруп алат [4]. • Резиденттик эмес вирустар – аппараттын оперативдик эс тутумун ээлебеген жана вирустук программанын аткарылышы учурунда бир гана жолу аткарылуучу вирустар.

Ошондой эле, иштеп жаткан программанын кодунун кичинекей бөлүгүн туураган же операциялык системаны [4] тууроочу жана андан кийин гана андагы программаны аткарган антивирустардын иштөө принцибине программанын жүрүм-туруму боюнча аныктоо ыкмасы. Мындай текшерүү өтө көп убакыт талап кылынышы мүмкүн, ошондуктан аны жөнөкөй компьютер колдонуучулар эмес, адистер колдонушат. Бирок бул чындыгында эффективдүү жана компьютерлерди ээлеген бардык вирустарды аныктай алат.

Антивирус программалары. Вирустарды аныктоо ыкмалары жөнүндө сөз кылып жатып, албетте, зыянкечтерге каршы күрөшүүнүн негизги каражаты антивирустук программалар экенин айтып өттүк. Алар колдонуучуга керектүү нерселердин бардыгын бириктирет: алар вирусту табышат, аны жок кылышат жана маалыматтар же башка программалар бузулган болсо, анын кесепеттерин жок кылышат. Ошол эле учурда антивирустук программалык камсыздоону дагы эле бир аз башкача функцияга ээ болгон бир нече түргө бөлүүгө болот [5]:

• Детекторлор. Булар жогоруда айтылган антивирустар гана. Алар көйгөйдү таап, сөздүк ыкмасын колдонуп, аны «дарылайт». Бул түргө белгилүү Doctor Web, Kaspersky антивирустары кирет.

• Фильтрлер. Мындай антивирустар дискти көзөмөлдөйт. Кандайдыр бир программа ага жазылууга аракет кылганда, чыпка колдонуучуга бул тууралуу кабарлап, андан операцияны аткарууга уруксат сурайт. Ошентип, жаңы белгисиз вирустар менен күрөшүүгө болот, эгерде алар, албетте, BIOS менен эмес, диск менен иштешсе [6].

• Вакцинаторлор. Антивирустун бул түрү белгилүү зыяндуу программалар менен күрөшүү үчүн гана колдонулат, анткени эмдөөчү вирустун белгилерин кабыл алышы керек. Андан кийин аларды колдонуучунун коопсуз программасына жазат жана вирус буга чейин жуккан деп ойлойт.

• Аудиторлор. Аудиторлор программалардын жана файлдардын абалы жөнүндө маалыматты сакташат

DOI:10.26104/IVK.2023.45.557

жана кайра сканерлөөдө аларды өзгөртүүлөрдү салыштыруу жана талдоо үчүн колдонушат. Файлдардын өлчөмүнөн жана алар түзүлгөн убакыттан баштап BOOT секторунун абалына чейинки факторлор текшерилет [7].

Ар кандай функционалдуу жана иштөө принциптери менен антивирустардын көптөгөн түрлөрү бар экендигине, ошондой эле бул программалык камсыздоону иштеп чыгуучулардын чоң реестрине карабастан, антивирустар, тилекке каршы, көптөгөн кемчиликтерге ээ. Ошентсе да, эч бир антивирус программасы кандайдыр бир вирустан 100% коргоону кепилдей албайт. Бул сөздүктөрдө жазыла элек жаңы белгисиз вирус же катуу шифрленген вирус болушу мүмкүн. Анда күчтүү Unpacker керек, ал албетте көптөгөн антивирустарда жок.

Мындан тышкары, антивирустар таптакыр коопсуз файлдардан коркунучту тапканды жакшы көрүшөт. Ошондуктан, жөнөкөй колдонуучулар өздөрү вирустар жана зыяндуу файлдар жөнүндөгү эскертүүлөрдү эске алышпайт, бул коргоону ишенимсиз кылат.

2017-жылы Google, Mozilla, Cloudflare жана бир нече университеттердин өкүлдөрү антивирустар жана тармактык фильтрлер менен HTTPS трафикти кармоо процесстерин кескин сынга алышкан. Изилдөөнүн аркасында антивирустук программалар менен HTTPS трафикти тармактык кармап калуу колдонуучулардын коопсуздугуна жана алардын дүйнөлүк желеге туташууларына коркунуч туудурушу мүмкүн экени аныкталган.

Эреже катары, бул программалык камсыздоо HTTPS пакеттерине кире албайт, бирок антивирустук компаниялар шифрленген байланыштар аркылуу өткөн маалыматтарды талдоо ыкмасын табышты: алар колдонуучунун түзмөгүнө өздөрүнүн түпкү сертификаттарын орното башташты, бул туташуунун коопсуздугун бир топ төмөндөтөт. Андан тышкары, талдоо көрсөткөндөй, кээ бир антивирустарда берилген трафик сканерлери, алардын кемчиликтеринен улам, дагы көп аялуу жактары бар. Кармалып калган байланыштар начар криптографиялык алгоритмдерди колдонушат жана мурда бузулган шифрлерди колдонушат, алар түзмөктөргө чабуул коюуга жана байланыштын шифрин чечүүгө мүмкүндүк берет. Ошентип, трафиктин кеминде 10% антивирустар гана эмес, аны колдонгон үчүнчү тараптын программалык камсыздоолору тарабынан да кармалат, аны өз максаттары үчүн оңой чечмелейт жана талдайт. Ошондуктан антивирустук компаниялар маалыматты чогултуунун жаңы ыкмасы жөнүндө ойлонушу керек.

Бирок көйгөйдүн жарымы гана HTTPS пакеттерин кармоо колдонуучунун жана анын тармактагы маалыматтарынын коопсуздугун азайтат. Дагы бир маселе - тармакты уурдоо канчалык кеңири таралган.

Кармоолордун санын өлчөө оңой иш эмес, андыктан TLS манжа изин чыгаруу технологиясынын өркүндөтүлгөн версиясы кармап алууну аныктоо үчүн колдонулат. Ошентип, ким байланышты түзөрү аныкталат: тосмо же браузер. Технология кардар TLS пакетинин дизайнын баалайт (негизинен шифрдик пакеттер жана TLS опциялары) жана аны белгилүү болгон маалыматтар базасы менен салыштырат.

Интернет-дүкөндүн, Cloudflare сайтынын жана Firefox жаңыртуу серверлеринин иш процесстери бааланды. Алар канча серепчи трафигин кармап жаткандын карап көрөлү. Ал эми натыйжалар, өз кезегинде, трафиктин 4% дан 10%га чейин кармалып турганын көрсөттү, анын 4% Firefox серверлери жана 10% Cloudfare. Бул көп, бирок кээ бир бөгөт коюулар кол салгандар тарабынан аткарылбай турганын эстен чыгарбоо керек.

Эгерде биз кармалган HTTPS пакеттерин операциялык тутум боюнча бөлсөк, алар MacOS же Linuxка караганда Windowstан алда канча көп кармалат экен. Мобилдик түзмөктөрдөн (Android жана IOS) трафик азыраак кармалат,

Азыркы учурда, бул HTTPS трафикти кармоо маселесин убактылуу чечүү мүмкүн болгон маневрлердин бири. Бирок маневрдин минусу, аны кармоону баштаган антивирус эмес, сервердин ээси жана сурал-ган интернет-ресурс камсыз кылат. Ар бир сайттын муну жасоо мүмкүнчүлүгү жок. Ошентип, биз тармактык бөгөт коюучулар тарабынан колдонуучуга келтирилген зыяндын масштабын так аныктай алабыз жана аны бир аз гана жок кыла алабыз, анткени бардыгы көптөгөн факторлордон көз каранды: колдонулган программалык камсыздоо жана байланыштар, сурал-ган сайт, колдонуучунун аппараты жана ага OS. Бирок, ошол эле учурда, антивирус сатуучулар HTTPS трафигин башкаруунун азыраак аялуу ыкмасына өтмөйүнчө, мындан качуу таптакыр мүмкүн эмес.

Корутунду. Жыйынтыктап айтканда, дүйнөдө канчалаган көп сандагы вирустар бар жана ар бир мүнөт сайын жаны түзүлүп жатканын, ошондой эле алар компьютер колдонуучуларына, интернетке кандай зыян алып келерин байкабай коюу мүмкүн эмес. Антивирустук программалар толугу менен болбосо да, зыяндын алдын алат же кесепеттерин жок кыла алат. Ошондуктан, колдонуучулар антивирустарды да, бейтааныш файлдарды жана шилтемелерди да туура колдонууну үйрөнүшү керек - каалаган убакта алар зыяндуу болуп чыгышы мүмкүн.

Мындан тышкары, антивирустук программалык камсыздоону иштеп чыгуучулардын да үстүндө иштей турган нерсеси бар. Бул макаладагы мисалдардан жана жеке тажрыйбадан көрүнүп тургандай, компьютерде вирустарды аныктоо жана жок кылуу ыкмалары идеалдуу эмес. Ал эми кесепеттүү программанын жа-

DOI:10.26104/IVK.2023.45.557

ратуучулары коду жана шифрлөөнү тынымсыз өркүндөтүп, бир жерде отурушпайт. Вирустардын жана антивирустардын эффективдүүлүгү үчүн ушундай жарышта колдонуучулар өздөрүнүн коопсуздугун камсыз кылуу үчүн ар кандай программаларды колдонууну үйрөнүшү керек.

Адабияттар:

1. Курилов Ф.М. Оптимизационный метод проведения сравнительного анализа средств защиты информации от несанкционированного доступа. // Технические науки: проблемы и перспективы: материалы III Междунар. науч. конф. - СПб.: Свое издательство, 2015. - 40-44.
2. Власов Д.В., Минаев А.С. Методы противодействия анализу исполняемых файлов в информационных системах. // Информация и безопасность. 2014. - 17(2). – 308-311.
3. Иванов В.Ю., Жигалов К.Ю. Методика обнаружения следов вредоносного программного обеспечения в дампах оперативной памяти. // Cloud of science. 2018. - 5(2). 2-5.
4. Рудниченко А.К., Шаханова М.В. Актуальные способы внедрения компьютерных вирусов в информационные системы. // Молодой ученый. 2016. - (11). – 221-223.
5. Кияев В.И. Безопасность информационных систем. // М.: Открытый Университет «ИНТУИТ»; 2016. – 192