УДК 004

БОРЬБА С КОМПЬЮТЕРНЫМИ ВИРУСАМИ И СПОСОБЫ ИХ ОБНАРУЖЕНИЯ

Журавлева В.В.
студент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Ткаченко А.Л.
к.т.н., доцент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Аннотация

В связи с почти полной зависимостью от электроники стало критически необходимо ее защищать от вредоносных программ. Человечество успешно справляется с этой задачей в настоящее время. Несмотря на все то, что было разработано, чтобы защитить личную информацию, она все равно остается в опасности, так как с каждым днем злоумышленники пытаются всеми силами добиться своей цели. Таким образом важно знать, чему противостоит человек и как бороться с этим, чтобы не стать жертвой такого неприятеля как компьютерный вирус.

Ключевые слова: программное обеспечение, компьютерный вирус, операционная система, Интернет, фишинг, мошенничество.

FIGHTING COMPUTER VIRUSES AND WAYS TO DETECT THEM

Zhuravleva V.V.
student,
Kaluga State University named after K. E. Tsiolkovsky,

Kaluga, Russia

Tkachenko A.L.
candidate of Technical Sciences,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Abstract

Due to the almost complete dependence on electronics, it has become critically necessary to protect it from malware. Humanity is successfully coping with this task at the present time. Despite all that has been developed to protect personal information, it still remains in danger, as every day attackers are trying their best to achieve their goal. Thus, it is important to know what a person is up against and how to deal with it, so as not to become a victim of such an enemy as a computer virus.

Keywords: software, computer virus, operating system, internet, phishing, fraud.

В мире высоких технологий человечество с развитием старого и созданием нового не успевает за прогрессом. Сложно стало определить, что нам действительно необходимо или чего нам стоит опасаться. Не так давно стали развиваться и вредоносные технологии такие, как компьютерные вирусы. Их количество и множество их вариаций растет очень быстро. Но с каждым новым вирусом создается антивирус. Но так как прогресс не стоит на месте вирусы эволюционируют, а система защиты устаревает. В 21 веке информационные технологии вышли на новый уровень развития, поэтому очень важно знать о том, как защитить себя и свою электронику [1-3].

Компьютерный вирус представляет собой программу, которая за счет встроенной системы способна поражать «здоровые» участки нашей компьютерной системы. Он способен внедряться во флэш-накопители, жесткий диск, через электронную почту, web-страницы, Интернет.

Существует множество источников, где предупреждают пользователей о незаконных способах внедрения в технику через различные скачиваемые программы или фотографии, а также странные сообщения с использованием фишинга. Но, как бы то ни было, очень трудно найти подделку там, где не ожидаешь ее увидеть. Мало быть бдительным человеком, важно понимать, как бороться с мошенничеством [4, 6].

Существует определенная классификация вирусов, различающихся по особенностям территориального размножения и своей физической характеристике. В настоящее время основным источником вирусов является Интернет и локальные сети. Компьютерные вирусы были неформально разделены на такие категории как:

1. По поражаемому сектору (файловые, сценарные вирусы, макровирусы);
2. По пораженной ОС (операционной системе) (Windows, Linux);
3. По языку программирования, с помощью которого был создан (ассемблер, сценарный язык) и др.

Согласно историческим данным первым вирусом считается вирус с незамысловатым названием «Brain», который был создан в 80-х годах 20 века. Этот вирус способствовал лишь отслеживанию копий пиратских ПО (программного обеспечения). Такого типа вирус не был способен причинять вред, а вот современный вирус способен украсть личную информацию, деньги, а также просто сломать технику.

За несколько лет в 21 веке было создано много вирусов, многие из них имели ошеломляющий успех для своего создателя, а некоторые стали настолько бесполезными, что уже и не пользуются большой популярностью.

В 2008 году была создана программа Conficker, которая была написана на языке программирования C++ в Microsoft Visual Studio. Целью данной программы было заражение через недостатки в ПО. Вирус отключает службы Windows (автоматическое обновление, систему безопасности и защиты) и в том числе доступ к сайтам, производящим антивирусы. За счет своего алгоритма

червь проводит генерирование сайтов, где находит файл с кодом, который впоследствии при успешной сверке может его выполнить. Свой успех программа получила за счет удаленной от сервера системы P2P. Данный вирус опасен даже сейчас.

Для того, чтобы не попасть в пропасть вируса Conficker необходимо вовремя устанавливать актуальные системы защиты. Так же существуют программы, которые способны провести поиск троянов и удалить их, например AVZ. Утилита способна используя свой код сканировать вашу систему и удалить поврежденные файлы. Очень важно так же сменить все пароли ко всем социальным сетям. Помимо антивируса для компьютера, существуют и утилиты, которые проверяют на вредоносность сайты и скачиваемые файлы (Oupost Firewall).

В 2007 году был распространен вирус Storm Worm. Также ополчившийся на ОС Windows. Данный вирус проживает в основном в электронной почте в сообщениях с заголовком «230 убитых как нападающие в Европе» и другими подобными. Программа с помощью встроенного кода способна после открытия письма взломать социальную сеть для рассылки спама и личной информации.

После открытия файла устанавливается служба wincom32. Обнаружить данную рассылку было сложно, так как каждые несколько минут менялся Ip-адрес сервера управления и пакетный код. Имя файла заражения **msagent.exe.** Такого типа файлы удаляются различными утилитами, в настоящее время в основном нет проблем с данным вирусом.

В 2004 году началась эпидемия вируса Mydoom. Это почтовый червь, который рассылает сообщения с темой «Тест», «Ошибка», «Доставка…» и т. д. Когда пользователь открывал ссылку, приложенную к письму, он давал доступ к адресной книге. Через некоторое время снижается скорость Интернета примерно на 10%. Через некоторое время появляется модификация Mydoom, в которой блокируется доступ к некоторым сайтам.

В 2023 году вирусы стали намного опасней. Появились новые пути вторжения в систему пользователя. Пример может стать программа Clop. Такая программа способна за считанные минуты зашифровать данные, а затем пользователю приходит уведомление о выкупе этих данных. Программу найти очень трудно. Каждой жертве индивидуальное нападение. Предвидеть, как будут проводить мошенничество очень трудно. Нужно следить за открываемыми ссылками и скачанными файлами [5, 7].

Примеров вирусов очень много. За всю богатую историю борьбы с вирусами человечество придумало множество способов противостояния им. Каждому вирусу был создан свой антивирус или его дополнения.

Обнаружить факт нападения достаточно просто. В основном заподозрить внедрение в компьютерную систему можно по внешним признакам, которые в обычное время не проявлялись, это: всплывающие окна, медленная работа компьютера, шум жесткого диска, пропажа файлов, постоянная потеря соединения или высокий трафик, неподдерживаемая многозадачность.

Перед тем как поднимать панику важно сканировать устройство. Скан позволит определить наличие вирусов. Подойдет практически любой скан в антивирусе. Предварительно важно сделать копию необходимого, так как это важно для сохранения востребованных файлов. Как только сканирование завершиться антивирусная программа предложит удалить вредоносные программы.

Бывают моменты, когда вирусы могут повлиять на ОС и вовсе отказать в запуске устройства. В таком случае используют метод аварийного USB. Для данной операции необходимо наличие дополнительного компьютера, через который возможно подключить и установить программу.

Самый распространенный метод, к которому прибегает каждый в критический момент – это переустановка системы, то есть полное удаление и возвращение к режиму по умолчанию.

Количество способов борьбы с вирусами растёт параллельно с их числом. Кажется, что мы все защищены достаточно, но это ошибочное мнение. Используя свое умение чувствовать человека и, способность творчески подходить к ситуации мошенники могут воспользоваться слабыми местами любого и поймать невинного в ловушку. Очень важно быть заранее подготовленным к любой ситуации, хотя бы на теоретическом уровне, чтобы не растеряться в критичный момент.

Библиографический список:

1. Иванец, М. Э. Анализ угроз информационной безопасности для коммерческой организации / М. Э. Иванец, А. Л. Ткаченко // Цифровая трансформация промышленности: тенденции и перспективы: Сборник научных трудов по материалам 2-й Всероссийской научно-практической конференции, Москва, 11 ноября 2021 года. – Москва: Общество с ограниченной ответственностью "Русайнс", 2022. – С. 364–370. – EDN RWMZDO.
2. Кондрашова, Н. Г. Экономическая безопасность и ее обеспечение в коммерческой организации / Н. Г. Кондрашова // Modern Economy Success. – 2021. – № 1. – С. 207-212. – EDN LKEBGG.
3. Ткаченко, А. Л. Анализ проблем защиты организации от межсетевых атак / А. Л. Ткаченко, В. В. Бурцева, В. И. Кузнецова // Дневник науки. – 2021. – № 8(56). – EDN PYEENM.
4. Захаров, П. Г. Оценка и направления улучшения системы менеджмента бизнес-процессов коммерческой организации / П. Г. Захаров, А. А. Мигел // Modern Economy Success. – 2020. – № 2. – С. 197-204. – EDN JVTAKC.
5. Ткаченко, А. Л. Анализ эффективности защиты персональных данных и проблема cookie файлов / А. Л. Ткаченко, Е. С. Сафронов, В. И. Кузнецова // Дневник науки. – 2021. – № 6(54). – EDN KIHHDT.

6. Панкова, А. С. Управление персоналом в современной организации с учётом цифровизации и интернет-технологий / А. С. Панкова, Н. Ю. Чаусов // Вектор экономики. – 2022. – № 6(72). – DOI 10.51691/2500-3666_2022_6_12. – EDN ELKMPM.
7. Кондрашова, Н. Г. Выявление внутренних угроз экономической безопасности на региональном уровне / Н. Г. Кондрашова // Russian Economic Bulletin. – 2021. – Т. 4. – № 4. – С. 300-305. – EDN TEUDRK.

Оригинальность 76%