УДК 004

Колосова Д. Е.

студентка

Научный руководитель: Гурова Е. А. ст. пр.

ФГБОУ ВО «Армавирский государственный педагогический университет», г. Армавир.

КОМПЬЮТЕРНЫЕ ВИРУСЫ И КАК ОТ НИХ ЗАЩИТИТЬСЯ

Аннотация: в данной статье рассмотрены основные типы компьютерных вирусов и способы защиты от них. В век компьютерных технологий подавляющее большинство людей являются пользователями компьютера. В связи с этим можно говорить о необходимости приватности данной информации и защите ее от компьютерных вирусов.

Ключевые слова: ПК, компьютерные вирусы, Интернет, безопасность данных.

Kolosova D. E.

student

Supervisor: Gurova E. A. Art. pr.

FSBEI HE "Armavir State Pedagogical University", Armavir.

COMPUTER VIRUSES AND HOW TO PROTECT FROM THEM

Annotation: this article discusses the main types of computer viruses and how to protect against them. In the age of computer technology, the vast majority of people are computer users. In this regard, we can talk about the need for the privacy of this information and its protection from computer viruses.

Key words: personal computer, computer viruses, Internet, data security.

Компьютерный вирус - это программа или фрагмент кода, предназначенный для повреждения вашего компьютера путем повреждения системных файлов, растраты ресурсов, уничтожения данных или других неприятностей [1].

Вирусы уникальны от других форм вредоносных программ тем, что они самовоспроизводятся - способны копировать себя через файлы или другие компьютеры без согласия пользователя.

В принципе, они действительно заразны.

Список различных типов компьютерных вирусов, которые в настоящее время существуют:

1) Вирус загрузочного сектора. Сектор загрузки - это часть жесткого диска вашего ПК, которая загружает операционную систему вашего компьютера, такую как Microsoft Windows. Вирус загрузочного сектора заражает главную загрузочную запись (MBR), поэтому вирус загружается на память компьютера во время запуска [2].

Вирусы загрузочного сектора раньше распространялись в основном через подключаемые устройства, такие как USB-ключи, дискеты и компакт-диски. По мере развития технологий вирусы загрузочного сектора стали гораздо реже, и в наши дни они в основном живут как вложения электронной почты.

2) Вирус прямого действия. Эти вирусы предназначены для «прохода» через ваш компьютер: они попадают внутрь, как правило, распространяются по файлам определенного типа (файлы COM или EXE), и когда они сделают свое дело, они удаляются сами. Это самый распространенный тип вирусов, и его легче всего создать, что также делает их самыми простыми для избавления.

Примеры вирусов прямого действия:

• Win64.Rugrat: также известный как вирус Rugrat, этот ранний пример вируса прямого действия может заразить все 64-разрядные исполняемые файлы, которые он может найти в каталоге и подкаталогах, в которых он был запущен.

• Венский вирус: венский вирус отличается тем, что он является первым вирусом, который будет уничтожен антивирусом. Он ищет файлы .com и уничтожает некоторые из них, пытаясь заразить их.

3) Резидентный вирус. В отличие от вирусов прямого действия, о которых мы упоминали ранее, резидентные вирусы памяти фактически создают лагерь в основной памяти вашего компьютера (ОЗУ). Это плохая новость, потому что они могут продолжать работать даже после того, как вы избавитесь от первоначального вируса. Некоторые действуют быстро, некоторые наносят свой урон медленно — и поэтому их труднее обнаружить [5].

4) Многосторонний вирус. Эти ультра-универсальные вирусы удваивают свою силу распространения, нацеливаясь как на ваши файлы, так и на ваше загрузочное пространство. Таким образом, даже после того, как вам удалось удалить все зараженные файлы на вашем компьютере, вирус все еще остается скрытым в загрузочном секторе, готовый нанести новый удар, и если вы очистите загрузочный сектор, вирус повторно заразит его, прыгнув с одного из зараженных файлов.

5) Полиморфный вирус. Мутанты мира компьютерных вирусов, эти вирусы меняют форму, чтобы избежать обнаружения, сохраняя при этом свои основные возможности угрозы. После заражения ваших файлов эти вирусы копируются немного по-другому, что делает их очень трудными для полного обнаружения и удаления.

6) Макро-вирусы. Некоторые вирусы написаны на макроязыке с целью внедрения их в программное обеспечение, позволяющее создавать макросы-мини-программы, такие как Microsoft Word.

Как защитить себя от вирусов?

- Используйте антивирусную защиту. Антивирус - это ваша первая линия защита от вирусов и целого ряда других вредоносных программ, с которыми вы не желали бы столкнуться [3].
- Помимо того, что вы позволите антивирусу обнаруживать и удалять вирусы, вы будете делать себе огромную услугу, в первую очередь используя надлежащую кибергигиену и следуя некоторым основным советам по безопасности в Интернете [4]:

1. Не нажимайте на каждую ссылку, которую ваши друзья отправляют вам в социальных сетях, особенно если сообщение является просто ссылкой без контекста, или если слова в сообщении не совсем похожи на них. Учетные записи людей в социальных сетях могут быть взломаны и использоваться для распространения вирусов и вредоносных программ. Если сомневаетесь, напишите своему другу напрямую и спросите, действительно ли они хотели отправить вам эту ссылку.

2. Не открывайте никаких вложений по электронной почте, если вы не знаете на 100%, что это такое. Киберпреступники часто полагаются на ваше естественное любопытство для распространения вирусов - они говорят вам, что вы что-то выиграли, но вы не участвовали ни в каких конкурсах.

3. Не попадайтесь на сообщения и всплывающие окна «Ваш компьютер заражен!», которые поступают не непосредственно из вашего антивируса. Есть очень хороший шанс, что они попытаются заманить вас загрузить поддельный антивирус и забрать ваши деньги, заразить компьютер вредоносным ПО или и тем, и другим.

Следуя этим несложным правилам можно защитить свой компьютер и всю используемую на нем информацию.

Использованные источники:

1. Гуляев, В. Р. Компьютерные вирусы — проблема XXI века / В. Р. Гуляев, В. А. Стрункина. — Текст: непосредственный // Юный ученый. — 2017. — № 1 (10). — С. 54-56. — URL: https://moluch.ru/young/archive/10/752/ (дата обращения: 17.06.2021).
2. Грушев, П.П. Восстановление данных с жесткого диска: спасаем свои файлы после удаления, сбоя файловой системы, повреждения вирусом, форматирования диска, сбоя Windows, неудачного изменения настроек HDD и т.п. / Грушев П.П., Прокди Р.Г., Ульянов О.В.. — Санкт-Петербург: Наука и Техника, 2019. — 208 c. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/35390.html (дата обращения: 17.06.2021)
3. Алексеев, П.П. Антивирусы: настраиваем защиту компьютера от вирусов / Алексеев П.П., Козлов Д.А, Прокди Р.Г.. — Санкт-Петербург: Наука и Техника, 2018. — 80 c. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/35387.html (дата обращения: 17.06.2021)
4. Вулф, М.М. Как защитить компьютер от вирусов / Вулф М.М., Разумовский Н.Т., Прокди Р.Г.. — Санкт-Петербург: Наука и Техника, 2010. — 192 c. — ISBN 978-5-94387-623-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/35399.html (дата обращения: 17.06.2021)
5. Гошко, С.В. Технологии борьбы с компьютерными вирусами : практическое пособие / Гошко С.В.. — Москва : СОЛОН-ПРЕСС, 2016. — 351 c. — ISBN 978-5-91359-059-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/90288.html (дата обращения: 17.06.2021).