**Припадчев Артём, группа 2125**

Компьютерные вирусы

*Что такое вирус?*

В 1983 году исследователь Фред Коэн определил компьютерный вирус как «программа, которая может «заразить» другие программы модифицируя их, включая в них свой код». Это означает, что вирусы копируют семя, обычно немного видоизменяясь при каждом копировании, чтобы не раскрывать себя.

Есть несколько типов вирусов, но те, которые являются самыми опасными, разработаны, чтобы повредить ваш компьютер или программы. Вирусы различаются от простых надоедливых сообщений, высвечивающихся на вашем мониторе до удаление данных на вашем жестком диске. Вирусы часто используют часы вашего компьютера в качестве триггера. Популярные используемые даты – это пятница 13 и известные дни рождения. Важно знать, что вирусы опасны, только если вы запускаете зараженную программу.

Есть три основных вида вирусов. Каждый вид основывается на способе, которым распространяется зараженная программа.

1. Загрузочные вирусы. Эти вирусы присоединяются к гибким дискам и затем копируют себя в загрузочный сектор вашего жесткого диска. (Загрузочный сектор – набор инструкций вашего компьютера, используемые, когда он включается) Когда вы включаете свой компьютер (или перезагружаете его) ваш жесткий диск заражен. Вы можете получить загрузочный вирус только от зараженного гибкого диска. Вы не можете добраться до его местоположения на диске обычными файловыми менеджерами. Этот тип вируса наименее распространен, потому что нынешние компьютеры не требуют загрузочного диска, но они всё еще могут быть обнаружены на дисках, которые хранят еще какие-либо данные. Один из наиболее распространенных загрузочных вирусов назывался «Monkey», также известной как «Stoned».
2. Программные вирусы. Эти вирусы (также известные как традиционные файловые вирусы) присоединяются к исполняемым файлам программ. Обычно вирус присоединяется к .exe или .corn файлу. Однако, они могут заразить любой файл на вашем компьютере, который когда-либо будет вызван. Когда вы запускаете программу, которая содержит вирус, вирус обычно загружается в память вашего компьютера. Когда вирус находится в ней, он может заразить любую другую запущенную программу. Программные вирусы, которые циркулировали недавно являются «SKA» (Happy99.exe) and «Loveletter».
3. Макровирусы. Эти вирусы добавляют себя к шаблонам (в персональных компьютерах это обычно «normal.dot» файл), которые используются, чтобы создать документы или электронные таблицы. Как только шаблон будет заражен, каждый документ или таблица открытая вами также будет инфицирована. Макровирусы широко распространены, потому что они заражают обычные офисные программы и распространяются между PC и Macintosh. Макровирусы включают «Concept», «Melissa», и «Have a Nice Day».

Вы не можете получить вирус от…

* Открытия электронного письма. Однако вы можете получить вирус из открытого вами прикрепленного файла к письму.
* Чтения веб-страницы. Вы можете заразиться вирусом только после загрузки и запуска программы. Обычно ваш веб-браузер будет предупреждать вас, когда вы начнете загрузку из сети.
* Загрузки файла. Загрузка файла не заразит ваш компьютер вирусом. Однако установка или открытие зараженного документа или программы инфицируют ваш компьютер.

Если вы думаете, что возможно имеете вирус, то задайте такие вопросы:

1. Ваши программы загружаются дольше чем обычно?
2. Ваши программы завершаются с ошибкой по непонятным причинам?
3. Ваш компьютер часто обращается к жесткому диску?
4. Ваши файлы не исчезают по непонятным причинам?
5. Часто ли происходит повреждение файлов?
6. Элементы, которые раньше работали, теперь не работают?
7. Использовали ли вы недавно гибкие диски, которые побывали в других компьютерах?
8. Загружали ли вы и запускали какие-то программы или игры из Интернета?
9. Получали ли вы электронные письма от неизвестного источника?
10. Получали ли вы электронные письма с вложениями?

*Обманы*

С 1988 года появились тысячи вирусных обманов. «Успешный» вирусный обман включает два фактора:

1. Употребление технических терминов. Например, в обмане «Good Times» сообщалось, что Федеральная комиссия по связи выпустила предупреждение об опасном вирусе. На самом деле комиссия не выпускала предупреждения, т.к. это вообще не ее ответственность.
2. Вероятность ассоциации. Любая компания или организация может прислать предупреждение при идентификации. Тщательно проверяйте e-mail адреса, т.е. они могут быть похожи на официальные, но ими не являться.

Есть много веб-сайтов, которые специализируются на вирусном обмане. Список самых популярных вы можете найти с помощью любой поисковой системы.

*Что делать, если вы получили предупреждение*

* Не отвечайте на вирусные предупреждения, сначала сверьтесь с авторитетным источником. Предупреждения без имени человека, отправившего уведомление или предупреждение, а также с именем, адресом и телефонным номером, которые не существуют, вероятно являются обманами.
* Проверьте, что вы имеете последнюю версию антивирусного программного обеспечения, и оно корректно работает.
* Если предупреждение ссылается на коммерческое программное обеспечение, то вы можете уточнить информацию в компании продукта. Это можно сделать, например, через их официальный веб-сайт.

*Антивирусное программное обеспечение*

На рынке антивирусного программного обеспечения существует множество продуктов, поэтому важно выбрать по-настоящему стоящее. Для этого при выборе рассмотрите следующие вопросы:

* У компании есть сертификат NCSA/ICSA? Последние версии антивирусного ПО должны сертифицироваться. Чтобы пройти сертификацию, ПО должно обнаружить все известные вирусы при тестировании, и 90% всех других вирусов.
* Сверьтесь с центрами вирусного тестирования. Информацию о них вы сможете найти в Интернете.
* Убедитесь, что вам будет удобно пользоваться выбранным антивирусным ПО.

Попросите в близлежащем компьютерном магазине антивирусное ПО, которое соответствует вышеупомянутым параметрам.