УДК 004.056.57

ЗАЩИТА ДОМАШНЕГО КОМПЬЮТЕРА

Михайлова Е.А., студентка 4 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *компьютер, угрозы, вирус, защита, антивирус, безопасность.*

Работа посвящена рассмотрению наиболее опасных вирусов и защите операционной системы домашнего ПК от них.

Компьютерный вирус - видвредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Значительное большинство современных вирусов попадают в ПК через сеть Интернет, многие, причем, по разрешению пользователя, под видом обыкновенного программного обеспечения. Также, достаточно легко перенести любую заразу с других компьютеров с помощью съемных дисков (гибких и лазерных) или обыкновенной флешки. Очень быстро один ПК может заразить другие, которые находятся в одном с ним сетевом окружении. [1]

Чем грозит проникновение вирусов (и любых других шпионских программ) на ПК:

- потеря данных сжестких дисков;
- частые зависания и сбои в работе компьютера, вплоть до полной потери работоспособности;
- рассылка спама, атаки на чужие сети и компьютеры от вашего имени;
- личная информация, логины, пароли, номера кредиток - всё это может стать добычей мошенников;
- баннеры и реклама порнографического характера, отображающиеся вашим веб-браузером независимо от вашего желания;
- вымогательство денег с помощью блокирования вашего компьютера различными баннерами и заставками. [3]

Статистика угроз, обнаруженных в 2016 году в почтовом трафике, демонстрирует схожую картину: чаще всего по каналам электронной по-

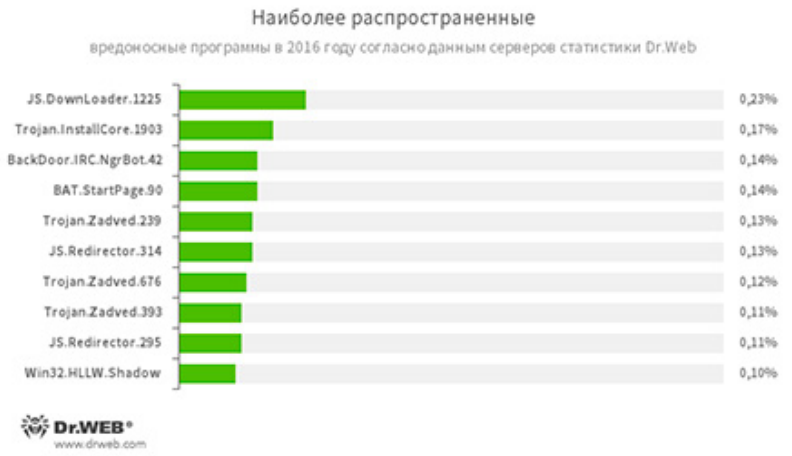

Рисунок 1 – Наиболее распространенные вредоносные программы в 2016 г.

чты злоумышленники рассылали вредоносные сценарии-загрузчики и рекламные трояны. Среди опасных вложений в сообщениях электронной почты также встречаются трояны-шпионы, шифровальщики, бэкдоры, и программы для подмены стартовой страницы в браузерах. Десять наиболее распространенных вредоносных приложений согласно данным почтового Антивируса Dr.Web представлено на рисунке 1.

JS.DownLoader Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Trojan.InstallCoreСемейство установщиков нежелательных и вредоносных приложений.

BackDoor.IRC.NgrBot.42 Довольно распространенный троян, известный специалистам по информационной безопасности еще с 2011 года. Вредоносные программы этого семейства способны выполнять на инфицированном компьютере поступающие от злоумышленников команды, а управление ими киберпреступники осуществляют с использованием протокола обмена текстовыми сообщениями IRC (InternetRelayChat).

BAT.StartPage.90 Вредоносный сценарий, позволяющий подменять стартовую страницу в настройках браузера.

Trojan.Zadved Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.

JS.Redirector Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.

Win32.HLLW.Shadow Червь, использующий для своего распространения съемные носители и сетевые диски. Кроме того, может распространяться по сети с использованием стандартного протокола SMB. Способен загружать с управляющего сервера и запускать исполняемые файлы.[4]

И в конце несколько советов, которые помогутзащитить ваш домашний компьютер от заражения вирусамии другим вредоносным кодом:

- обязательно установите антивирус, причем тот, какой имеет возможность сканировать не только файлы на жестком диске, но и проверяет интернет-трафик (http, ftp), электронную почту (smtp, pop3) и другие интернет-сервисы (icq и др.);
- настройте автоматическое ежедневное обновление антивирусных баз;
- настройте автоматическое обновление операционной системы;
- выходите в Интернет только через брандмауэр (фаервол) встроенный в Windows, а лучше - программный или аппаратный фаервол стороннего производителя;
- не заходите на сомнительные интернет-сайты, на которых чаще всего вместе со скачиванием какой-нибудь бесплатной программы вы наверняка загрузите на свой компьютер вредоносный код;
- не открывайте письма, и тем более вложения к ним, от неизвестных отправителей;
- регулярно делайте резервные копии важной информации на внешние носители - CD-DVD диски, флешки, внешние жесткие диски. [2]

Соблюдая эти простые правила можнозначительно повысить защиту домашнего компьютера от вирусов.

Библиографический список

1. Леонтьев, В.П. Новейшая энциклопедия. Компьютер и Интернет / В.П. Леонтьев.- М.: Из-во Полигон, 2016. -516с.
2. Мэйволд, Э. Безопасность сетей / Э. Мэйволд.- 2-е изд.- Из-во ИНТУ-ИТ, 2016. - 572с.
3. Соколов, А.В. Методы информационной защиты объектов и компьютерных сетей.- М.: Из-во Полигон, 2015. - 272с.

PROTECTINGYOURHOME COMPUTER

Mikhailova E.A.

Keywords: *computer, threats, virus, protection, antivirus, security.*

The work deals with the most dangerous viruses and protect the operating system home PC from them.