

УДК 004.056.57

## ПОЧТОВЫЕ ВИРУСЫ

*Бакальский В. Ю., студент 3 курса экономического факультета  
Научный руководитель - Голубев С. В., к.э.н., доцент  
ФГБОУ ВО Ульяновский ГАУ*

**Ключевые слова:** *виды вредоносных программ, интернет, электронная почта, файлы вложений, троянская программа.*

*В настоящий момент почтовые вирусы представляют собой большую угрозу, так как электронная почта пользуется большой популярностью.*

Почтовые вирусы составляют группу самых опасных и распространенных программ для повреждения ПО компьютера.

Почтовый вирус использует для своего распространения каналы электронной почты. Заражение почтовым вирусом происходит в результате действий пользователей, просматривающих почту, а также из-за ошибок в почтовых программах и операционных системах [2].

Если компьютер был заражен подобным образом, то пользователь продолжит рассылку вирусов, просто прикрепив к письму необходимый для отправки файл.

Часто подобные вирусы самостоятельно рассылают зараженные письма всем пользователям, мейлы которых хранятся в памяти компьютера. Таким образом, распространяясь, вирус вредит и репутации пользователя [3].

Существует 4 основных вида почтовых вирусов, распространенных в РФ: трояны; руткиты; черви; непосредственно сами вирусы (рисунок 1).

Разберем поподробнее каждый из почтовых вирусов.

**Трояны.** Под видом безобидной программы скрывается угроза, которая может уничтожить данные. Общая суть у троянов одна – они выдают себя за обычные программы, либо файлы, хотя таковыми совсем не являются. Подавляющая масса вирусов Trojan успешно отлавливается антивирусами. В основном трояны серьезной угрозы не представляют (рисунок 2).

**Руткиты.** Одна из наиболее сложных для обнаружения угроз. Руткит (Rootkit) прячутся глубоко в системе, они могут входить в какую-либо программу и отбирать себе часть ресурсов для функционирования.

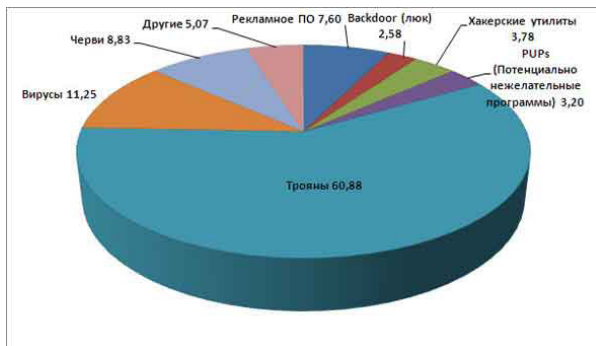


Рисунок 1 - Статистика распространения почтовых вирусов

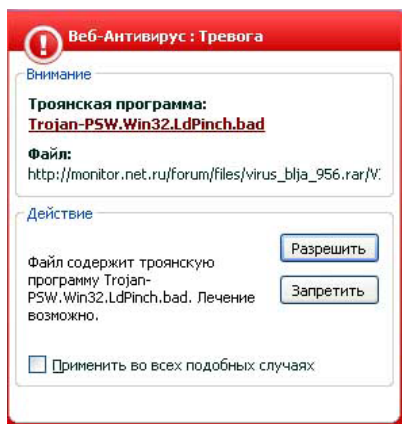



Рисунок 2 - Обнаружение антивирусом трояна

Руткит сложно не только обнаружить, но и удалить. Проблема поиска заключается в том, что прячется вирус глубоко в ОС, а кроме того умеет маскировать свое присутствие, чтобы антивирус ничего не заподозрил.

Компьютерный червь. В то время как вирус стремится проникнуть в максимально возможное количество программ, червь не инфицирует другие файлы. Поскольку компьютерный червь не прячется в структуру других файлов и программ, обнаружить его обычно проще, чем вирус или руткит. При этом скорость распространения червя выше. Многие

FW: Notice to Appear in Court

To You

Message  Notice\_to\_Appear\_0000699858.zip (2 KB)

-----Original Message-----  
 From: District Court [<mailto:darryl.rosenberg@gic-web-bsd-033.genotec.ch>]  
 Sent: Wednesday, August 5, 2015 9:41 AM  
 To:  
 Subject: Notice to Appear in Court

Notice to Appear,

You have to appear in the Court on the August 13.  
 Please, prepare all the documents relating to the case and bring them to Court on the specified date.  
 Note: The case will be heard by the judge in your absence if you do not come.

The copy of Court Notice is attached to this email.

Kind regards,  
 Darryl Rosenberg,  
 District Clerk.

**Рисунок 3 - Письмо, содержащее вирус «Шифровальщик»**

Имя	Тип	Размер	Дата
 Notice_to_Appear_0000699858.doc	js	<папка> 12 191	05.08.2015 09:40 05.08.2015 08:41

**Рисунок 4 - Архив письма**

из них находят адреса других компьютеров через почтовые аккаунты либо мессенджеры, и без ведома пользователя отправляют всему списку контактов ссылку на свою копию.

Одним из примеров простого почтового вируса является вирус «Шифровальщик», который распространяется через электронную почту под видом серьёзных документов:

- судебной повестки;
- счетов;
- запросов из налоговой (Рисунок 3).

Чтобы определить вирусное сообщение или нет, нужно присмотреться к наиболее выделяющимся несоответствиям писем:

- угрожающий заголовок - «Notice to Appear in Court», что в переводе означает «Повестка в суд»;
- адрес отправителя – [darryl.rosenberg@gic-web-bsd-033.genotec.ch](mailto:darryl.rosenberg@gic-web-bsd-033.genotec.ch). Явно показывает, что это не официальное письмо, а спамер/хакер;
- архив письма - есть файл, который должен сразу насторожить (в

имя файла входит .doc, но расширение js – вирус маскируется под документ Microsoft Word) (Рисунок 4).

Если компьютер был заражен шифровальщиком, то с вероятностью 95% информация будет утеряна безвозвратно. После скачивания и запуска вредоносного файла происходит обращение к удаленному серверу, с которого скачивается вирусный код. Все данные на компьютере шифруются случайной последовательностью символов.

Для «раскодирования» файлов понадобится ключ, который есть только у хакера. Мошенник обещает расшифровать информацию обратно за дополнительную плату [1].

#### *Библиографический список*

1. Взлом с доставкой: вирусы, получаемые через почту. Хакинг чужими руками. Почтовые вирусы [Электронный ресурс].– Режим доступа: <http://webmartsoft.ru/blog/haking-pochtovye-virusy.html>
2. ДиалогНаука [Электронный ресурс] / Почтовый вирус. – Режим доступа: <http://www.dialognauka.ru/support/golossary/4582/>
3. Софт-Архив Способы распространения компьютерных вирусов [Электронный ресурс]. – Режим доступа: <http://soft-arhiv.com/publ/4-1-0-57>

## **EMAIL VIRUSES**

***Bakalskiy V.Yu.***

***Keywords:*** *malware, Internet, electronic mail, file attachment, a Trojan program.*

*At the moment, email viruses constitute a serious threat, since email is very popular.*