УДК 34.03:339.543

Вирусы-шифровальщики

Ковалькова И. А.
Белорусский национальный технический университет

Вирусы-шифровальщики **(или** ***криптографические вирусы*****)** – это вредоносный вид программного обеспечения, который осуществляет шифрование всех или некоторой части файлов на жёстком диске. При шифровании все файлы превращаются в набор нулей и единиц, то есть представляют собой бессмысленный набор информации, который невозможно открыть ни одной программой.

Вирусы-шифровальщики (Virus-Encoder, Trojan-Encoder) появились в 2005 году. Их основная цель – получение выкупа за предоставление кода для расшифровки данных. В основном, создатели шифровальщиков используют для оплаты Bitcoin, чтобы их было сложнее найти. Большинство вирусов-шифровальщиков написаны для ОС Windows и Android, а также для MacOS и Linux. Как правило, вирусы-шифровальщики отсылаются злоумышленниками в виде электронного письма, представляясь официальным приложением банка, новой версией программного обеспечения, либо под видом обновления Adobe Flash Player или Oracle Java. Но основным способом распространения шифровальщиков остаётся спам.

После зашифровки, вирус-шифровальщик оставляет инструкцию в виде фона рабочего стола, либо как текстовый документ *readme* на рабочем столе, или в каждой папке с зашифрованными файлами. После оплаты выкупа пользователь получает более подробные инструкции по расшифровке файлов, либо специальный *decryptor* (программу-дешифратор). Обычно, шифровальщики требуют за разблокировку от $300, но не все из них действительно расшифровывают файлы после оплаты.

В настоящее время вирусы-шифровальщики обладают более качественным кодом, более серьёзными и сложными методами шифрования и представляют собой ещё более серьёзную опасность, чем раньше.

Чтобы защититься от вирусов-шифровальщиков необходимо придерживаться следующих советов: не открывать сомнительные письма из почты и мессенджеров, а если открыли – не переходить по вложенным ссылкам; регулярно обновлять операционную систему, антивирус и все ключевые приложения; не подключать к компьютеру чужие флешки, а если без этого нельзя, постоянно проверять их с помощью антивируса или специальных утилит; ограничивать права доступа на папки и файлы, устанавливая пароли с помощью специальных программ; использовать лицензионное антивирусное программное обеспечение.