Д. А. Будаев, Н. А. Жиляк
(БГТУ, Минск)

СОВРЕМЕННЫЕ ВИРУСЫ

Появление в сети интернет таких людей, как злоумышленники, мошенники, вымогатели было неизбежно с возникновением «всемирной паутины». Вся эта малопочтенная публика так или иначе пытается использовать просторы интернета в своих корыстных целях. Так, например, в 2016 году активно использовался язык JavaScript для написания e-mail вложений, содержащих вредоносное программное обеспечение (ПО). Однако теперь, чтобы обмануть пользователей, злоумышленники переключились на менее подозрительные типы файлов.

Microsoft Malware Protection Center сообщает о новой волне спам-писем, которые содержат в себе расширение .LNK файлы внутри ZIP архива. Кроме того, к этим файлам прикреплены вредоносные PowerShell-скрипты.

PowerShell – это язык сценариев для автоматизации задач системного администрирования операционной системы (ОС) Windows. В прошлом этим языком злоупотребляли при загрузке вредоносных программ. На сегодняшний день существуют программы полностью написанные на языке PowerShell.

Исследования .lnk-файлов, проводимые корпорацией Microsoft, выявили, что данные типы файлов заражают компьютер так называемым трояном Kovter. Особенность данного трояна заключается в том, что он имеет «бестелесную» архитектуру. Работает он в оперативной памяти инфицированного компьютера, а скрывается в реестре. Данный троян ухудшает производительность компьютера, изменяет системные настройки и параметры реестра, крадёт конфиденциальную информацию о системе и делает компьютер более уязвимым к другим угрозам. Обычно данный вирус используется злоумышленниками для увеличения просмотров рекламы, за счёт которой получают прибыль.

Кроме вышеупомянутых файлов, в последнее время часто используются SVG-файлы (файлы масштабируемой векторной графики). Пользователи, которые открывают изображения в браузерах, даже не подозревают, что такие картинки могут содержать вредоносные элементы JavaScript.

Совсем недавно в известной социальной сети Facebook данный вирус распространился довольно широко и успел заразить не один

компьютер. Картинка, на которую нажимал пользователь, перенаправляла его на поддельный Youtube-канал, где с его же согласия устанавливалось расширение. Это расширение якобы позволяло просматривать видео на сайте, но на деле воровало модифицированные пользовательские данные с различных сайтов. Также злоумышленники получали доступ к аккаунту Facebook.

Данные примеры показывают, что в современном мире при помощи всего лишь пару нажатий по клавиатуре, посторонние люди могут получить информации о нас больше, чем наши знакомые, а мы об этом даже не узнаем. Именно по этой причине необходимо искать методы защиты и борьбы с новейшими вирусами и пресекать попытки кражи данных.