Уважаемые клиенты!

Примите к сведению информацию о вирусе, который может заражать компьютеры с 1С.

Специалисты «Доктор Веб» обнаружили троянец 1C.Drop.1, который заражает компьютеры с установленными бухгалтерскими программами 1С и запускает на них опасного троянца-шифровальщика. Зловред стал первым троянцем, написанным «на русском языке».

Вирусная программа сохраняет на диск архиватор 7z и защищенный паролем архив, из которого затем извлекает файлы по одному. В этом архиве содержится несколько программ и динамических библиотек, имеющих разное назначение. Одно из приложений, которое распаковывает и запускает троянец-шпион, способный передавать киберпреступникам набираемый пользователем текст в окнах различных приложений, в том числе бухгалтерских.

Как сообщают специалисты «Доктор Веб», записи о нажатиях клавиш троянец сохраняет на диске в специальном файле и с интервалом в минуту передает его содержимое на управляющий сервер. Вместе с кодами самих нажатых клавиш вредоносное ПО отсылает злоумышленникам и название окна, в котором произошло нажатие.

По имеющейся информации, троянец отслеживает активность пользователя в таких приложениях, как 1С версии 8, 1С версий 7 и 7.7. Эксперты поясняют, что вирус написан на встроенном языке программирования 1С, который использует для записи команд кириллицу.

Вредоносное ПО распространяется по электронной почте среди зарегистрированных в базе контрагентов с темой «У нас сменился БИК банка». В тексте письма приводится просьба обновить классификатор банков с помощью прикрепленного файла. Если получатель откроет его в программе «1С:Предприятие», на экране отобразится диалоговое окно. Независимо от выбора кнопки («да» или «нет») 1C.Drop.1 будет запущен на выполнение, рассылая контрагентам аналогичные письма.

После завершения рассылки вирус извлекает из своих ресурсов, сохраняет на диск и запускает троянца-шифровальщика, который шифрует хранящиеся на дисках зараженного компьютера файлы и требует выкуп за их расшифровку.

Будьте внимательны! Не открывайте письма и вложенные в них файлы, полученные по электронной почте от неизвестных Вам отправителей, а также следуйте другим рекомендациям о мерах безопасного использования систем ДБО, размещенным на сайте банка в разделе Главная/Система Банк-Клиент/Информация.