Автор: Administrator
20.02.2016 12:07 -

Исследователи компании Palo Alto Networks обнаружили новый вид вымогательского ПО, нацеленного на компьютеры под управлением ОС Windows. Отличительной **особенностью нового вредоноса Locky является способ загрузки**, во многом напоминающий банковского трояна Dridex.

Locky распространяется с помощью спама с прикрепленным вложением в виде документа Microsoft Word. Документ содержит макрос, загружающий вымогательское ПО с удаленного сервера. Аналогичный способ загрузки использует банковский троян Dridex.

По словам специалистов Palo Alto, Dridex и Locky могут быть связаны. Вероятно, вредоносы разрабатывает одна и та же группа. «Схожие способы распространения, одинаковые имена файлов и резкий спад активности Dridex на момент выхода Locky свидетельствуют о явной связи между создателями вредоносного ПО», - заявили эксперты.

Locky шифрует и добавляет расширение *.locky к файлам на системе. Для восстановления доступа к информации пользователь должен отправить определенную сумму средств в биткоинах. В отличие от других видов вымогательского ПО, Locky использует C&C-инфраструктуру для осуществления обмена ключами в памяти до шифрования файлов. Как отметили эксперты, данную особенность можно применять для предотвращения потери доступа к информации.

Хакеры осуществили крупномасштабную атаку с применением Locky. Эксперты обнаружили более 400 тысяч сессий, использующих один и тот же загрузчик Bartallex для распространия вредоноса. Более половины пострадавших систем находились в США.