Авторы троянского вируса Win32/Sheldor.NAD, который попадает в компьютер вместе с модифицированной версией программы для удаленного управления, получили доступ к счету клиента одного из крупнейших российских банков и похитили около 5 млн. рублей. Об этом РИА Новости сообщили представители компаний ESET и Group IB, принимавшие участие в расследовании инцидента.

Инцидент случился около трех недель назад. Неизвестные хакеры модифицировали один из модулей бесплатной версии программы TeamViewer 5.0, предназначенной для удаленного управления другим компьютером, и распространили ее в Сети. Потенциальной жертвой вирусописателей становился любой, кто устанавливал на своей машине инфицированный TeamViewer.

«Использование программ удаленного администрирования злоумышленниками мы встречаем не впервые. В данном случае создатели вируса стремились достичь максимальной схожести с легальным программным продуктом, чтобы оставаться незамеченными», – говорит Александр Матросов, директор центра вирусных исследований и аналитики компании ESET.

По данным ESET, за исключением одного модуля все компоненты модифицированной преступниками версии TeamViewer имели цифровую подпись, идентичную легальной версии софта, поэтому большинство антивирусов не обнаруживали зловредный код.

По словам представителей компании Group IB, занимающейся расследованием киберпреступлений, пока неизвестно, была ли это атака, направленная на клиентов только одного банка, или нападение было более масштабным. Пока известно лишь об одном случае хищения денег со счетов российского банка из числа 20 крупнейших.

В Group IB сообщили, что жертвой атаки стало юридическое лицо – небольшая компания, пользовавшаяся услугами системы дистанционного банковского обслуживания.

Источник: banker.ua