Портал Bleeping Computer предупредил пользователей популярного менеджера паролей KeePass с открытым исходным кодом о том, что некая группа киберпреступников распространяет троянскую версию менеджера через рекламные объявление в поисковой системе Bing.

Аналитики компании WithSecure, специализирующейся на кибербезопасности, выявили хакерскую кампанию, обнаружив изменённую версию KeePass под названием KeeLoader, содержащую водяные знаки Cobalt Strike, связанные с атаками серьёзного вредоноса Black Basta ransomware. Эти водяные знаки служат как идентификаторы, которые используются для генерации различной вредоносной полезной нагрузки.

Согласно сообщениям WithSecure, водяные знаки Cobalt Strike связаны с брокером начального доступа (IAB), который, как считается, в прошлом был причастен к атакам с использованием программы-вымогателя Black Basta и использовался участниками нынешней кампании для распространения вредоносного ПО для кражи паролей и других данных. А нацеленность злоумышленников на KeePass объясняется открытым исходным кодом приложения.

«Этот водяной знак часто встречается в контексте маяков и доменов, связанных с программой-вымогателем Black Basta. Он, вероятно, используется злоумышленниками, работающими в качестве брокеров начального доступа и тесно сотрудничающими с Black Basta», — объясняет WithSecure.