Новый инструмент киберпреступников SessionShark, обнаруженный экспертами SlashNext, представляет серьёзную угрозу для пользователей Microsoft Office 365, сообщается на Dark Reading. Этот “фишинговый набор” использует технику «посредника» (adversary-in-the-middle, AitM), перехватывая сессионные токены — цифровые ключи, позволяющие оставаться в системе без повторного ввода пароля. Это позволяет хакерам обходить многофакторную аутентификацию.

SessionShark рекламируется на подпольных киберфорумах как «этический» инструмент для обучения, но его возможности явно нацелены на кражу данных, включая логины и сессионные куки. Набор интегрируется с Telegram для мгновенных уведомлений о взломе и использует Cloudflare для сокрытия серверов, что затрудняет его блокировку.

Эксперты предупреждают, что SessionShark упрощает атаки даже для новичков, предоставляя удобный интерфейс и техподдержку. Для защиты организации должны усиливать мониторинг сетей, использовать условные политики доступа и обучать сотрудников распознавать фишинговые страницы, пишут аналитики.