

Россиян предупредили о вирусах, которые распространяют через Telegram в период отпусков

Перед майскими праздниками сотрудники российских компаний начали получать подозрительные сообщения в [Telegram](#) с предложением скачать «пак аватарок для отпуска». Архив, прикреплённый к письмам, содержал вредоносный скрипт, который собирает данные с устройств жертв и отправляет их злоумышленникам. Об этом сообщил эксперт по [информационной безопасности](#) Александр Блезнеков.

По словам эксперта, рассылка якобы от HR-отделов компаний выглядела достаточно убедительно. В письме говорилось, что дизайнеры подготовили аватарки для мессенджеров, чтобы коллеги знали, что сотрудник ушёл в отпуск. На самом деле открытие вложенного RAR-архива активировало вредоносный скрипт, который искал и похищал важные файлы, такие как документы с ключевыми словами в названиях. Блезнеков отметил, что [кибератака](#) была нацелена в основном на пользователей Windows, а количество сообщений превысило 300, особенно в IT-компаниях.

Эксперт подчеркнул, что для защиты корпоративной информации важно использовать системы мониторинга угроз, такие как SOC (Security Operation Center). Такие системы анализируют подозрительные действия сотрудников и моментально реагируют. Например, если скрипт запускается, учётную запись можно заблокировать, а устройство изолировать от сети. Также помогает ограничение на запуск макросов в загруженных файлах, что предотвращает активацию вредоносного кода.