Киберпреступники разместили в реестре npm три фальшивых пакета, имитирующих популярную библиотеку Telegram Bot API, чтобы внедрять SSH-бэкдоры в Linux-системы. Как сообщает The Hacker News, пакеты node-telegram-utils, node-telegram-bots-api и node-telegram-util, обнаруженные фирмой Socket, содержат вредоносный код, обеспечивающий постоянный доступ к заражённым устройствам и кражу данных. Эти библиотеки копируют внешний вид node-telegram-bot-api, популярной у разработчиков с более чем 100 000 еженедельных загрузок.

После установки пакеты подключаются к командному серверу через зашифрованный SSH-туннель, собирают системные данные, такие как имя хоста и сведения о процессоре, и отправляют их атакующим. Для повышения доверия хакеры используют технику «starjacking», присваивая фальшивым репозиториям звёзды с легитимных проектов на GitHub. Несмотря на низкое число загрузок (73–132), даже одна заражённая система может стать плацдармом для масштабных атак.

Npm — это менеджер пакетов для JavaScript, широко используемый разработчиками. Бэкдор — это скрытый доступ, позволяющий хакерам управлять системой. Socket рекомендует проверять имена и код пакетов перед установкой.