Хакеры постоянно ищут новые способы для доступа к ценным ресурсам. Недавнее исследование, проведённое Группой Компаний «Солар», выявило тревожную тактику восточноевропейской хакерской группировки. Они использовали серверы, управляющие лифтами в подъездах, как платформу для своих атак на российские ИТ-компании.

По данным исследования, хакеры взламывали контроллеры IT-системы компании «Текон-Автоматика», входящие в состав SCADA-систем. Эти серверы затем использовались для атак на другие цели, хотя сами лифты не подвергались нападению. Уязвимость, которую злоумышленники использовали, позволяла им получать доступ и контроль над оборудованием, но не настраивать его на целенаправленные повреждения.

Специалисты из Группы Компаний «Солар» отмечают, что использование инфраструктуры Starlink от SpaceX для атак является особенно тревожным. Это указывает на высокий уровень технической сложности и проникновения хакерской группировки Lifting Zmiy. В результате под удар попали организации из различных секторов, включая госсектор, IT и телекоммуникации.