Компания GreyNoise выявила масштабную кампанию взлома, затрагивающую тысячи роутеров ASUS, подключенных к интернету. Хакеры получили несанкционированный и устойчивый доступ к устройствам, что может стать основой для создания мощной сети зараженных устройств — ботнета.

Атака отличается высокой степенью скрытности и сложностью. Злоумышленники используют встроенные функции системы роутеров, чтобы сохранить контроль даже после перезагрузки или обновления прошивки. Для этого они обходят аутентификацию, эксплуатируют известную уязвимость и умело используют легитимные настройки, не оставляя явных следов заражения.

Особенность этой кампании — ее долгосрочный характер и способность избегать обнаружения. Методы, применяемые хакерами, похожи на тактики, используемые продвинутыми группами кибершпионажа, что говорит о высоком уровне подготовки и ресурсах атакующих.

Обнаружить атаку помогла собственная система анализа сетевого трафика GreyNoise — инструмент Sift, работающий на базе искусственного интеллекта. В сочетании с эмуляцией работы роутеров ASUS это позволило выявить тонкие попытки взлома, которые скрывались в общем интернет-трафике, и полностью восстановить последовательность атак.