Злоумышленники могут устанавливать на недорогие веб-камеры закладки–бэкдоры для доступа в

Автор: Надо.ua
20.01.2016 14:39

Хотя дешёвые беспроводные веб-камеры могут показаться кому-то небольшими гаджетами, не имеющими большого значения, но размещённые в домах и офисах (и подключённые к домашним и офисным сетям) они могут стать просто идеальной находкой для злоумышленников.

Исследователи из Лаборатории угроз Vectra продемонстрировали, как легко можно найти лазейки к веб-камерам в виде программ-закладок, с целью доказать, что развитие Интернета вещей расширяет возможности злоумышленников для атак на сети.

Они взяли веб-камеры потребительского класса D-Link WiFi примерно за 30 долларов за штуку и успешно взломали их, сняв содержимое чипа флэш-памяти камеры. Затем они нашли загрузчик операционной системы, ядро Linux и изображения.

После получения доступа к файловой системе изображений Linux, они обнаружили двоичный код, который выполняет проверку и обновление прошивки.

«На данный момент добавление закладки-бэкдора обеспечивает добавление сервиса внутри Linux», — объясняют исследователи.

«Когда мы делаем модификацию, мы также можем удалить возможность для перепрошивки устройства в будущем. Это позволит избежать обновления прошивки по инициативе администратора, которое могло бы убрать нашу закладку».

ИспользуяTelnetd / BusyBox / Netcat злоумышленники могут вернуть телнет сокет

внешнему хосту, чтобы иметь постоянно удаленный доступ к веб-камере. С помощью веб-камеры, действующей в качестве прокси-сервера, они теперь могут послать трафик в сети для осуществления своей атаки, а также использовать веб-камеру, чтобы перекачать украденные данные, отметили они.

Ограничения этого типа атак очевидны: злоумышленники должны быть достаточно квалифицированы, чтобы создать флеш изображение с бэкдором и найти способ для его доставки на устройство — либо с его «обновлением» или, получив доступ к нему перед его установкой.

Источник

Перевод