Вирусы умной детской игрушки

«При покупке для детей умных устройств необходимо обращать внимание не только на их развлекательные и образовательные опции, но и на уровень защищенности», – советует старший исследователь Kaspersky ICS CERT Николай Фролов. И как последовало из дальнейшей беседы, у эксперта были на то основания.

Исследователи Kaspersky обнаружили в детском интерактивном роботе уязвимости, которые потенциально могли позволить злоумышленникам использовать камеру в игрушке для общения с ребенком без ведома родителей. Эксперты уведомили производителя, и к настоящему моменту он устранил описанные проблемы безопасности. Основные результаты исследования компания Kaspersky представила на Mobile World Congress 2024.

Робот, «начинку» которого проанализировали специалисты, – это интерактивное устройство на базе операционной системы Android. Он оснащен большим цветным экраном, микрофоном, видеокамерой и может передвигаться – условный «планшет на колесах». Функциональность робота включает игровые и обучающие приложения для детей, голосовой ассистент, возможность выхода в интернет и связи с родителями через приложения на их смартфонах.

Перед началом использования робота его необходимо связать с аккаунтом взрослого. Для этого пользователь должен установить на своем мобильном устройстве специальное приложение. При первом включении игрушка просит выбрать сеть Wi-Fi, привязать робота к мобильному устройству родителя, ввести имя и возраст ребенка.

Какие уязвимости были найдены? Первый серьезный недостаток с точки зрения кибербезопасности заключался в том, что информация о ребенке передавалась по протоколу HTTP в открытом виде. Таким образом, теоретически злоумышленники могли бы перехватить ее, используя программное обеспечение для анализа сетевого трафика. При этом протокол HTTP применялся до обновления прошивки робота до актуальной версии, после обновления стал использоваться HTTPS.

Эксперты изучили некоторые сетевые запросы и увидели, что один из них возвращает токен доступа к API на основе следующих аутентификационных данных: имя пользователя, пароль и ключ. Причем происходило это даже в том случае, если запрос содержал заведомо неправильный пароль из произвольного набора символов.

Следующий сетевой запрос возвращал параметры конфигурации для конкретного робота по уникальному идентификатору, состоящему из девяти символов. Но, поскольку этот набор символов был коротким и предсказуемым, потенциально злоумышленники

могли быстро подобрать его и получить информацию о владельце игрушки, в том числе IP-адрес, страну проживания, имя, пол и возраст ребенка, а с помощью еще одного запроса – адрес электронной почты, номер телефона взрослого и код для привязки его мобильного устройства к роботу.

Звонки от злоумышленников. При установке сеанса видеосвязи отсутствовали должные проверки безопасности. Злоумышленники потенциально могли бы использовать камеру и микрофон робота для звонков детям без авторизации с родительского аккаунта. То есть, если бы ребенок принял звонок, недоброжелатель мог бы начать общаться с ним без ведома взрослых.

Удаленный контроль. Используя метод брутфорса (полного перебора паролей) для восстановления шестизначного одноразового пароля и не имея ограничений на количество неудачных попыток, злоумышленник потенциально мог удаленно привязать робота к своей учетной записи вместо родительского аккаунта. В таком случае, чтобы восстановить связь легитимным путем, пришлось бы обратиться в техподдержку производителя.

После того как компания Kaspersky сообщила о проблемах безопасности производителю, он их исправил.

«*Приобретая умные устройства для детей, не стоит полагаться на цену,* – советует Николай Фролов. – *Даже самые дорогие смарт-устройства могут иметь уязвимости, которыми способны воспользоваться злоумышленники. Мы рекомендуем родителям внимательно изучать обзоры умных игрушек, следить за новостями об обновлениях программного обеспечения и по возможности присматривать за ребенком, пока он взаимодействует с таким гаджетом*».

Эксперты Kaspersky рекомендуют пользователям умных устройств, в том числе умных игрушек:

- регулярно обновлять прошивку и программное обеспечение всех подключенных устройств, поскольку обновления часто содержат важные исправления безопасности, устраняющие известные уязвимости;
- перед покупкой изучать информацию об устройстве и разработчике: лучше доверять проверенным игрокам рынка;
- просматривать и ограничивать разрешения, предоставляемые мобильным приложениям для управления умным устройством;
- обеспечивать безопасность мобильных устройств, через которые происходит управление умными гаджетами, с помощью надежного защитного решения.