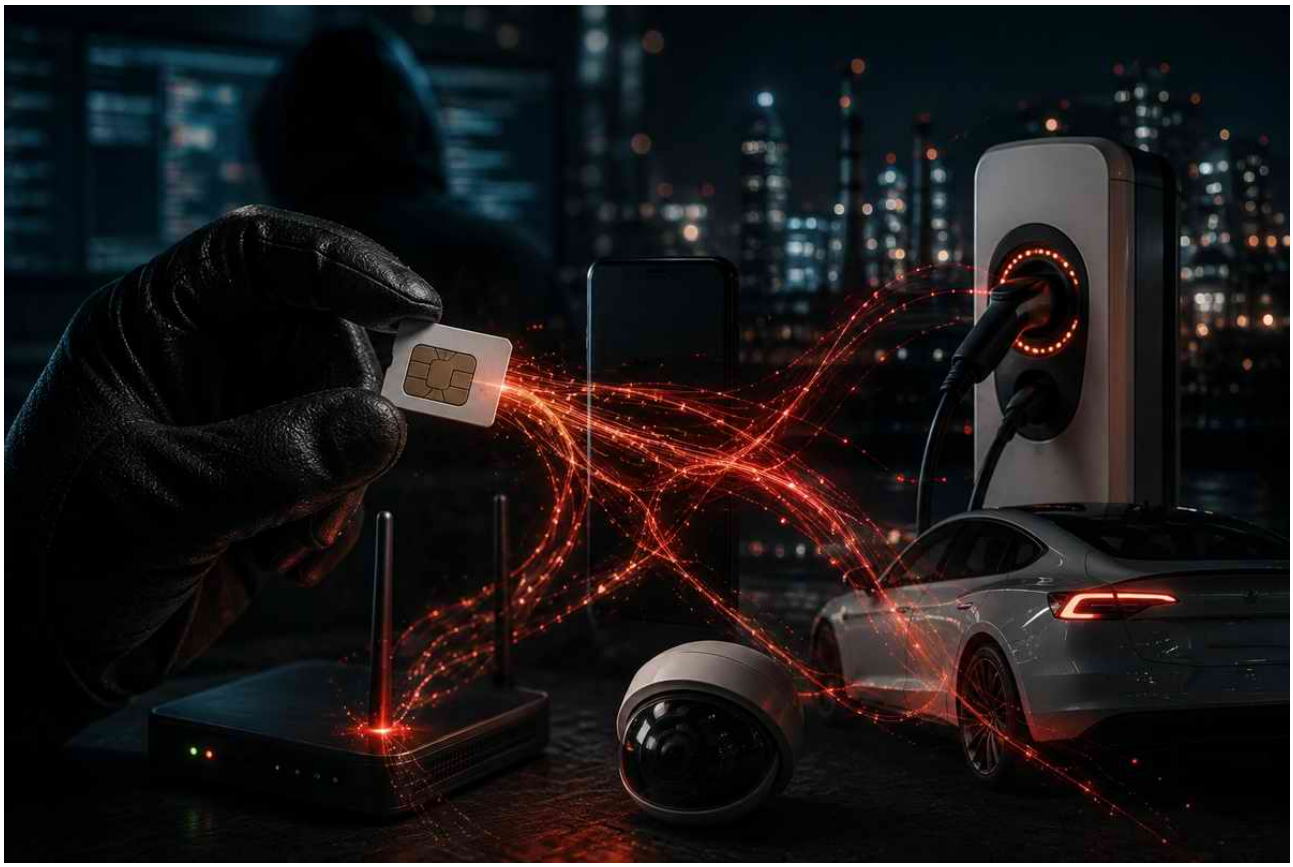
Вредоносная SIM-карта может превратить смартфон и даже электромобиль в цель для кибератаки



Дата публикации: 12.08.2026

Обычная SIM-карта кажется одним из самых простых компонентов смартфона: небольшой чип идентифицирует абонента и позволяет устройству подключаться к мобильной сети. В действительности это защищенный электронный элемент с собственными вычислительными возможностями, программным обеспечением и механизмами взаимодействия с телефоном. Исследователи из Бирмингемского университета показали, что при компрометации SIM-карты эти возможности способны превратиться в неожиданную точку входа для кибератаки. Причем потенциальными целями становятся не только смартфоны, но и подключенные автомобили, маршрутизаторы, промышленное оборудование и зарядные станции для электромобилей.

Результаты исследования были представлены на конференции USENIX WOOT 2026. Основное внимание ученые уделили технологии Proactive SIM. Она позволяет SIM-карте самостоятельно инициировать определенные действия и

передавать устройству ограниченный набор специальных команд. Механизм создавался для вполне легитимных функций мобильной связи, однако проблема возникает, если сама SIM-карта больше не считается доверенным компонентом.

Особый интерес вызвала возможность инициировать AT-команды. Они появились еще во времена ранних модемов и десятилетиями используются для настройки и управления коммуникационным оборудованием. Современные сотовые модемы также поддерживают множество подобных команд. В зависимости от реализации они могут управлять сетевым соединением, звонками, сообщениями, настройками модема и диагностическими функциями. Получается необычная ситуация: крошечный чип, который большинство пользователей воспринимает исключительно как электронный идентификатор, потенциально получает канал для передачи управляющих инструкций коммуникационному процессору.

Чтобы исследовать этот механизм систематически, специалисты создали инструментарий CATana. С его помощью они проверили 26 различных устройств: 18 смартфонов и восемь сотовых IoT-модулей, подобных тем, которые устанавливаются в промышленном оборудовании, автомобилях и системах зарядки электромобилей. Исследование не ограничивалось одной операционной системой или одним производителем, поскольку задача заключалась в проверке самого архитектурного механизма взаимодействия SIM-карты с модемом.

Выяснилось, что некоторые устройства действительно выполняют AT-команды, инициированные со стороны SIM-карты. После обнаружения доступных интерфейсов исследователи начали проверять их на наличие опасных комбинаций и ошибок реализации. Это позволило выявить сценарии, при которых потенциальные возможности вредоносной SIM-карты выходят далеко за пределы простого нарушения мобильного соединения.

В зависимости от конкретного оборудования и обнаруженной уязвимости атака могла приводить к повторному включению отключенных отладочных интерфейсов, получению идентификаторов устройства, отправке сообщений или инициированию звонков, выполнению произвольных команд на коммуникационном процессоре, принудительному переходу с 4G на менее защищенную сеть 2G, выключению устройства или полной потере сотового соединения. Эти сценарии не означают, что каждая SIM-карта способна автоматически выполнить все перечисленные действия. Речь идет о поверхности атаки, возникающей при сочетании враждебной SIM-карты, поддерживаемых команд и уязвимой реализации конкретного устройства.

Необычность проблемы заключается в том, что некоторые потенциально опасные возможности не являются тайными или недокументированными. Они

происходят из предусмотренных стандартами функций. Долгое время архитектура строилась вокруг предположения, что SIM-карта относится к доверенной части системы. Если же этот элемент становится враждебным, функциональность, созданная для управления связью, начинает работать уже против устройства.

Существует несколько путей, по которым SIM или eSIM теоретически может оказаться скомпрометированной. Исследователи рассматривают удаленную эксплуатацию уязвимости программного обеспечения SIM-карты, физическую замену карты или вмешательство в устройство, злоупотребление инфраструктурой удаленного управления со стороны имеющего соответствующий доступ злоумышленника, компрометацию SIM-карты на этапе производства или распространения. Для eSIM физической карточки вообще не требуется, но сама концепция защищенного элемента и удаленно загружаемого профиля создает собственную модель угроз.

Особое значение работа имеет для интернета вещей. В смартфоне существует множество уровней защиты, интерфейсов и механизмов обновления, тогда как специализированный IoT-модуль может годами работать внутри устройства практически незаметно для владельца. Сотовые модули используются в платежных терминалах, автомобильной телематике, промышленных контроллерах, маршрутизаторах, системах мониторинга и зарядных устройствах для электромобилей. Если доступ через SIM позволяет добраться до неожиданного управляющего интерфейса, он способен стать первым этапом более сложной атаки.

Для зарядной станции электромобиля это особенно показательный сценарий. SIM-карта может обеспечивать связь станции с удаленной инфраструктурой оператора, передачу телеметрии и обслуживание платежных функций. Пользователь практически никогда с ней не взаимодействует и может даже не подозревать о наличии внутри оборудования сотового модуля. Поэтому компрометация подобного компонента сложнее заметить, чем подозрительное приложение на смартфоне.

Исследователи обращают внимание и на потенциальную возможность превращения мобильного устройства в инструмент наблюдения. В предшествующей работе команда обнаружила сценарий, при котором вредоносная SIM-карта на современных Android-устройствах могла инициировать открытие контролируемого злоумышленником веб-ресурса без действий пользователя, в том числе при заблокированном телефоне. Подобные механизмы особенно важны именно потому, что атака начинается на уровне, который рядовой владелец устройства практически не контролирует.

Однако работа не означает, что владельцам смартфонов следует срочно отказываться от SIM-карт или считать любую eSIM потенциально опасной. Исследование представляет собой анализ неблагоприятного сценария, в котором защищенный элемент уже оказался под контролем злоумышленника. Цель таких работ — понять, насколько далеко может распространиться атака после нарушения исходной модели доверия, и устранить дополнительные возможности до их практического использования.

Команда передала результаты GSMA, производителям микросхем и компаниям, выпускающим затронутое оборудование. После уведомлений начали появляться изменения программного обеспечения и более безопасные конфигурации. Это особенно существенно из-за масштаба технологии: SIM и eSIM используются в миллиардах устройств, а сотовая связь давно перестала быть исключительно функцией мобильного телефона.

Исследование демонстрирует более общую проблему современной кибербезопасности. Чем сложнее становится подключенное устройство, тем больше в нем компонентов, которые исторически считались доверенными и поэтому получали привилегированный доступ. Модем, SIM-карта, беспроводной контроллер или служебный интерфейс могут десятилетиями сохранять функции, созданные в совершенно другой технологической эпохе. Когда меняется модель угроз, старое удобство способно превратиться в новую поверхность атаки.

Работа с CATana показывает, почему безопасность будущих смартфонов, автомобилей и IoT-систем необходимо оценивать не только с точки зрения приложений и основной операционной системы. Атака может начинаться гораздо глубже — внутри компонента, о существовании которого пользователь почти никогда не задумывается. Чем больше окружающих нас устройств постоянно подключено к мобильным сетям, тем важнее принцип минимальных привилегий: даже традиционно доверенный элемент не должен получать больше возможностей, чем ему действительно необходимо.