**Обзор угроз для IoT-устройств в 2023 году**

[**Публикации**](https://securelist.ru/category/publications/)

21 Сен 2023

 8 мин. на чтение

**Авторы**

* [Виталий Моргунов](https://securelist.ru/author/vitalymorgunov/)
* [Ярослав Шмелев](https://securelist.ru/author/yaroslavshmelev/)
* [Kaspersky Security Services](https://securelist.ru/author/securityservices/)
* [Kaspersky ICS CERT](https://securelist.ru/author/icscert/)

Количество IoT-устройств — роутеров, камер, NAS-хранилищ, компонентов «умного дома» — растет с каждым годом. Портал Statista [прогнозирует](https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/), что к 2030 году оно превысит 29 миллиардов. С увеличением числа подключенных устройств растет и необходимость их защищать. Первые массовые атаки на IoT-устройства с использованием вредоносного ПО [были зафиксированы](https://securelist.com/heads-of-the-hydra-malware-for-network-devices/36396/#hydra-an-open-source-prototype-of-router-malware) еще в 2008 году, и с тех пор подобных атак становится только больше. Мы проанализировали ландшафт угроз, актуальных для IoT-устройств в 2023 году, а также товары и услуги в даркнете, связанные со взломом подключенных устройств. В этой статье мы приводим основные результаты нашего исследования.

**Векторы атаки**

Существует два основных пути заражения IoT-устройств: перебор слабых паролей и эксплуатация уязвимостей в сетевых сервисах.

В первом случае наиболее распространенным методом является перебор паролей к сервисам, использующим протокол Telnet — крайне популярный в IoT-среде нешифрованный текстовый протокол. Успешный перебор пароля позволяет киберпреступникам выполнять произвольные команды на устройстве и запускать на нем вредоносное ПО. Аналогичные результаты дает и перебор паролей к сервисам, использующим SSH — более современный протокол, предусматривающий шифрование трафика. Однако атака на SSH требует больших ресурсов, а доступных из интернета сервисов меньше, чем в случае с Telnet.

За первую половину 2023 года 97,91% попыток перебора паролей, зафиксированных нашими ханипотами, были связаны с протоколом Telnet и 2,09% — с SSH. Больше всего инфицированных устройств, совершавших эти атаки, находилось в Китае, Индии и США, а по количеству атак лидируют Китай, Пакистан и Россия.

***TOP 10 стран и территорий, в которых находилось большинство устройств, атаковавших ханипоты «Лаборатории Касперского», H1 2023 (***[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183526/02-ru-iot-charts.png)***)***

***TOP 10 стран и территорий — источников атак на ханипоты «Лаборатории Касперского», H1 2023 (***[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183617/01-ru-iot-charts.png)***)***

Атаки с перебором паролей довольно распространены, поскольку часто Telnet- и SSH-сервисы на IoT-устройствах защищены широко известными паролями по умолчанию, которые пользователи, как правило, не меняют. Более того, в некоторых случаях на IoT-устройствах установлены несменяемые главные пароли, заданные производителем.

К компрометации устройства также могут приводить и уязвимости работающих на нем сервисов. Самый распространенный тип уязвимостей, которые эксплуатируют злоумышленники, — внедрение вредоносных команд при выполнении запросов к веб-интерфейсу. Ущерб от таких атак может быть весьма значительным, как, например, в случае с [уязвимостью реализации протокола TR-064](https://securelist.com/new-wave-of-mirai-attacking-home-routers/76791/), который интернет-провайдеры используют для автоматической настройки устройства в локальной сети. Уязвимость позволила злоумышленникам отправлять пакеты TR-064 без аутентификации, чем они и воспользовались для распространения зловреда Mirai.

Вне зависимости от метода компрометации, атаковать IoT-устройства могут как злоумышленники со своих серверов, так и сами зловреды за счет так называемого механизма самораспространения — способности вредоносных файлов самостоятельно обнаруживать уязвимые устройства в интернете и устанавливать на них свою копию множеством различных методов. Во втором случае атака может исходить и со стороны зараженного ранее IoT-устройства.

**Услуги в даркнете: DDoS-атаки, ботнеты и уязвимости нулевого дня в IoT**

Среди услуг в даркнете, связанных с IoT, в первую очередь стоит рассмотреть DDoS. Ботнеты, построенные на основе IoT-устройств и использующиеся для проведения распределенных DoS-атак, стали чаще встречаться в объявлениях на различных теневых форумах и пользоваться спросом у злоумышленников.

Всего за первую половину 2023 года аналитики сервиса Kaspersky Digital Footprint Intelligence обнаружили более 700 объявлений об услугах по проведению DDoS-атак на различных форумах в даркнете.

***Распределение количества публикаций, связанных с услугами по проведению DDoS-атак, по месяцам, H1 2023 (***[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183647/03-ru-iot-charts.png)***)***

Цена такой услуги зависит от множества факторов, влияющих на сложность атаки, среди которых: наличие у жертвы защиты от DDoS, наличие капчи и JavaScript-верификации. В общей сложности стоимость атаки варьируется от $20 за сутки до $10 000 за месяц, а средняя цена для изученных объявлений составила $63,5 за сутки или $1350 за месяц.

Покупают в даркнете и услуги по взлому IoT. В частности, злоумышленники ищут эксплойты к уязвимостям нулевого дня в устройствах интернета вещей.

Также на теневых форумах можно найти предложения о продаже и покупке вредоносного ПО для IoT. Иногда к собственно зловреду прилагается инфраструктура и дополнительные утилиты. Так, на скриншоте ниже продавец предлагает самописный DDoS-бот с C2-сервером и ПО для загрузки зловреда через Telnet или SSH:

Ниже скриншот объявления, в котором злоумышленник ищет не только вредоносное ПО, но и помощь в его установке.

В некоторых случаях злоумышленники обозначают, для каких типов IoT-устройств они ищут или продают зловреды.

*Скриншот объявления из потока Kaspersky Threat Intelligence Portal*

Иногда в даркнете продают и сети уже зараженных устройств, хотя такие объявления не очень распространены. Например, пользователь на скриншоте ниже ищет покупателя для ботнета из 200 роутеров и камер, расположенных в Аргентине.

**Цели и виды вредоносного ПО, атакующего IoT**

Злоумышленники, заражающие IoT-устройства, могут преследовать разные цели. В частности, они могут в дальнейшем использовать зараженную технику как инструмент для проведения кибератак, маскировки вредоносного трафика, использовать мощности устройства для майнинга или требовать выкуп за возвращение доступа к нему. При этом некоторые злоумышленники атакуют любые IoT-устройства, а другие — только технику определенного типа, способную выполнять интересующие их задачи. Ниже мы приводим виды вредоносного ПО для IoT в зависимости от его цели.

**DDoS-ботнеты**

Наиболее распространенный вид вредоносного ПО для IoT-устройств — троянские программы, перехватывающие контроль над устройством для ведения DoS-атак на различные сервисы. Для DDoS-зловредов нет разницы, какие устройства атаковать. Функциональностью, которая интересует злоумышленников, — способностью отправлять запросы по сети — обладают все. Значительная часть подобных зловредов — это модификации кода Mirai, но существует и множество других семейств, различающихся методами распространения и закрепления на устройстве.

Так, вредоносное ПО RapperBot, хотя и позаимствовало некоторые части кода Mirai, по большей части состоит из уникального кода. Оно способно на [умный перебор паролей](https://securelist.ru/crimeware-report-uncommon-infection-methods-2/107293/#rapperbot-171-umnyj-podbor-parolej-187), основанный на анализе получаемого от Telnet-сервиса первого сообщения с запросом аутентификационных данных. По этому сообщению зловред может распознать тип устройства и перебирать только пароли к устройствам этого типа, что значительно повышает эффективность его самораспространения.

**Программы-вымогатели**

В отличие от DDoS-зловредов, вымогатели атакуют преимущественно IoT-устройства, на которых есть пользовательские данные — NAS-хранилища. Одним из ярких примеров IoT-шифровальщика является DeadBolt, [поразивший тысячи устройств QNAP NAS](https://arstechnica.com/information-technology/2022/09/new-wave-of-data-destroying-ransomware-attacks-hits-qnap-nas-devices/) в 2022 году. Для атаки использовалась уязвимость [CVE-2022-27593](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27593), позволяющая злоумышленникам модифицировать системные файлы на устройстве. В результате пользовательские файлы оказались зашифрованы, а интерфейс устройства заблокировало сообщение о том, что для восстановления данных нужно заплатить выкуп в размере 0.03 BTC. Производитель выпустил обновление, закрывающее уязвимость, но подобные атаки все еще остаются актуальными.

**Майнеры**

Несмотря на относительную неэффективность майнинга на IoT-устройствах, связанную с их низкой вычислительной мощностью, злоумышленники предпринимали попытки [добывать криптовалюту Bitcoin](https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/) в ходе кампаний Mirai. Однако эти попытки не получили широкого распространения.

**DNS changer**

Атакующие могут использовать скомпрометированные IoT-устройства и для атаки на подключающихся к ним пользователей. Так, в 2022 году в ходе вредоносной кампании Roaming Mantis (также известной как Shaoye) злоумышленники [распространяли](https://securelist.com/roaming-mantis-dns-changer-in-malicious-mobile-app/108464/) приложение для Android, одной из функций которого была смена настроек DNS на Wi-Fi-роутерах через интерфейс администрирования. Зловред получал доступ к роутеру, если на нем использовались учетные данные по умолчанию, например admin:admin. На подходящем устройстве он менял конфигурацию так, чтобы роутер использовал сервер DNS, подконтрольный злоумышленнику. Этот сервер перенаправлял всех, кто подключался к роутеру, на ресурс, определяющий ОС клиента: если устройство работало под управлением Android, ресурс раздавал вредоносные файлы APK, а пользователей iOS перенаправлял на фишинговые страницы.

**Прокси-боты**

Также довольно широко распространено использование зараженных устройств в качестве прокси-серверов — промежуточных узлов в сети, перенаправляющих трафик злоумышленника через себя, таким образом затрудняя его отслеживание. Чаще всего такие прокси-серверы используются для рассылки спама, обхода antifraud-систем и совершения различных сетевых атак.

**Вредоносное ПО для IoT: конкуренция и персистентность**

Одна из основных особенностей вредоносного ПО для IoT — существование множества различных семейств, основанных на обнаруженном в 2016 году зловреде Mirai, исходный код которого был опубликован на одном из подпольных форумов. Это привело к быстрому развитию сотен модификаций, различающихся способами ведения DoS-атак, словарями для перебора учетных данных и выбором уязвимостей для самораспространения.

Большое количество игроков, в свою очередь, привело к жесткой конкуренции среди киберпреступников, причем не только специализирующихся на DDoS, но и в целом нацеленных на интернет вещей. Поэтому IoT-зловреды постепенно начали включать в себя функции для «нейтрализации» конкурентов непосредственно на зараженном устройстве и предотвращения его повторного заражения.

Наиболее популярная среди злоумышленников тактика закрепления доступа за собой — добавление правил сетевого экрана, блокирующих попытки подключения к устройству; несколько реже используется отключение сервисов удаленного управления устройством. Для борьбы с конкурентами, уже присутствующими на устройстве, обычно применяется ряд методов обнаружения, например проверка имен процессов, используемых ими портов и анализ памяти на «вредоносные» паттерны. Если IoT-зловред что-то обнаружит, он завершает чужие процессы и удаляет чужие файлы. Так злоумышленники борются друг с другом за контроль над устройством.

**Прочие угрозы, связанные с небезопасностью устройств IoT**

Как мы видели из объявлений о покупке-продаже доступа к скомпрометированным IoT-устройствам, среди типов устройств, интересующих злоумышленников, встречаются подключенные к интернету видеокамеры. Способы монетизации доступа к камере могут быть разными. Ее могут использовать не только как «компьютер» (например, для майнинга криптовалюты или размещения вредоносного ПО для организации DDoS-атак) или «маршрутизатор» («прокси» или VPN для анонимизации различной вредоносной деятельности), но и (внезапно!) по прямому назначению.

Показателен [недавний инцидент](https://t.me/moscowmi/14898) с жительницей московской области, обнаружившей на китайских вебсайтах материалы приватного характера, сделанные с домашней видеокамеры, которую она приобрела на AliExpress для наблюдения за собакой.

Исследователь безопасности Пол Маррапезе (Paul Marrapese) изучил пользовательский сегмент видеокамер и выяснил, что проблемы информационной безопасности в них присутствуют и, к сожалению, производители устройств их далеко не всегда исправляют. Например, он обнаружил  критические уязвимости в протоколах и прошивках некоторых видеокамер, причем [один из вендоров так и не вышел на связь для устранения уязвимостей](https://hacked.camera/cves/).

Кроме того, хочется отметить, что часто производители подобных видеокамер используют различные реализации P2P-протоколов (peer-to-peer-, пиринговых). Такие, например, как Shenzhen Yunni iLnkP2P и CS2 Network P2P, которые используются на более чем пятидесяти миллионах устройств. Эти реализации, в свою очередь, имеют слабое шифрование трафика или не шифруют его вовсе, что дает злоумышленнику возможность совершить атаку типа MitM (Man-in the-Middle) — прослушивать трафик устройства, чтобы узнать учетные данные пользователя или перенаправить на свои ресурсы видеопоток, идущий с камеры.

Согласно [исследованию коллег из Trend Micro](https://www.trendmicro.com/vinfo/ie/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras), подглядывание за жизнью владельцев видеокамер — далеко не редкость. При этом стоит помнить, что помимо собственно камер инструментом шпионажа могут стать многие другие IoT-устройства, которые, несмотря на то что их основное назначение не связано с видеонаблюдением, также оснащены камерой. В частности, возможность записывать аудио и видео в режиме реального времени есть у большинства умных кормушек для питомцев. Спрос на них растет, число моделей множится, заполняя новый сегмент рынка, однако вендоры не всегда уделяют должное внимание их защите. Так, [исследование кормушки](https://securelist.com/smart-pet-feeder-vulnerabilities/110028/) из популярной линейки показало целый ворох уязвимостей и проблем безопасности, эксплуатация которых превращает устройство в инструмент подглядывания за хозяевами питомца и открывает другие возможности для злоумышленников.

Другой тип IoT-устройств, требующих особого внимания к вопросам безопасности, — умные устройства для детей. К сожалению, не все вендоры серьезно подходят к защите таких устройств. Впервые мы столкнулись с проблемой их небезопасности несколько лет назад, когда один из производителей умных детских часов заказал у нас [сервис по исследованию зрелости безопасности продукта](https://ics-cert.kaspersky.com/services/) по методологии [IoT Security Maturity Model от Industry IoT Сonsortium](https://www.iiconsortium.org/smm/). Аттестацию вендор тогда провалил, и сертификата мы не выдали — проблемы безопасности в продукте превращали его, по сути, в устройство слежения за ребенком и за всем(и), что (кто) находится в его окружении.

Проблема недостаточной защищенности IoT-устройств характерна не только для пользовательского рынка. Системы промышленного IoT могут также содержать тривиальные уязвимости, а рекомендованные вендором настройки — быть небезопасными.

Распространенной ошибкой конфигурации промышленных устройств являются пароли по умолчанию. Так, например, они вместе с весьма небезопасными рекомендациями по подключению и настройке были [приведены в документации](https://ics-cert.kaspersky.ru/publications/blog/2022/03/30/uyazvimosti-v-reshenii-tekon-avtomatika-bez-otvetstvennoe-raskrytie-i-masshtab-bedstviya/) производителя медиаконвертеров  для подключения лифтового оборудования к системам мониторинга в диспетчерских. Кроме того, наши исследователи обнаружили в устройствах уязвимости, эксплуатация которых доступна даже не слишком квалифицированным злоумышленникам и позволяет им получить полный контроль над конвертером. Небезопасные настройки из рекомендаций впоследствии убрали. Однако производитель устройств, вначале продемонстрировавший оперативность в устранении проблем безопасности, растерял по дороге всю ответственность, и многие из обнаруженных нами уязвимостей по сей день остаются неисправленными — спустя более года после того, как мы предоставили вендору информацию о них.

Из приведенных выше примеров может сложиться впечатление, что мы считаем все устройства IoT небезопасными, а их производителей — пренебрегающими культурой безопасной разработки. Однако это не так. Например, компания Bosch успешно [получила наш сертификат зрелости безопасности](https://ics-cert.kaspersky.com/smm-assessment/?item=bosch-ip-video-surveillance-camera-platforms) для умной видеокамеры, предназначенной для использования на промышленных предприятиях. Нам бы очень хотелось, чтобы как можно больше вендоров IoT-устройств, в том числе систем промышленного IoT, включали кибербезопасность своих продуктов в число первых приоритетов.

**Заключение**

IoT-устройства интересуют злоумышленников по целому ряду причин: их можно использовать для DDoS-атак, перенаправлять через них трафик или подсматривать за владельцами с помощью встроенных видеокамер. NAS-хранилища также могут быть целью вымогателей, а роутеры привлекательны для злоумышленников, нацеленных на подключенные к ним устройства, например на мобильные устройства в общественной Wi-Fi-сети или на устройства локальной сети жертвы.

Злоумышленники непрерывно атакуют IoT и предлагают в даркнете услуги, связанные с такими атаками. Тем не менее большинство подключенных устройств, в том числе в промышленной среде, по-прежнему остается легкой добычей: для подключения используются пароли по умолчанию, в устройствах находят уязвимости, не все из которых получают патчи от производителя. Вендорам IoT-устройств, как домашних, так и промышленных, следует ответственно подходить к безопасности своей продукции и внедрять механизмы защиты от кибератак на стадии разработки. В частности, мы рекомендуем отказаться от практики использования паролей по умолчанию и генерировать уникальные пароли для каждого конкретного устройства. Также следует регулярно выпускать патчи к обнаруженным уязвимостям.