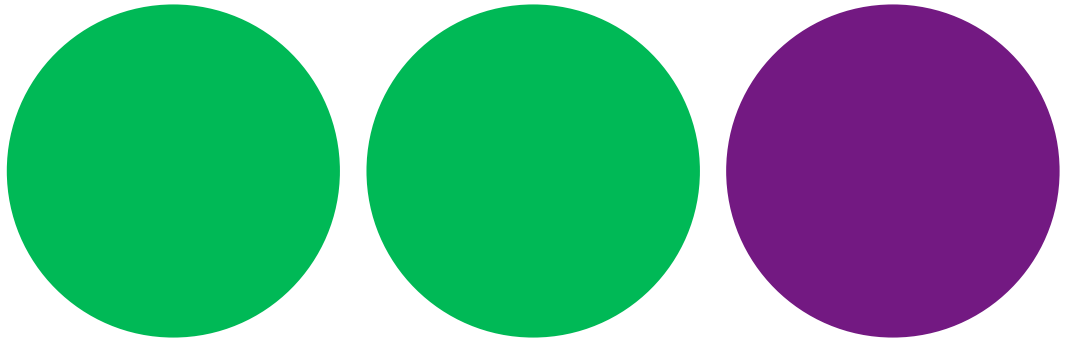


МегаФон Антивзлом

Приложение для защиты мобильных устройств от вредоносных сообщений, вирусов и сетевых атак

МегаФон

Основные типы мобильных атак

Перехват данных в Wi-Fi сети – при подключении к незащищённому или взломанному Wi-Fi трафик может быть перехвачен. Потенциально опасными являются общественные сети и другие сети без пароля. При подключении к такой сети пароли от банковских приложений и социальных сетей окажутся в руках мошенников за пару минут.

Вирус – вредоносное приложение, которое заражает устройство и мешает его работе. Может замедлять или блокировать устройство, шифровать данные и доставлять прочие неприятности. Защищаться от вирусов необходимо, но для полноценной защиты только антивируса уже недостаточно.

Троянская программа (троян) – программа, которая отслеживает действия пользователя и передает их злоумышленнику. Получает доступ к датчикам на устройстве, таким как камера, микрофон и динамик.

Фишинг – атаки, в которых злоумышленник выманивает у жертвы логин и пароль. Например, создается копия известного пользователям сайта — банка, портала государственных услуг или рабочей почты. Ставка делается на невнимательность пользователя: он вводит свои данные, не проверяя адрес. Зачастую ссылки на такие сайты-двойники приходят на почту или в SMS.

МегаФон

Сетевые атаки

Основной вид мобильных сетевых атак

Man-in-the-Middle – злоумышленник внедряется в Wi-Fi сеть и получает все данные, которые вводит пользователь. А еще он может их изменять.

Основной инструмент MitM-атак

SSL-Strip – с зашифрованных протоколом HTTPS сайтов снимается шифрование, и злоумышленник может видеть все действия пользователя.

Как получают доступ к устройству?

При автоматическом подключении устройство выбирает сеть по названию. Общественные сети, например Wi-Fi в метро, легко подменить: злоумышленник создаст точку доступа с таким же именем, и устройство не увидит разницы. Оно подключится к такой сети, и все данные будут передаваться через сеть злоумышленника. Та же опасность подстерегает и при подключении к открытым сетям.

Чем опасны?

Собирают логины и пароли

Крадут информацию о действиях пользователя – могут читать, изменять и блокировать сообщения и команды

Изменяют передаваемые данные, например, могут добавить ссылку на вредоносное ПО

МегаФон

Вирусы

Основные виды вирусов

– Обычные вирусы – портят устройство и снижают производительность
– Шифровальщики – шифруют данные на устройстве или стирают их
– Вымогатели – шифровальщики, требующие денег за расшифровку файлов

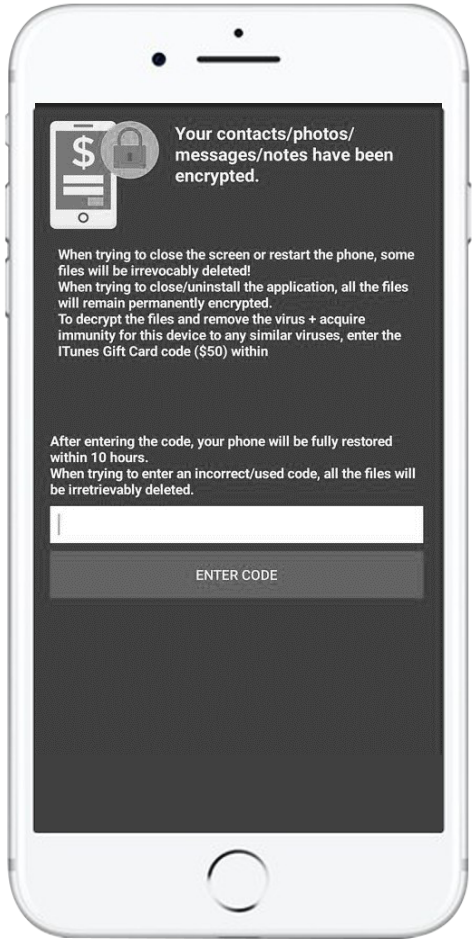
Как попадают на устройство?

Маскируются под известные приложения и файлы. Пользователь сам непреднамеренно их скачивает и устанавливает.

Распространяются на форумах в интернете, торрент-трекерах, через сообщения и по электронной почте.

Чем опасны?

– Воруют деньги с мобильного и банковских счетов
– Крадут информацию и собирают данные о действиях пользователя
– Мешают нормальной работе устройства или блокируют его



Пример вируса-вымогателя

МегаФон

Троянские программы

Примеры программ

Triada – опасный модульный троян на Android, который очень сложно обнаружить и устранить. Становится частью каждого установленного приложения.

Hesperbot – банковский троян для Android, Symbian и Blackberry, контролирующий SMS онлайн-банкинга.

AceDeceiver – первый троян на iOS, распространившийся с помощью уязвимости в системе DRM.

Как попадают на устройство?

Вредоносный код добавляется в стандартное приложение и работает параллельно с ним.
Непреднамеренно скачиваются и устанавливаются самим пользователем или загруженным до этого трояном.

Чем опасны?

Воруют конфиденциальную информацию и читают переписку

Контролируют устройство, могут незаметно загружать новые трояны и выводить деньги со счетов

Собирают логины и пароли пользователя от социальных сетей, банковских счетов и других систем

Отслеживают окружающую обстановку и действия пользователя на устройстве

МегаФон

Фишинг

Phishing, от английского fishing – рыбалка

Стратегии выманивания данных

- Внешне похожие ссылки (mos.ru и rnos.ru)
- Внешне похожие сайты
- SMS-фишинг

Чем опасен?

- Передает ссылки на скачивание вирусов
- Собирает логины и пароли пользователя от социальных сетей, банковских счетов и пр.

Как попадают на устройство?

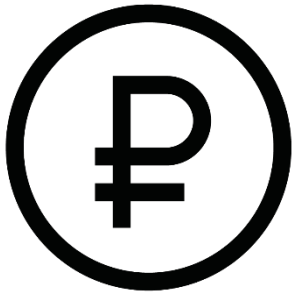
Ссылка на сайт-двойник может прийти в социальной сети, SMS или электронной почте. Зачастую на пользователя для более быстрого ввода данных оказывается психологическое давление (таймеры, опасность и прочее).

90% кибератак начинаются с фишинговой ссылки*

МегаФон

*2018 Data Breach Investigations Report

Последствия

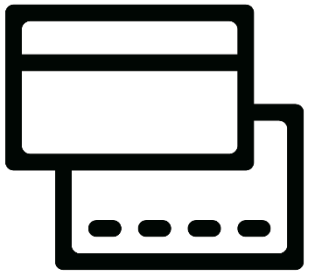


Кража денег

Использование банковских приложений в незащищенной сети позволяет злоумышленникам перехватить логины и пароли, что даёт им возможность совершать операции с вашего счета.

Блокировка устройства

Вирусы и программы-шифровальщики могут заблокировать устройство с целью получения выкупа за разблокировку. На устранение последствий уходит время, бизнес несет расходы, а сами данные могут быть утеряны безвозвратно.



Утечка данных

Вредоносное ПО или незащищенная сеть Wi-Fi могут привести к утечке важных для бизнеса данных: документов, логинов и паролей от корпоративных систем или персональной информации клиентов.

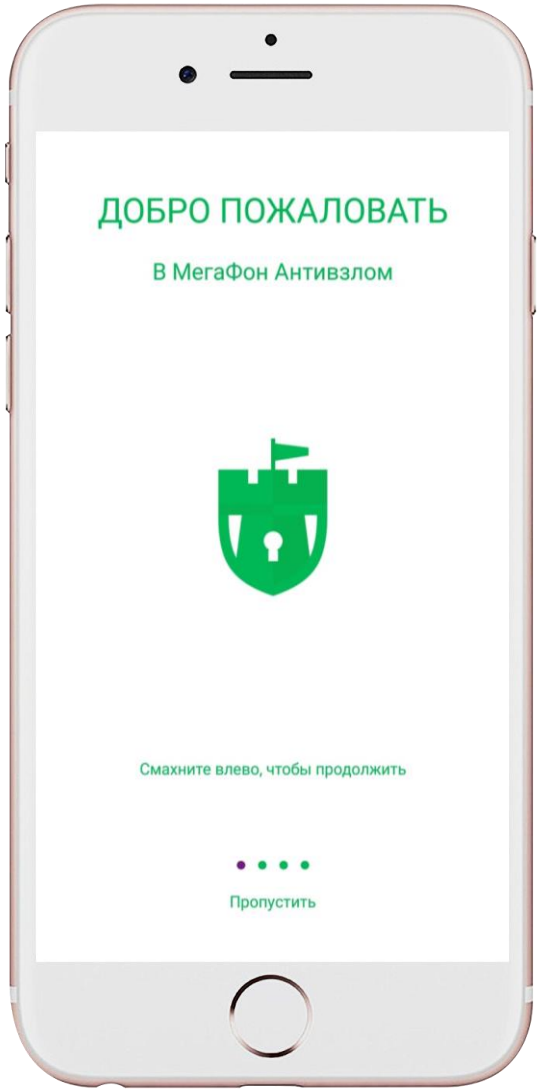
МегаФон

Решение

МегаФон Антивзлом – новое приложение для защиты мобильных устройств с функциональностью шире, чем у обычного антивируса. Защищает от всех основных типов мобильных атак.

Приложение построено на базе технологии Check Point семейства SandBlast – унифицированного кросс-платформенного решения для защиты от вредоносных программ и угроз нулевого дня.

Доступно для Android и iOS.



МегаФон

Преимущества Антивзлома

Функциональность	Антивзлом	Антивирус
Обнаружение и защита от вирусов	✓	✓
Блокировка фишинговых ссылок	✓	✓
Защита от сетевых атак	✓	
Обнаружение зараженных точек Wi-Fi	✓	
Защита от несанкционированного доступа к устройству	✓	
Блокировка вредоносных сайтов	✓	
Блокировка вредоносных модулей на сайтах	✓	
Версия для iOS	✓	

МегаФон

Функциональность

Защита от сетевых атак и обнаружение зараженных точек Wi-Fi

Антивзлом распознает атаки на уровне сети и уведомляет о них пользователя. Предупреждает о подключении к незащищенным и подозрительным сетям Wi-Fi, в которых злоумышленник может перехватить пользовательскую информацию.

Блокировка фишинговых ссылок и вредоносных модулей на сайтах

Антивзлом находит фишинговые ссылки в сообщениях и предлагает пользователю сразу же их удалить. Ограничивает переход по вредоносным ссылкам и блокирует вредоносные модули на сайтах. Выступает фильтром между интернет-ресурсом и устройством пользователя, предотвращая утечку данных.

Обнаружение файлов-шифровальщиков и прочих вредоносных файлов и приложений. Защита от вирусов

Антивзлом проверяет установленные приложения, установочные файлы и другие доступные данные на устройстве. Проверка происходит при первоначальном сканировании, установке новых приложений и обновлений. Для сохранения заряда устройства непрерывного сканирования данных не производится, но уровень защиты остается неизменным.

Антибот и оценка конфигурации устройства

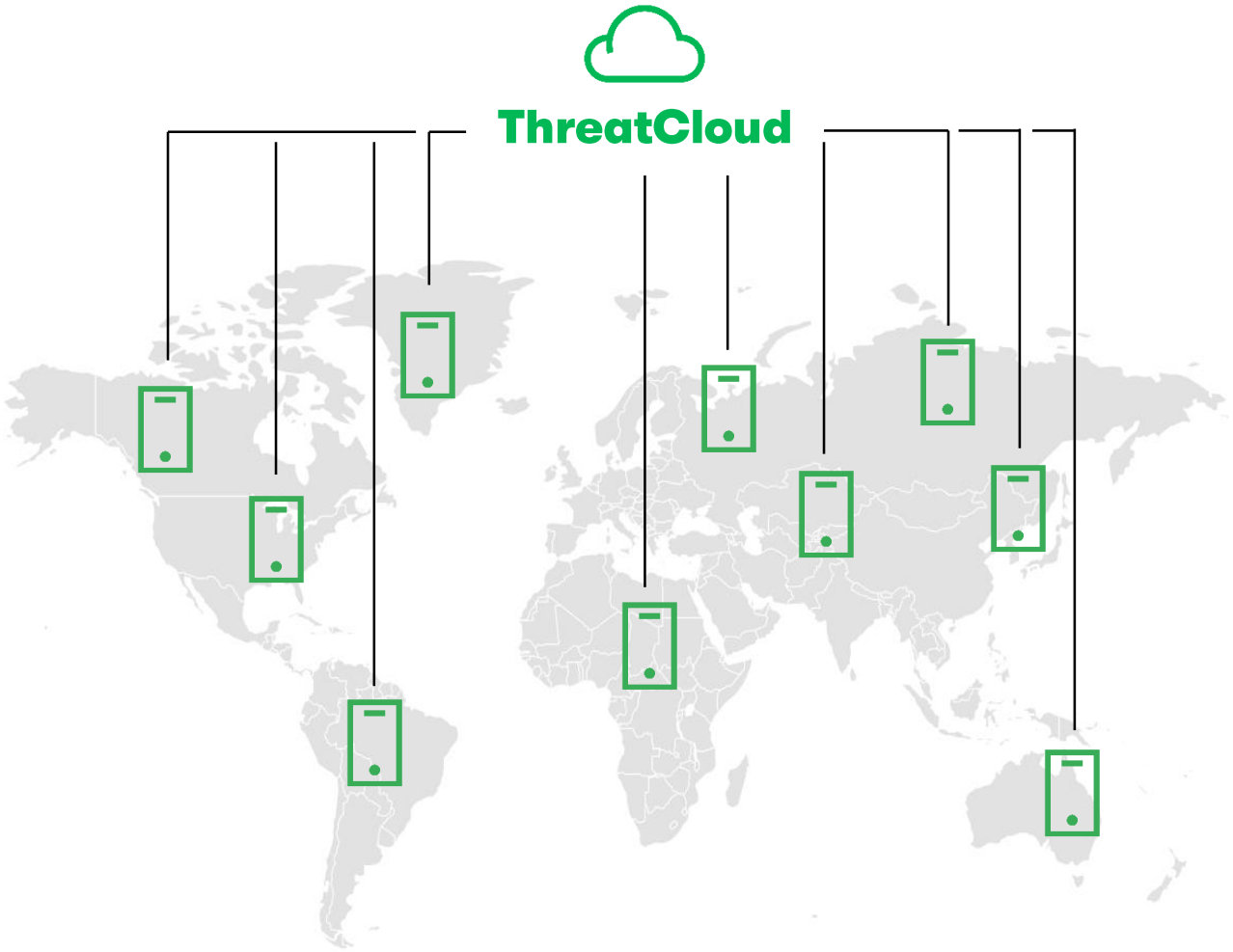
Антивзлом следит за наличием обновлений ОС, настройками устройства и приложениями, полученными из непроверенных источников. Предупреждает пользователя о наличии уязвимостей и предлагает пути их устранения. Это позволяет защитить устройство от несанкционированного доступа и предотвратить отправку данных в ботнет или использование устройства злоумышленниками для DDoS-атак.

МегаФон

ThreatCloud

Антивзлом проверяет угрозы по базе ThreatCloud

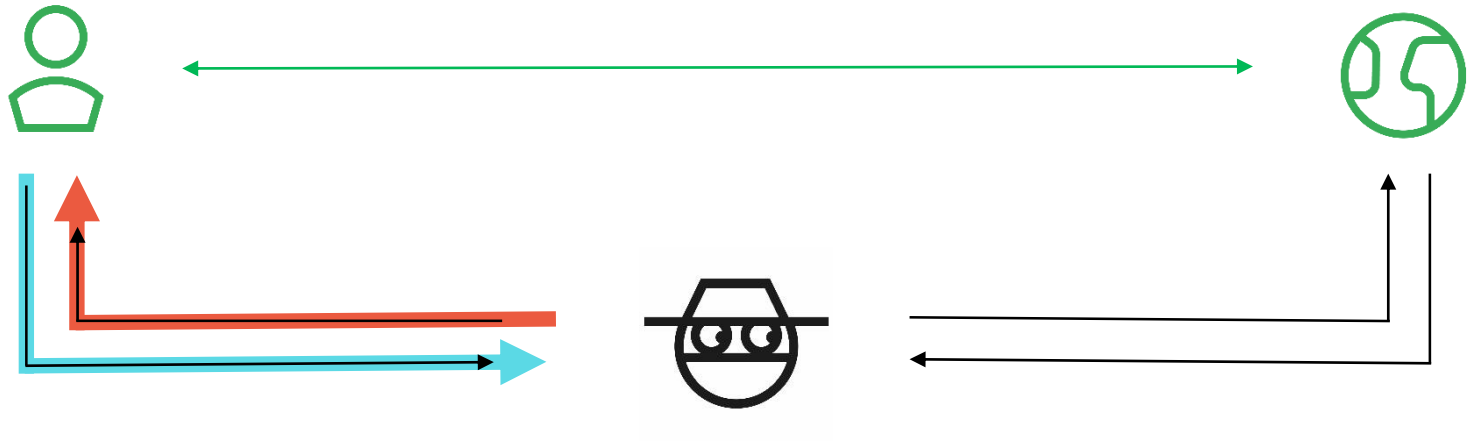
Это крупнейшей база киберугроз, которая собирает данные по всему миру 24/7. Действия пользователя поступают в облако, где среди них выбираются наиболее значимые. При обнаружении вредоносного ПО пользователь сразу же уведомляется и получает предложения по его обезвреживанию. Также облако предоставляет рекомендации по настройке устройства для оптимального уровня защиты. ThreatCloud обеспечивает работу функций антифишинга, безопасного интернета и URL сканирования.



МегаФон

Как Антивзлом защищает от сетевых атак?

Антивзлом располагает базой SSL-сертификатов для ряда доверенных сайтов. При подключении к Wi-Fi сети он отправляет на них запрос и проверяет целостность входящего SSL-сертификата. Если она нарушена, то сеть считается опасной. При обнаружении подозрительного поведения в сети, Антивзлом предлагает ее отключить.



Незашифрованное подключение

SSL сертификат

Сертификат злоумышленника

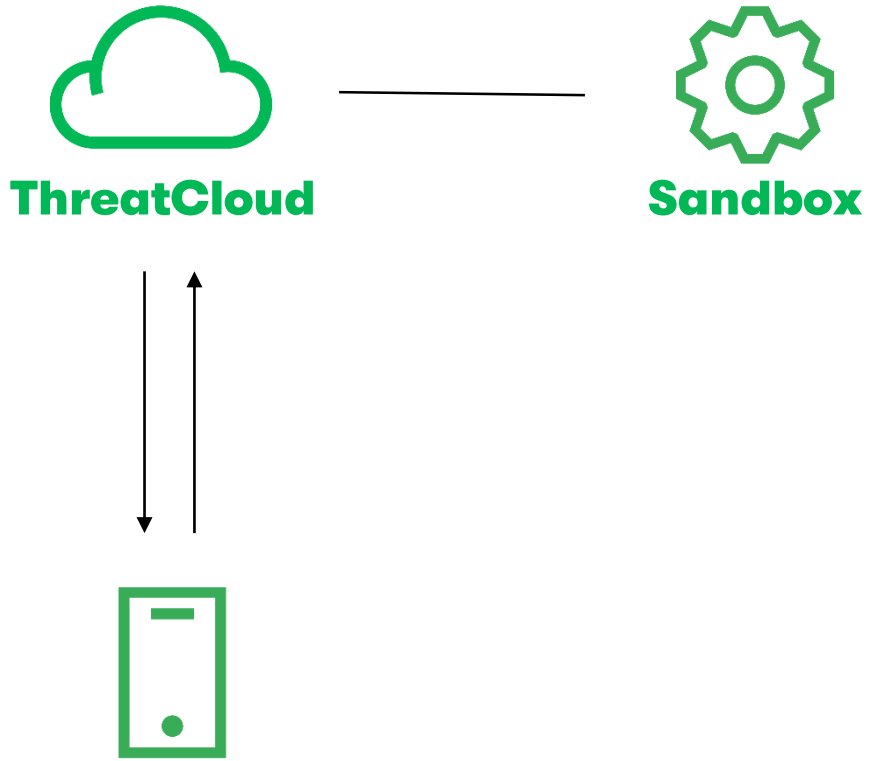
МегаФон

Как Антивзлом защищает от вирусов?

Вредоносный код в приложениях может быть найден во время сканирования по уникальной двоичной подписи (сигнатуре). Эти подписи, как и алгоритмы известных атак, хранятся в базе ThreatCloud.

Для обнаружения новых угроз (атаки нулевого дня) используется облачная песочница SandBlast. Это изолированное пространство, где новые приложения проверяются на наличие угроз. Алгоритм воспроизводит различные внешние условия и действия пользователя для выявления уязвимостей или вредоносного ПО.

При обнаружении вредоносного ПО выводится предупреждение с предложением его удалить. Пользователь сам решает, стоит ли принимать меры.

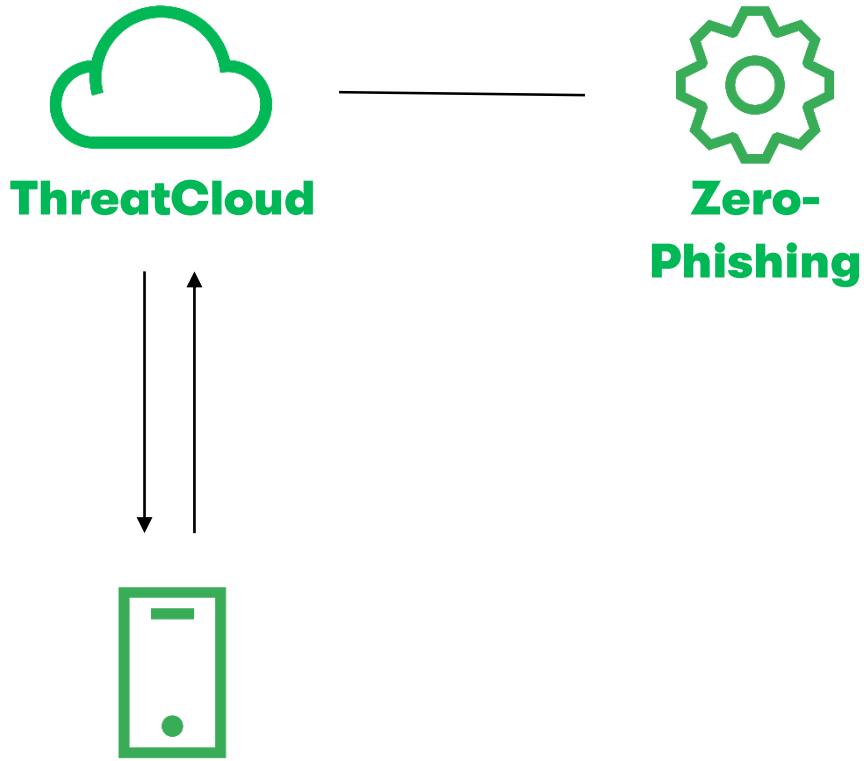


МегаФон

Как Антивзлом защищает от фишинга и вредоносных сайтов?

Антивзлом мгновенно обнаруживает и блокирует фишинговые атаки через электронную почту и SMS.
Он сканирует ссылки и сравнивает их с глобальной базой ThreatCloud – крупнейшей динамически обновляемой базой киберугроз. Также используется функция Zero-Phishing от CheckPoint, которая распознает новые фишинговые сайты и блокирует к ним доступ.

Тот же подход используется при блокировке вредоносных сайтов. Антивзлом сравнивает ссылки, по которым переходит пользователь на устройстве, с базой известных вредоносных сайтов ThreatCloud и предотвращает переход, если ссылка опасна.



МегаФон

Как Антивзлом защищает от несанкционированного доступа?

Определенные настройки конфигурации открывают уязвимости, которыми могут воспользоваться злоумышленники.

Антибот автоматически блокирует соединение между вредоносным ПО и командами его контролирующего сервера. Он изолирует вредоносное ПО и не дает ему контролировать устройство пользователя. Если устройство находится в зоне риска, Антивзлом не даст ему подключиться в корпоративную сеть.

МегаФон

Для нас важна ваша приватность

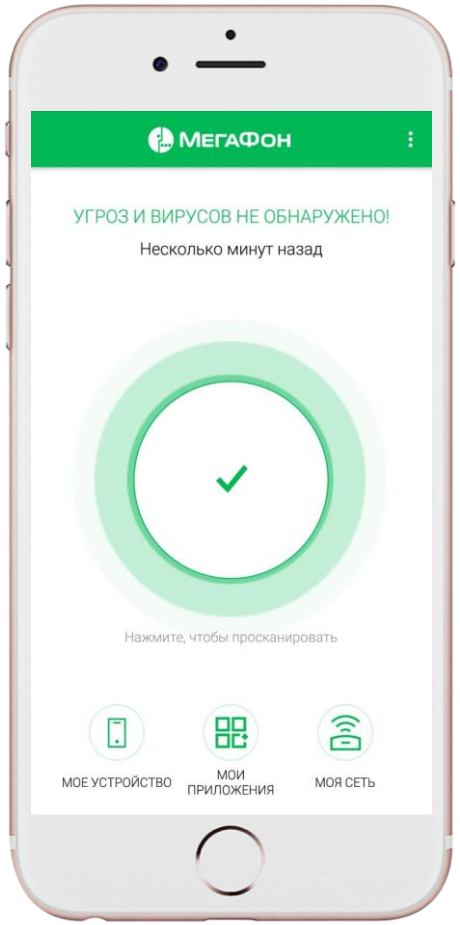
Антивзлом не сканирует личную информацию и не перенаправляет ее через внешний шлюз или прокси. Также не сканируются история браузеров, файлы и данные приложений.

После сканирования Антивзлом не хранит и не передает ваши данные. Ваша переписка остается только вашей, просто она станет безопасней.

При анализе ссылок сравниваются их зашифрованные значения. Информация о ваших действиях и посещаемых сайтах недоступна Антивзлому.

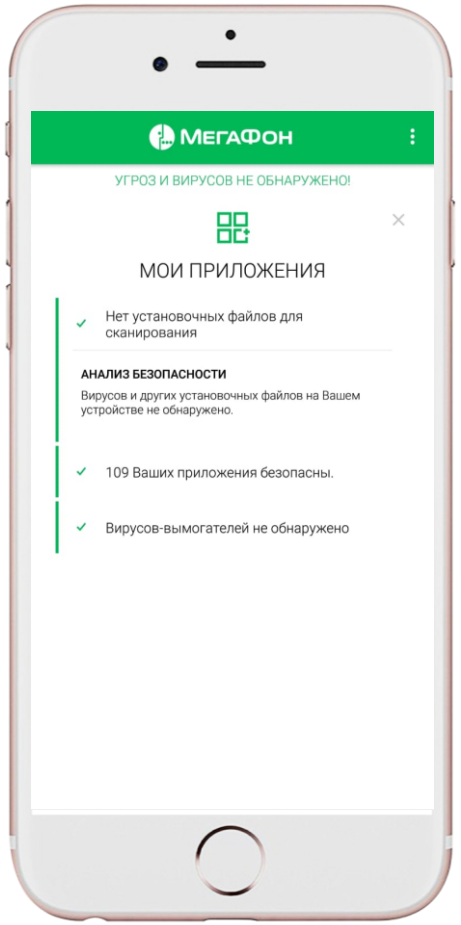
МегаФон

Интерфейс



Предупреждайте угрозы

Сканируйте устройство на наличие возможных угроз безопасности

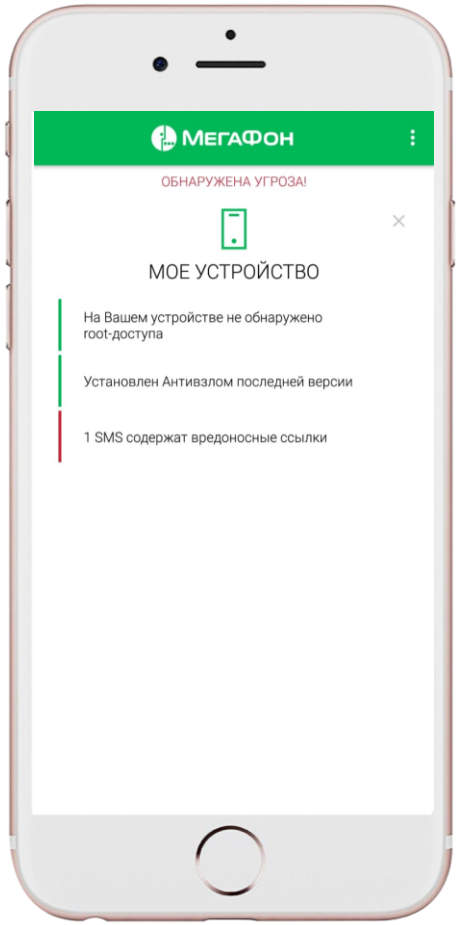


Проверяйте приложения на вирусы

Следите за установленными приложениями и получайте уведомления, если что-то не так

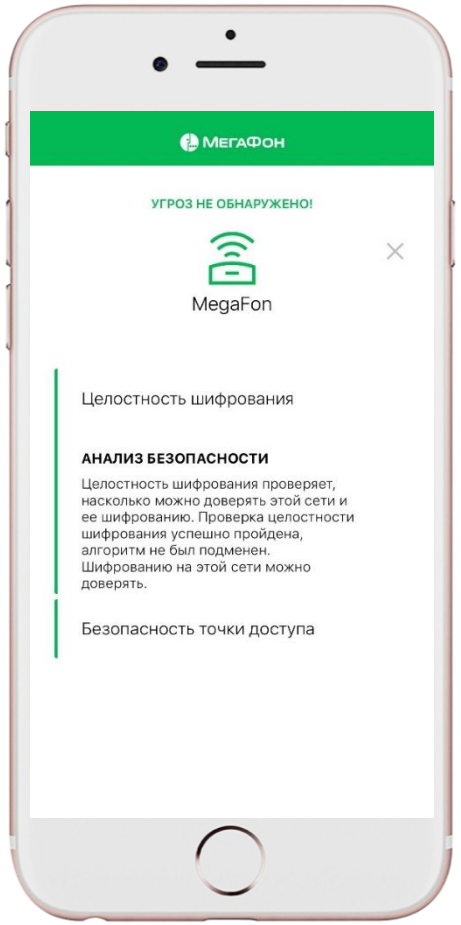
МегаФон

Интерфейс



Следите за безопасностью

Проверяйте доступные обновления и удаляйте вредоносные сообщения прямо из приложения



Контролируйте подключение

При обнаружении новой Wi-Fi сети убедитесь, что она не представляет угрозы

МегаФон

Как начать пользоваться

Для подключения услуги на устройства своих сотрудников:

1 → Выберите номера сотрудников, на которые вы хотите установить Антивзлом в МФ.Бизнес или ЛК B2B, и подключите услугу

2 → Выбранные сотрудники получат сообщение со ссылкой на приложение. Его нужно скачать

3 → На первом экране приложения надо ввести номер телефона и получить код активации

4 Следуйте шагам из руководства и подсказкам в приложении

Если вы сами управляете своими услугами и тарифным планом:

1 → Подключите себе услугу через приложение МегаФон Личный Кабинет: Услуги и опции -> Дополнительные услуги -> Другое

2 → Вам придет сообщение об успешном подключении услуги со ссылкой на приложение. Его нужно скачать

3 → На первом экране приложения надо ввести номер телефона и получить код активации

4 Следуйте шагам из руководства и подсказкам в приложении

МегаФон