positive technologies

knockin.ptsecurity.com

Проверить почту

PT Knockin

Онлайн-сервис проверки защищенности почты

Тестирование безопасности электронной почты

PT Knockin позволяет проверить и оптимизировать уровень защищенности вашей почты. Сервис симулирует атаки на почтовый сервер, проверяя настройки фильтрации, и дает методические рекомендации по повышению безопасности.

Все начинается с почты

Электронная почта — самый популярный способ доставки вредоносных программ для компрометации корпоративной среды.

Исследования показывают, что **более 57%** кибератак в России начинаются с вредоносных писем, и их число продолжает расти. Чаще всего инструментом для проникновения становятся файловые вложения, в которых могут содержаться шифровальщики, загрузчики, майнеры, вредоносные программы для удаленного управления и другие малвари.

Наиболее популярные у злоумышленников типы отправляемых файлов

- Архивы (.zip, .rar, .7z)
- Текстовые документы (.doc, .odt, .one)
- Статические веб-страницы (.html, .chm, .htm)
- Электронные таблицы (.xls, .xlsx)
- PDF-файлы
- Исполняемые файлы (.bat, .exe, .msi)
- Образы данных (.iso, .vhd, .vhdx)
- Файлы презентаций (.ppt, .pptx)

Почему почтовые средства защиты не всегда справляются

Любое изменение или обновление IT-систем (например, почтового сервера) может привести к изменению параметров почтовых средств защиты и правил фильтрации. Нет гарантий, что после этого в обороне вашей почты не появятся уязвимости, которые долгое время могут оставаться незамеченными.

Кроме того, злоумышленники постоянно модифицируют вредоносное ПО и придумывают новые тактики и техники для обхода традиционных средств защиты. С развитием искусственного интеллекта стали появляться вредоносные программы, способные самостоятельно изменять свой исходный код, чтобы скрываться от статических инструментов анализа, основанных на YARA-правилах. Искусственный интеллект также используется для генерации фишинговых писем и проведения разведки потенциальных целей.

Превентивная проверка безопасности

Чтобы быть уверенным, что почтовые средства защиты работают корректно, рекомендуется регулярно тестировать электронную почту на проникновение. Для этого подойдет сервис, имитирующий доставку зловредов. PT Knockin тестирует средства контроля безопасности почты, отправляя письма с эксплойтами, замаскированными под часто используемые вложения. Сервис моделирует реальные атаки на ящики сотрудников компании и показывает, могут ли вредоносные письма обойти первую линию защиты.

Как работает PT Knockin

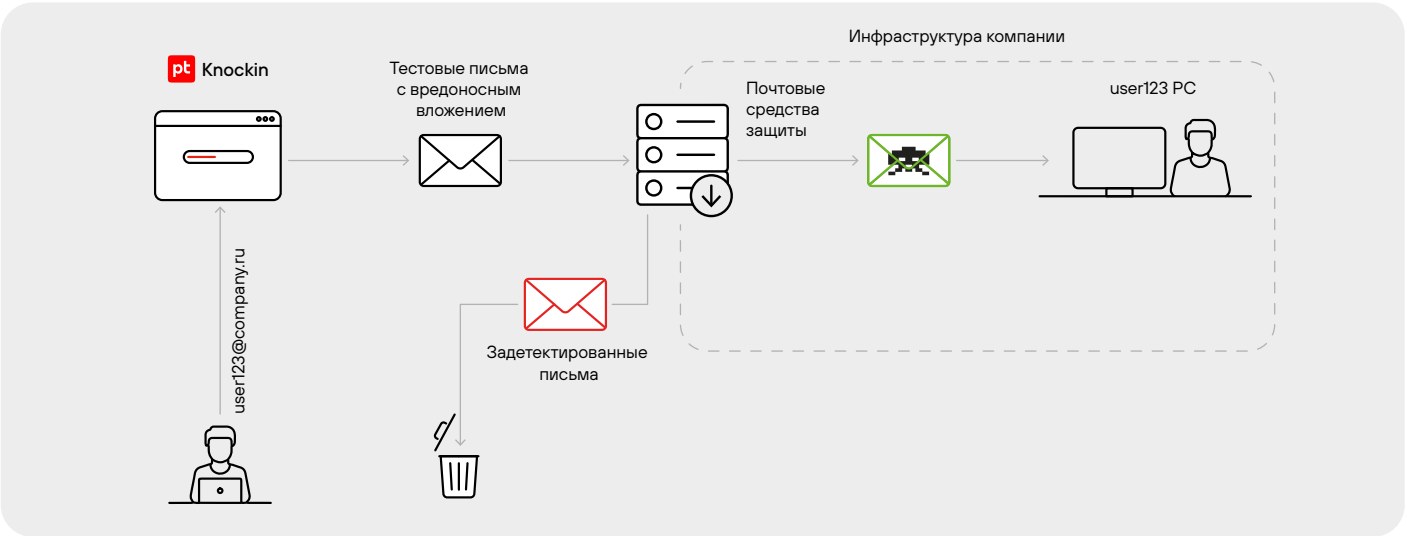
Сервис доступен онлайн — для старта работы нужно ввести адрес почты с корпоративным доменом и пройти аутентификацию. После регистрации вы можете выбрать типы атак, на которые хотите протестировать ваш ящик, или воспользоваться всеми доступными вариантами проверки.

После старта симуляции на почту начнут приходить тестовые письма с имитацией вредоносных вложений. Если средства защиты пропустят письма с такой нагрузкой — значит, в системе фильтрации есть уязвимости, которые нужно исправить.

После того как вы отметите в личном кабинете, какие атаки оказались успешными, PT Knockin сформирует отчет о состоянии защищенности почты. Сервис выявляет проблемы в работе почтового шлюза, песочницы, межсетевого экрана уровня веб-приложений и других средств защиты и предоставляет рекомендации для их правильной настройки. Повторное тестирование покажет, как сработали улучшения, а регулярная проверка позволит поддерживать постоянную защищенность электронной почты.

Ключевые особенности PT Knockin

- **Проверяет защищенность почты от самого популярного у злоумышленников вредоносного ПО.** В арсенале сервиса более 100 семплов с вредоносной полезной нагрузкой, замаскированных под файлы разных форматов.
- **Доступен онлайн.** Для проверки не требуется скачиваний и установок — достаточно перейти в веб-консоль на странице **knockin.ptsecurity.com,** ввести адрес корпоративного ящика и начать проверку.
- **Безопасен для корпоративной сети.** Все вредоносные программы, которые использует PT Knockin, только симулируют атаки и не могут нанести реального вреда инфраструктуре.
- **Защищен от попадания в спам-листы.** Использует для отправки проверочных писем разные адреса, которые постоянно изменяются, что позволяет достоверно проверить защищенность корпоративного сервера.
- **Формирует подробный отчет с рекомендациями** по устранению недостатков почтовой защиты, что позволяет принять оперативные меры для усиления барьера.



Проверить почту

О Positive Technologies

Positive Technologies — лидер рынка результативной кибербезопасности, ведущий разработчик продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют около 4000 организаций по всему миру.

positive technologies