Kaspersky Network Security Threat Data Feeds

kaspersky активируй будущее

Одной защиты конечных точек недостаточно – усиливайте вашу защиту на уровне сети.

Почему это важно:

- Эффективная защита от различных типов атак должна быть многоуровневой
- Не все конечные точки в вашей сети будут защищены, например, критически важные серверы или устройства в промышленной сети
- Некоторые «защищенные» узлы могут не иметь актуальных сигнатур / хэшей / правил обнаружения

Потоки данных для сетевых средств защиты

Почти в каждой компании сегодня есть межсетевой экран нового поколения (NGFW). Это одно из самых эффективных современных средств сетевой безопасности, повышающее уровень защиты корпоративных сетей от кибератак.

Большинство NGFW способны не только использовать внутренние знания о киберугрозах, но и обладают функциональностью, позволяющей использовать динамические списки индикаторов компрометации (IoC) из внешних источников для блокирования киберугроз в режиме реального времени

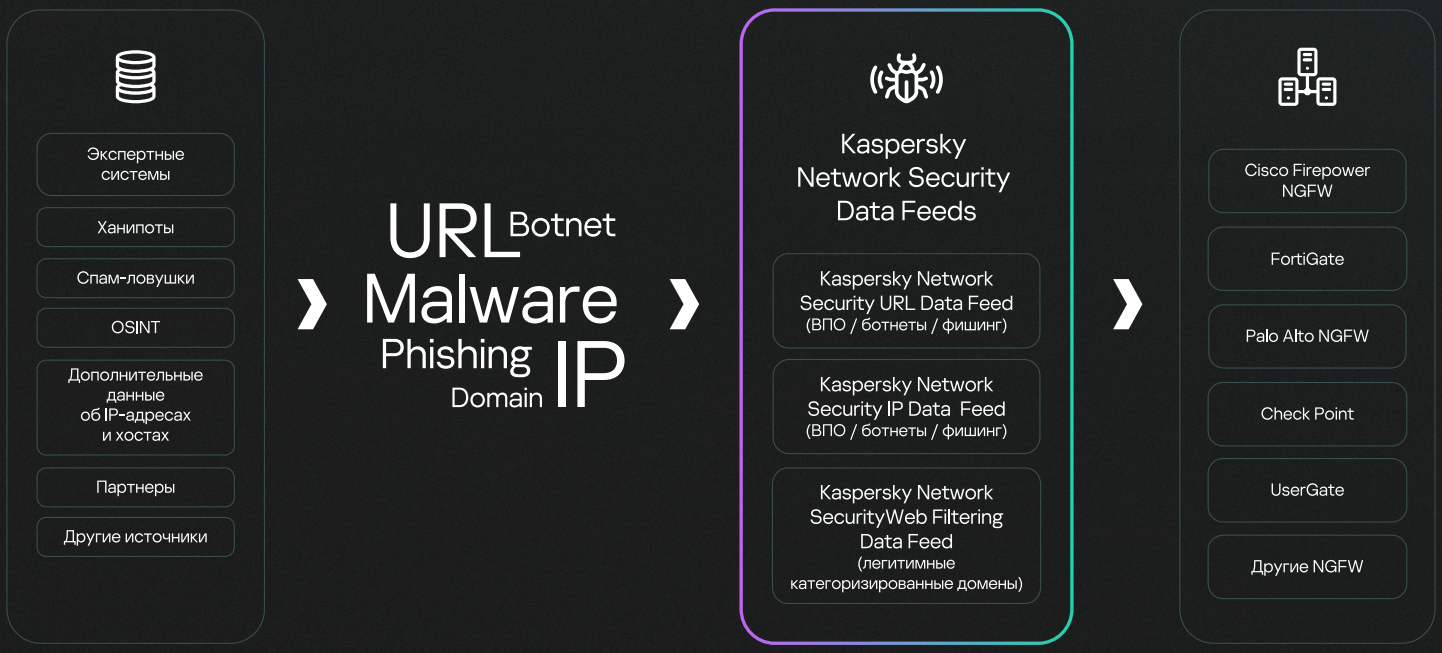
Быстро перенастраивать правила обнаружения NGFW с целью всегда опережать противников практически невозможно. Вот почему так важны внешние данные об угрозах – они привносят в вашу корпоративную сеть дополнительный элемент защиты, усиливающий используемые средства обеспечения безопасности.

«Лаборатория Касперского» предлагает специально созданные коллекции IoC, которые при импорте в NGFW значительно повышают уровень защиты корпоративной сети от наиболее распространенных угроз, не требуя сложной интеграции и настройки, сохраняя текущую топологию сети.

Kaspersky Network Security Threat Data Feeds содержат регулярно обновляемые списки различных типов индикаторов (IP-адресов и доменов). Использование этой информации позволяет контролировать / блокировать доступ пользователей к опасным сетевым ресурсам.

Подробнее

Интеграция со средствами сетевой защиты



Сбор и обработка данных

Kaspersky Network Security Data Feeds состоят из нескольких потоков данных, каждый из которых посвящен определенному типу киберугроз. В них содержатся списки IP-адресов с наивысшей оценкой угроз, а также доменные имена верхнего и второго уровней ресурсов, которые распространяют вредоносное ПО, выступают в качестве командно-контрольных центров ботнетов (C&C), размещают фишинговые ресурсы или относятся к нежелательным категориям.

Данные собираются из разнообразных и высоконадежных источников, таких как сеть Kaspersky Security Network, собирающая данные от миллионов пользователей по всему миру, веб-краулеры, сервис мониторинга ботнетов, сервисы получения данных об IP адресах и хостах и другие.

Полученные данные тщательно анализируются командами исследователей угроз и обрабатываются современными автоматизированными системами, такими как «песочницы», эвристические движки, инструменты сходства, превращаясь в гарантированно проверенную и актуальную информацию.

Особенности

Обновление в реальном времени

Данные автоматически генерируются в режиме близкому к реальному времени, что обеспечивает высокий уровень обнаружения и точности. Сеть KSN обеспечивает видимость значительной доли всего интернет-трафика, охватывая десятки миллионов пользователей в более чем 213 странах

Бесшовная интеграция

Поддержка популярных NGFW:

- Cisco
- FortiGate
- Palo Alto
- Check Point
- UserGate
- NGFW других производителей (с функциональностью внешних динамических списков с поддержкой базовой аутентификации)

Защищенная аутентификация

Потоки данных предлагают ряд методов аутентификации, отвечающих различным требованиям безопасности и предпочтительным интеграциям

Простота внедрения

Дополнительные пошаговые руководства по настройке для каждой поддерживаемой NGFW и техническая поддержка обеспечивают простоту настройки и немедленное получение выгоды

Бесперебойность

Потоки данных генерируются и контролируются инфраструктурой с высокой отказоустойчивостью, что обеспечивает постоянную доступность

100% проверенные данные

Данные предварительно проходят тщательную проверку и фильтрацию, что гарантирует их актуальность и практически исключает ложноположительные срабатывания

Преимущества

Усиление защитных решений

за счет доступа к постоянно обновляемым IoCs для автоматической блокировки наиболее распространенных киберугроз

Предотвращение утечек

конфиденциальных данных и интеллектуальной собственности с зараженных компьютеров за пределы вашей организации

Блокирование угроз

для защиты вашей организации от киберугроз и поддержания непрерывности бизнеса

Kaspersky Threat Data Feeds

Подробнее

www.kaspersky.ru

#kaspersky
#активируй будущее