Обогащаем NGFW данными об угрозах в новых ИБ-условиях

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Наши данные об угрозах собираются из множества надёжных источников:

- Сеть Kaspersky Security Network
- Собственные поисковые роботы
- Сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами, их целями и действиями)
- Ловушки для спама
- Данные исследовательских групп и партнёров

В подготовке потоков данных участвуют сотни специалистов: аналитики безопасности со всего мира, эксперты из глобального центра исследования и анализа угроз (GReAT) и ведущие команды отдела исследований и разработки (R&D) «Лаборатории Касперского». Так интегрированные с нашими потоками данных об угрозах решения NGFW оперативно получают достоверную и релевантную информацию и тем самым повышают уровень безопасности организаций.

Новый подход к NGFW

Как сетевым экспертам и ИБ-специалистам поддерживать корпоративные межсетевые экраны следующего поколения (NGFW) в эффективном работоспособном режиме, если производители этих решений ушли с российского рынка, ввели различные ограничения и перестали обновлять свои устройства?

«Лаборатория Касперского» готова помочь справиться с этой проблемой и наладить поставки данных об угрозах (дата-фидов) прямо в NGFW.

Kaspersky Threat Data Feeds

позволит службам сетевой и информационной безопасности получать релевантные дата-фиды для поставки в уже приобретённое оборудование NGFW — и сохранить, таким образом, вложенные инвестиции. Благодаря этому решению ИБ-специалисты восполнят потери качественной аналитики за счёт автоматизированного процесса загрузки дата-фидов в сетевые устройства.

Kaspersky Threat Data Feeds

- IP reputation feed
- Malicious hash feed
- Malicious URL feed
- Phishing URL feed
- C&C URL feed
- Ransomware URL feed
- И другое

NGFW

Межсетевой экран следующего поколения

Другие производители NGFW

Kaspersky Threat Data Feeds обогатит NGFW потоками данных об угрозах, содержащими подозрительные и вредоносные IP-адреса, веб-адреса и хеши файлов

Kaspersky Threat Data Feeds протестированы и работают со следующими сериями NGFW (что не исключает интеграции с другими решениями этого класса):

Вся информация тщательно проверяется и очищается в режиме реального времени с помощью различных методов предварительной обработки: статистических критериев, песочниц, средств эвристического анализа, инструментов для определения сходств, профилирования моделей поведения и проверки аналитиками.

Производитель оборудования	Поддерживаемые устройства	Поддерживаемые потоки данных об угрозах «Лаборатории Касперского»
cisco	Все модели NGFW, работающие под управлением Cisco Firepower Management Center версии 6.2.3 и выше, с модулем Threat Intelligence Director	• IP-адреса подозрительных и вредоносных хостов (IP reputation) • URL командных серверов ботнетов Botnet C&C URL) • URL вредоносных сайтов (Malicious URL)
FORTINET	Все модели NGFW FortiGate с FortiOS версии 6.0 и выше. В том числе: • FG/FWF-40F, FG/FWF-60F, FG/FWF-80F, FG-100F • FG-200F, FG-400E, FG-600E, FG-1100E • FG-1800F, FG-2200E, FG-2600F, FG-3000F • FG-3300E, FG-3400E, FG-3500F, FG-3600E • FG-3960E, FG-3980E, FG-4200F, FG-4400F • FG-6300F, FG-6500F, FG-7060E, FG-7121F/-2	• IP-адреса подозрительных и вредоносных хостов (IP reputation) • URL и хосты командных серверов ботнетов (Botnet C&C URL) • URL вредоносных сайтов (Malicious URL) • URL фишинговых сайтов (Phishing URL) • URL сайтов, распространяющих программы-вымогатели (Ransomware URL) • Хеши вредоносных файлов (Malicious Hashes)
paloalto NETWORKS	• PA-220, VM-50, VM-50 (Lite), VM 100, VM-1000-HV • Серии PA-850, PA-820, PA-3200 • Серии PA-5200, PA-7000	• IP-адреса подозрительных и вредоносных хостов (IP reputation) • URL командных серверов ботнетов (Botnet C&C URL) • URL вредоносных сайтов (Malicious URL) • URL фишинговых сайтов (Phishing URL) • URL сайтов, распространяющих программы-вымогатели (Ransomware URL)

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«Лаборатория Касперского» обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. И предлагает лидирующие во всём мире сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Узнать больше о предложении и заказать пилот

Подробнее

www.kaspersky.ru