PARUS
Powered by kaspersky

Как PARUS SECURITY CLOUD и «Лаборатория Касперского» совместно обеспечивают безопасность web-трафика компаний из РФ и РБ

Одна из насущных задач в области информационной безопасности – ограничивать доступ к небезопасным ресурсам в сети Интернет. И желательно это делать как можно ближе к периметру сети предприятия: не допускать трафик с таких ресурсов до конечного пользователя или сервиса внутри корпоративной сети.

Для решения такой задачи необходимо, во-первых, использовать на периметре сети современный межсетевой экран. Он позволит в реальном времени дешифровывать проходящий через него web-трафик, определять ресурсы, с которыми пытаются установиться сессии, получать из внешних источников оценку текущего уровня риска этих ресурсов, кешировать данную информацию и в итоге, согласно настроенным политикам, блокировать или разрешать установление таких сессий.

Во-вторых, необходим внешний источник информации по ресурсам в сети Интернет (домены любого уровня, URL и IP-адреса), позволяющий с минимальной задержкой выдать по запросу категорию ресурса и его уровень риска, ведь межсетевой экран стоит в разрыв трафика, он не должен долго ждать или не принять решение из-за отсутствия информации по ресурсу. То есть внешний источник информации должен быть не только быстрым, но и точным.

Таким источником информации является облачный сервис динамической категоризации **PARUS URL FILTERING** – модуль **PARUS SECURITY CLOUD**, который позволяет в реальном времени определять категории и уровень риска для любых URL-адресов, доменов и IP-адресов. Данный сервис имеет возможность нативной интеграции с межсетевыми экранами Palo Alto Networks, признанного мирового лидера в этой области.

Под капотом модуля **PARUS URL FILTERING**, помимо своих алгоритмов категоризации, работающих с использованием технологий машинного обучения, также используется база URL-фильтрации Palo Alto Networks (**PANDB**).

Для увеличения возможностей сервиса **PARUS URL FILTERING** предусмотрено использование сторонних источников информации об угрозах. Примером такого источника является **Kaspersky Threat Data Feeds** (потоки данных об угрозах **«Лаборатории Касперского»**).

«Лаборатория Касперского» предлагает постоянно обновляемые данные о киберугрозах, чтобы информировать ваш бизнес или клиентов о рисках и последствиях, связанных с нарушениями безопасности. Постоянные обновления также помогают более эффективно устранять опасности и защищаться от атак ещё до их запуска.

Интеграция **PARUS URL FILTERING** с потоками данных об угрозах **«Лаборатории Касперского»** осуществляется через **PARUS KFEED PLUGIN**.

Базовое условие работы плагина **KFEED**: если при проверке в базе **PANDB** запрашиваемый ресурс не попадает во вредоносные категории, то срабатывает дополнительная проверка ресурса в потоках данных об угрозах от компании **«Лаборатория Касперского»**.

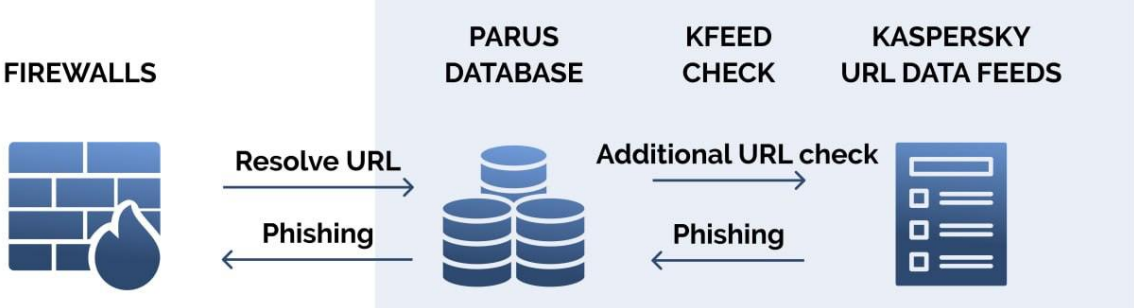

Рисунок 1 – Принцип работы **PARUS KFEED PLUGIN**

Статистика работы PARUS KFEED PLUGIN

За последние три месяца работы **PARUS KFEED PLUGIN** определено, что его использование для межсетевых экранов Palo Alto Networks на территории РФ и РБ, улучшает определение вредоносных ресурсов по сравнению с базой **PANDB** в среднем более чем **4,5%.** А для некоторых предприятий показатель доходит до **15%-20%**.

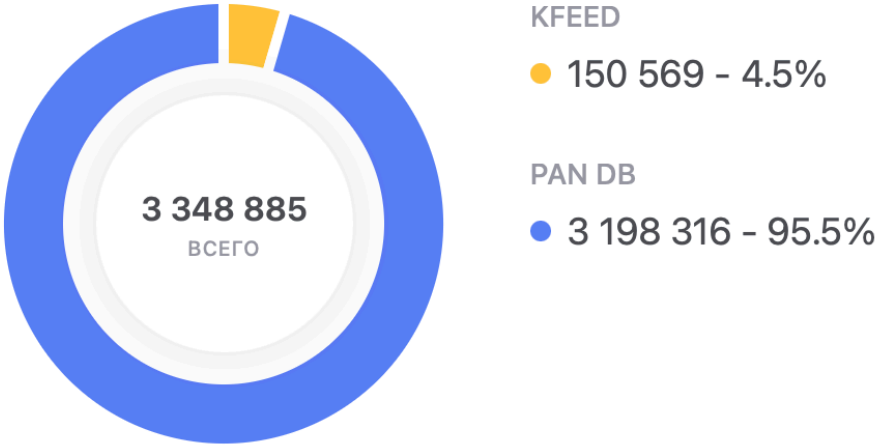

Рисунок 2 – Доля запросов к вредоносных ресурсам, которые не определяются через **PANDB**, но определяются потоками данных об угрозах **«Лаборатории Касперского»**, всего по сервису

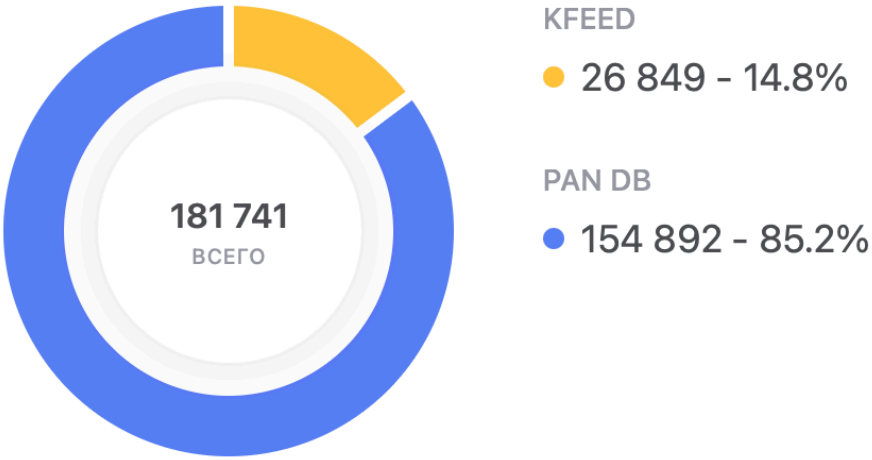

Рисунок 3 – Доля запросов к вредоносных ресурсам, которые не определяются через **PANDB**, но определяются потоками данных об угрозах **«Лаборатории Касперского»**, одно из предприятий

Параметры подсчета статистики

- Период – 3 месяца.
- Запросов на категорию ресурсов и уровень их риска от межсетевых экранов – 870 млн.
- Количество межсетевых экранов – 292.
- География – РФ, РБ.
- Отрасли – всевозможные (финансы, банки, ритейл, металлургия и т. д.).

Вредоносными считались ресурсы из следующих категорий:

Название категории	Описание
Malware	Сайты, содержащие вредоносный контент, исполняемые файлы, скрипты, вирусы, трояны и код
Phishing	Кажущиеся авторитетными сайты, которые собирают личную информацию у своих пользователей с помощью фишинга или фарминга
Command and Control	Домены и URL-адреса, используемые вредоносными программами для установления управления и контроля, утечки данных и других действий по сети после взлома системы
Ransomware	Сайты, на которых, как известно, размещаются программы-вымогатели или вредоносный трафик, участвующий в проведении кампаний по вымогательству, которые обычно угрожают публикацией личных данных или блокированием доступа к определенным данным или системам, обычно путем их шифрования, до тех пор, пока не будет выплачен требуемый выкуп
Grayware	Веб-контент, который не представляет прямой угрозы безопасности, но демонстрирует другое навязчивое поведение и побуждает конечного пользователя предоставить удаленный доступ или выполнить другие несанкционированные действия. Вредоносное ПО включает в себя незаконную деятельность, криминальное ПО, мошенническое ПО, рекламное ПО и другие нежелательные или незапрашиваемые приложения, такие как встроенные криптомайнеры, кликджекинг или угонщики, которые изменяют элементы браузера. Домены с опечатками, которые не проявляют вредоносности и не принадлежат целевому домену, будут классифицированы как вредоносное ПО

При подсчете статистики работы Parus Kfeed Plugin учитывалась сработка только по ресурсам, которые не были категорированы с помощью PANDB как вредоносные. Таким образом данная статистика демонстрирует процент дополнительных детектов, который достигается за счет подключения Parus Kfeed Plugin.

.

Олег Шабуров, менеджер по развитию бизнеса TI в «Лаборатории Касперского»:

«Статистика **PARUS SECURITY CLOUD** демонстрирует большое количество соединений, каждое из которых несет потенциальные риски и может оставаться незамеченным в течение продолжительного времени. Бывает так, что одно подключение к небезопасному адресу может привести к непоправимым для компании последствиям, а в данном случае количество таких соединений измеряется многими тысячами. Приятно видеть, что потоки данных об угрозах от «Лаборатории Касперского» помогают нашим технологическим партнерам повышать качество предоставляемых сервисов, а нашим заказчикам оставаться защищенными от современных атак**»**.

Для получения дополнительной информации и тестирования сервиса свяжитесь со своим менеджером **PARUS**.

PARUS – проект российской компании **ООО «Стайл Телеком».**

Под эгидой **PARUS** осуществляется как комплексная поддержка решений зарубежных производителей, покинувших рынок Российской Федерации и Республики Беларусь, так и разработка собственных решений в области информационной безопасности.

www.parus.su

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 года.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые технологии для защиты конечных устройств, ряд специализированных продуктов и сервисов, а также кибериммунные решения для борьбы со сложными и постоянно эволюционирующими киберугрозами.

www.kaspersky.ru