KASPERSKY

Kaspersky Threat Lookup: Защита сети без пробелов

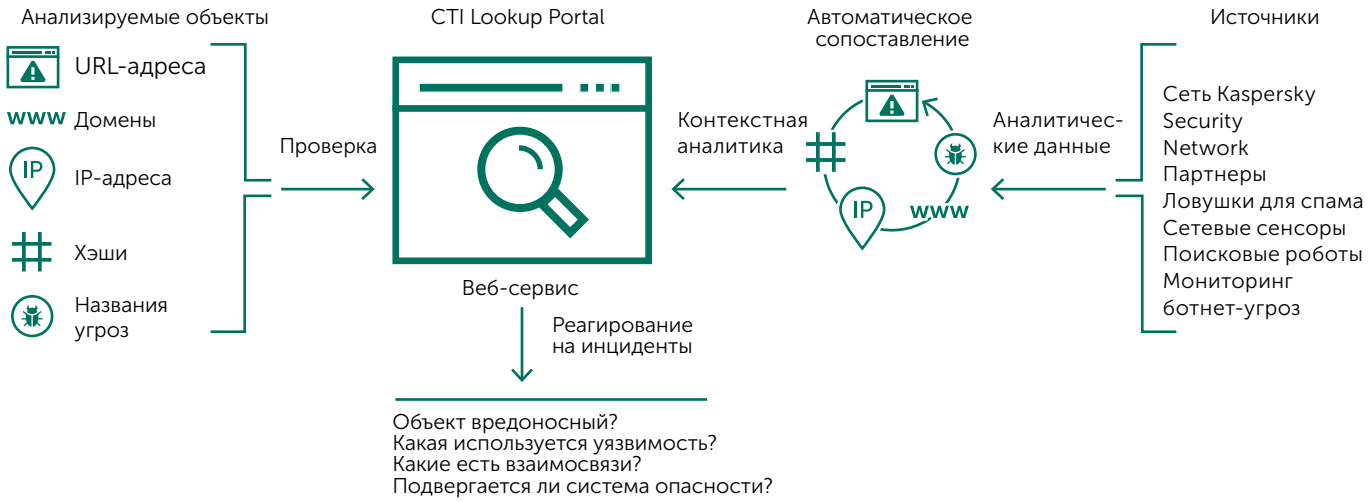
www.kaspersky.ru
#ИстиннаяБезопасность

Защита сети без пробелов

Современная киберпреступность не знает границ, а ее техническая база быстро совершенствуется: злоумышленники, используя ресурсы «подпольного» интернета, проводят все более изощренные целевые атаки. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для кампаний, направленных на нарушение ваших рабочих процессов, кражу активов и нанесение ущерба вашим клиентам, злоумышленники используют сложные вредоносные цепочки, а также специально подобранные тактику, методы и процедуры.

Сервис Kaspersky Threat Lookup позволяет получать надежные и оперативные аналитические данные о киберугрозах, легитимных объектах, их взаимосвязях и индикаторах. Используя этот сервис, ваша компания или клиенты узнают о возникающих рисках, возможных последствиях и о том, как их избежать. Благодаря этим данным вы сможете эффективнее реагировать на угрозы, защищаясь от атак еще до их запуска.

Kaspersky Threat Lookup – это мощная единая платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет вашим специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Платформа собирает подробные актуальные сведения об угрозах: URL-адреса, домены, IP-адреса, контрольные суммы файлов, названия угроз, статистику и поведенческие данные, данные WHOIS/DNS и т. д. Это обеспечивает глобальную видимость новых и возникающих угроз, помогает ускорить реагирование и повысить его эффективность.



Возможности

- **Надежная информация об угрозах.** «Лаборатория Касперского» предоставляет надежную информацию об угрозах с практическими рекомендациями по их нейтрализации. Продукты «Лаборатории Касперского» показывают наилучшие результаты при тестировании решений для защиты от вредоносных программ[1]. Непревзойденное качество аналитических данных подтверждается самым высоким уровнем обнаружения практически без ложных срабатываний.
- **Сбор данных в режиме реального времени.** Аналитические данные об угрозах генерируются автоматически в режиме реального времени на основе данных, собираемых по всему миру (в сеть Kaspersky Security Network входят десятки миллионов пользователей более чем в 213 странах, что позволяет отслеживать значительный объем интернет-трафика и данные всех типов). Это обеспечивает широкий охват и точность предоставляемой информации.
- **Активный поиск скрытых угроз.** Проактивное выявление и предотвращение атак позволяет минимизировать их воздействие и сократить частоту. Вы сможете отслеживать и устранять атаки на самых ранних этапах. Чем раньше будет обнаружена атака, тем меньший будет нанесен ущерб и тем быстрее будет восстановлена работоспособность ресурсов и сети.

- **Разнообразие данных.** Kaspersky Threat Lookup собирает данные об угрозах самых разнообразных типов, в том числе контрольные суммы, URL- и IP-адреса, данные WHOIS, pDNS и GeoIP, атрибуты файлов, статистику и сведения об активности, цепочки загрузки, временные метки и многое другое. Вооружившись этой информацией, вы сможете оценить все разнообразие угроз, которым подвергаетесь.
- **Постоянная доступность.** Аналитические данные об угрозах генерируются и отслеживаются мощной отказоустойчивой инфраструктурой, что обеспечивает постоянную доступность и непрерывную работу.
- **Постоянное сотрудничество с экспертами по безопасности.** В подготовке аналитических данных участвуют сотни экспертов, включая аналитиков по безопасности со всего мира, специалистов глобального центра исследования и анализа угроз и лучшие разработчики.
- **Анализ в «песочнице».** Для выявления неизвестных угроз подозрительные объекты можно запускать в безопасной среде, получая доступные для восприятия отчеты с полной информацией об их поведении и артефактах.
- **Разнообразие форматов экспорта данных.** Поддерживается экспорт индикаторов компрометации (IoC) и практических контекстных рекомендаций в популярные машиночитаемые форматы, такие как STIX, OpenIOC, JSON, Yara, Snort и даже CSV. Это позволяет применять данные об угрозах с максимальной пользой, автоматизируя рабочие процессы и интегрируя эти данные в системы управления безопасностью, такие как системы SIEM.
- **Простота использования через веб-интерфейс или API на основе REST.** К сервису можно обращаться в ручном режиме через веб-интерфейс (открывается в браузере) или через простой API на основе REST.
- **«Обратный» поиск в базе WHOIS.** Сервис позволяет находить информацию о владельцах доменных имен и IP-адресов, задавая точные критерии поиска в базе WHOIS (например, контактные данные владельца доменного имени, дату создания домена и т. д.).
- **Мониторинг по базе WHOIS.** Доступен регулярный автоматический поиск записей в базе WHOIS на основе заданных критериев. При появлении в базе WHOIS новых записей, соответствующих вашим критериям поиска, на заданные адреса автоматически отправляется оповещение по электронной почте.

Ключевые преимущества

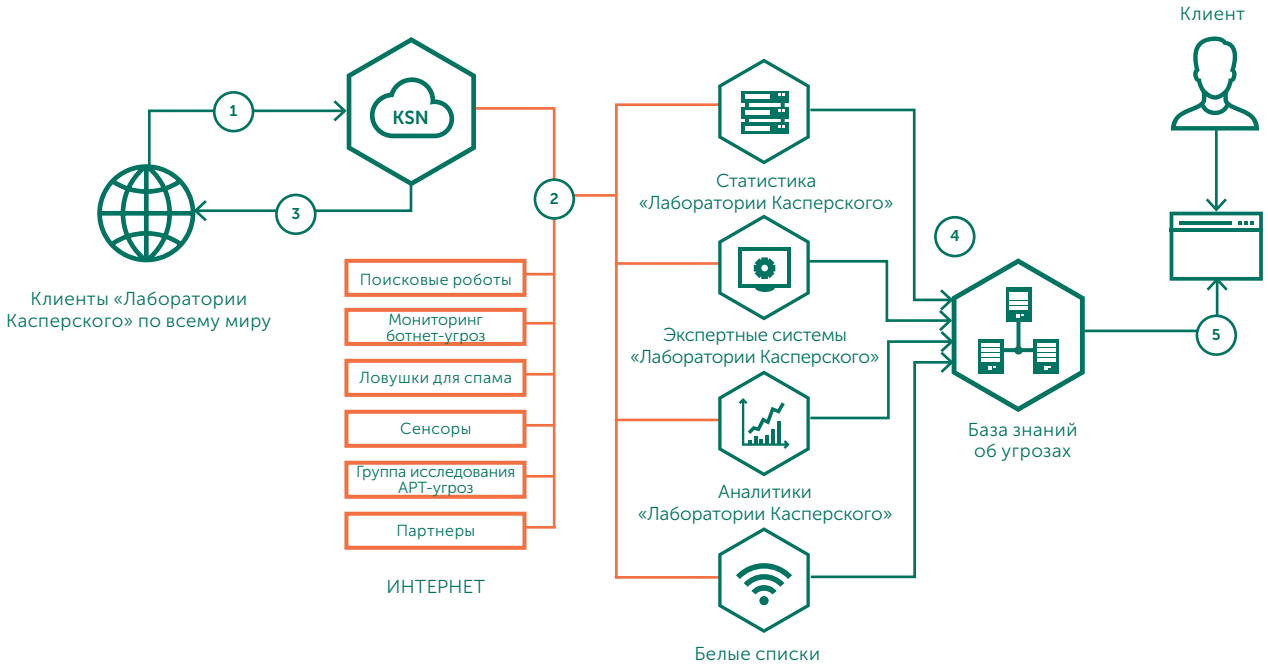
- **Улучшение и ускорение реагирования на инциденты и экспертного анализа.** Сотрудники отделов IT-безопасности и SOC получают ценную информацию об угрозах, а также результаты глобальных исследований об источниках целевых атак. Это позволяет распознавать и анализировать инциденты безопасности на хостах и в сети более эффективно и результативно, а также приоритизировать сигналы внутренних систем о неизвестных угрозах, сводя к минимуму время ответа на инциденты и разрушая вредоносные цепочки (kill chain) до того, как будут скомпрометированы критически важные системы и данные.
- **Углубленное исследование индикаторов угроз,** таких как IP- и URL-адреса, домены и контрольные суммы файлов, предоставляемые в проверенном контексте связанных с ними угроз. Это позволяет приоритизировать атаки, оптимально распределять специалистов и ресурсы и устранять в первую очередь те угрозы, которые потенциально наиболее опасны для вашей организации.
- **Защита от целевых атак.** Тактические и стратегические данные об угрозах позволяют усовершенствовать защитную инфраструктуру, адаптируя стратегии безопасности для противодействия конкретным атакам, направленным на вашу организацию.

---

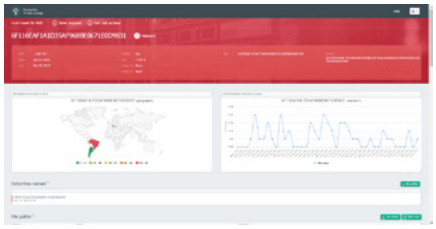
1 http://www.kaspersky.ru/top3

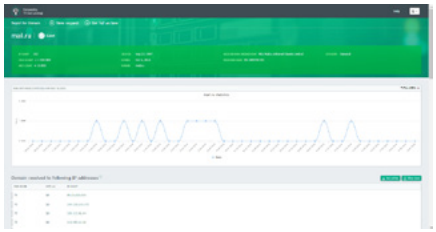
Источники данных об угрозах

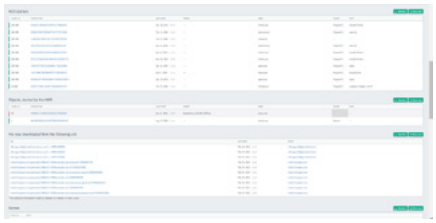
Данные об угрозах собираются из множества гетерогенных высоконадежных источников, включая сеть Kaspersky Security Network (KSN), наши собственные поисковые роботы, наш сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами и их мишенями) и ловушки для спама. Мы также получаем информацию от исследовательских групп и партнеров, используются также исторические данные о вредоносных объектах, собранные «Лабораторией Касперского» почти за два десятилетия работы. Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: статистических критериев, инструментов экспертных систем «Лаборатории Касперского» (таких как «песочницы» и средства эвристического анализа, определения сходства и профилирования моделей поведения), проверки аналитиками и сопоставления с белыми списками.



Аналитические сервисы «Лаборатории Касперского» используют тщательно отобранную информацию об индикаторах угроз, получаемую со всего мира в режиме реального времени.



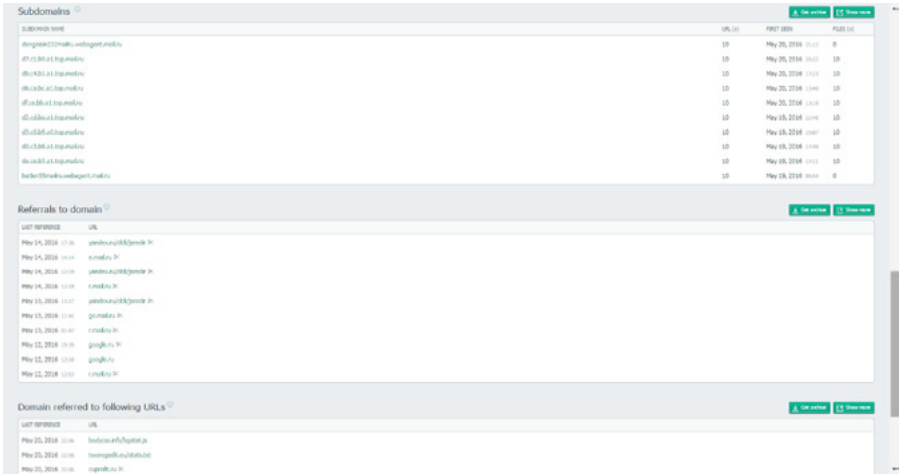




Сервис позволяет:

- проверять индикаторы угроз через веб-интерфейс или API на основе REST;
- узнавать, почему объект считается вредоносным;
- выяснять, является ли обнаруженный объект распространенным или уникальным;
- получать подробные сведения, включая относящиеся к объектам сертификаты, распространенные названия, пути файлов и URL-адреса, для выявления новых подозрительных объектов.

И это лишь некоторые из возможных действий. Kaspersky Threat Lookup – это постоянно обновляемый источник детальной информации обо всех исследуемых объектах, который можно использовать множеством различных способов.



Знать, какие объекты не несут потенциальной угрозы, так же важно, как уметь выделять опасные объекты. Игнорируя файлы, URL- и IP-адреса, безопасность которых подтверждена, вы повысите скорость расследования инцидентов. Когда каждая секунда на счету, не стоит тратить время, анализируя доверенные объекты.

Наша миссия – защищать мир от всех видов киберугроз. Выполнить ее и сделать интернет безопасным можно, лишь имея возможность передавать и получать сведения об угрозах в режиме реального времени. Своевременный доступ к информации абсолютно необходим для эффективной защиты данных и сетей. Kaspersky Threat Lookup позволяет получать нужную информацию об угрозах быстро и просто.

За более подробной информацией о сервисе Kaspersky Threat Lookup или о других сервисах Kaspersky Security Intelligence обращайтесь по адресу электронной почты intelligence@kaspersky.com.

www.kaspersky.ru

#ИстиннаяБезопасность