KASPERSKY lab

СЕРВИСЫ KASPERSKY SECURITY INTELLIGENCE

Сервисы информирования об угрозах

www.kaspersky.ru

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ

Наблюдать за постоянно развивающимися киберугрозами, анализировать их, вовремя реагировать на атаки и сводить к минимуму их последствия – процесс чрезвычайно трудоемкий. Современные организации сталкиваются с нехваткой актуальных и оперативно обновляемых сведений об угрозах IT-безопасности во всех отраслях – а недостаток таких данных усложняет управление соответствующими рисками.

Информационные сервисы «Лаборатории Касперского» дают доступ к информации об угрозах, полученной нашими аналитиками и исследователями мирового класса. Такие данные помогут любой организации выстроить защиту от киберугроз.

«Лаборатория Касперского» обладает глубокими знаниями, богатым опытом и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому компания стала доверенным партнером наиболее влиятельных правоохранительных и правительственных организаций по всему миру, в их число входит Интерпол и подразделения CERT. Вы можете использовать весь этот потенциал для повышения уровня IT-безопасности вашей компании.

Сервисы «Лаборатории Касперского» для анализа угроз предоставляют:

- Потоки данных об угрозах
- Мониторинг ботнет-угроз
- Аналитические отчеты

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ
Потоки данных об угрозах
Мониторинг ботнет-угроз
Аналитические отчеты

ПОТОКИ ДАННЫХ ОБ УГРОЗАХ

Дополните свои решения для защиты сети постоянно обновляемыми аналитическими данными о киберугрозах и целевых атаках. Такими решениями являются системы SIEM, сетевые экраны, системы обнаружения и предотвращения вторжений, технологии противодействия комплексным таргетированным угрозам (Advanced Persistent Threat – APT-угрозы) и среда моделирования («песочница»).

В последние годы число новых семейств и разновидностей вредоносного ПО стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325 000 уникальных образцов вредоносных программ. Чтобы защитить рабочие места от этих угроз, большинство организаций используют классические средства – антивирусные решения и системы предотвращения вторжений и обнаружения угроз. В динамично меняющихся условиях, когда сотрудники отделов IT-безопасности пытаются делать все, чтобы хоть на шаг опережать киберпреступников, для эффективной работы этих классических решений необходим доступ к самым актуальным сведениям об угрозах.

Данные об угрозах, предоставляемые «Лабораторией Касперского», интегрируются в существующие системы управления данными и инцидентами безопасности (SIEM), образуя дополнительный уровень защиты. Интеграция данных об угрозах позволяет сопоставлять журналы, поступающие в SIEM-систему от разных устройств сети, со сведениями об опасных URL-ссылках, предоставляемыми «Лабораторией Касперского». Поддерживается интеграция с системой SIEM HP ArcSight. Также доступны соединительные модули для Splunk® и QRadar®.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ И ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

Данные об угрозах, предоставляемые «Лабораторией Касперского»:

- дополняют решение SIEM информацией о вредоносных URL-адресах. В SIEM-систему поступают уведомления о вредоносных и фишинговых URL-ссылках, а также URL-адресах командных серверов ботнетов, содержащихся в журналах, которые передаются в SIEM с различных устройств сети (компьютеров пользователей, прокси-серверов, сетевых экранов и других серверов);
- с помощью постоянно обновляемых аналитических данных об угрозах повышают эффективность основных решений для защиты сети, таких как сетевые экраны, системы обнаружения и предотвращения вторжений, системы SIEM, технологии противодействия APT-угрозам, среды моделирования («песочницы»), UTM-устройства и т. д.;
- расширяют возможности экспертного анализа, предоставляя службе безопасности ценную информацию об угрозах и возможность раскрыть структуру целевых атак;
- поддерживают исследовательскую работу. Сведения о вредоносных URL-адресах и MD5-хэши вредоносных файлов служат весомым вкладом в проекты исследования угроз.

«Лаборатория Касперского» предлагает три типа данных об угрозах:

1) вредоносные URL-адреса и маски;
2) база MD5-хэшей вредоносных объектов;
3) данные об угрозах для мобильных устройств.

ОПИСАНИЕ ТИПОВ ДАННЫХ

URL-адреса вредоносных ссылок – набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.

URL-адреса фишинговых ссылок – набор URL-адресов, распознаваемых «Лабораторией Касперского» как фишинговые. Доступны записи с масками и без масок.

URL-адреса командных серверов ботнетов – набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов.

Хэши вредоносных объектов (ITW) – набор файловых хэшей и соответствующих вердиктов, охватывающий наиболее опасные и распространенные вредоносные программы, с которыми сталкивались пользователи сети KSN.

Хэши вредоносных объектов (UDS) – набор файловых хэшей, обнаруженных облачными технологиями «Лаборатории Касперского» (аббревиатура UDS обозначает систему мгновенного обнаружения) по метаданным файла и статистическим данным (без доступа к самому объекту). Такой подход позволяет выявлять новые, только что появившиеся, вредоносные объекты («нулевого дня»), которые нельзя обнаружить другими методами.

Хэши вредоносных объектов для мобильных устройств – набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства.

Данные о троянцах P-SMS – набор хэшей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать сообщения, отвечать на них и удалять их.

URL-адреса командных серверов ботнетов – набор URL-адресов с контекстной информацией для выявления командных серверов ботнетов, в том числе мобильных.

МОНИТОРИНГ БОТНЕТ-УГРОЗ

Экспертный сервис мониторинга и уведомления об обнаружении ботнетов, угрожающих вашим клиентам и репутации.

Многие сетевые атаки проводятся с использованием ботнетов. Такие атаки могут угрожать обычным пользователям, но чаще нацелены на конкретные организации и их онлайн-пользователей.

Экспертное решение «Лаборатории Касперского» отслеживает активность ботнетов и оперативно (в течение 15 минут) предоставляет уведомления об угрозах, направленных против пользователей платежных и банковских систем. Располагая этими сведениями, вы сможете информировать своих онлайн-пользователей, поставщиков услуг по обеспечению безопасности и правоохранительные органы об актуальных угрозах. Сервис «Лаборатории Касперского» по мониторингу ботнет-угроз поможет вам сохранить репутацию и защитить онлайн-пользователей вашей организации.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ И ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

- Проактивные уведомления о ботнет-угрозах, нацеленных на ваших онлайн-пользователей, позволят вам всегда быть на шаг впереди злоумышленников.
- Наличие списка URL-адресов командных центров ботнетов, атакующих ваших онлайн-пользователей, дает возможность их заблокировать, направив соответствующий запрос в подразделение CERT или правоохранительные органы.
- Повышение уровня безопасности личных кабинетов в системах электронных платежей и интернет-банкинга благодаря пониманию природы атак.
- Возможность обучения ваших онлайн-пользователей распознаванию методов социальной инженерии, применяемых для атак.

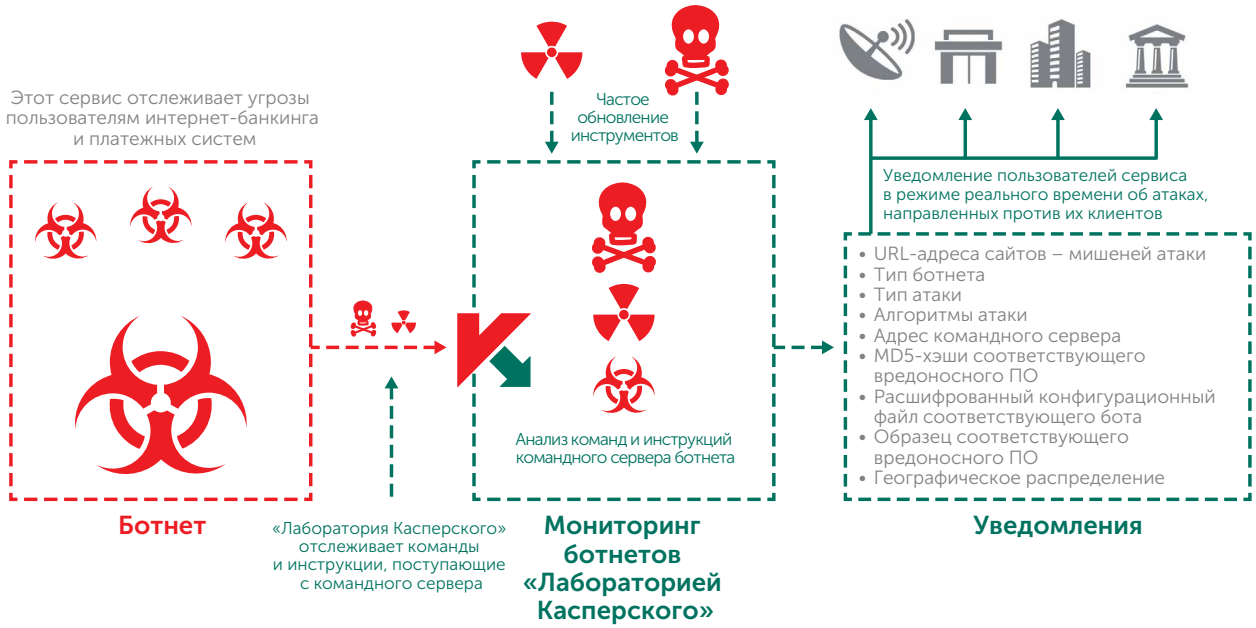
ЗАЩИТИТЕ СВОИХ ОНЛАЙН-ПОЛЬЗОВАТЕЛЕЙ, ОПИРАЯСЬ НА ДАННЫЕ, ПОСТУПАЮЩИЕ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Сервис включает подписку на персонализированные уведомления с информацией об обнаруженных ботнетах, атакующих онлайн-ресурсы компании клиента. Уведомления отправляются в формате HTML или JSON по электронной почте или через RSS и содержат следующие данные.

- **URL-адрес цели ботнета**. Вредоносное ПО активизируется и запускает алгоритм атаки в тот момент, когда пользователь посещает сайт атакуемой ботнетом организации.
- **Тип ботнета**. Наименование вредоносного ПО, используемого киберпреступниками для перехвата транзакций клиентов. Типами такого ПО могут быть, например, ZeuS, SpyEye, Citadel.
- **Тип атаки**. Информация о том, каким образом преступники используют вредоносное ПО. Варианты могут включать веб-инъекцию, снятие скриншотов, захват видеоизображения или переадресацию на фишинговый URL-адрес.
- **Алгоритмы атаки**. Сведения об использованном алгоритме инъекции веб-кода: HTML-запросы (GET/POST), данные на веб-странице до и после инъекции и др.
- **Адрес командного сервера**. Уведомив интернет-провайдеров о сервере управления ботнетом, можно оперативнее изолировать угрозу.
- **MD5-хэши вредоносного ПО**. «Лаборатория Касперского» предоставляет хэши для идентификации вредоносного ПО.
- **Расшифрованный конфигурационный файл соответствующего бота**. Полный список адресов целей (по запросу).
- **Географическое распределение (ТОП-10 стран)**. Статистические данные по глобальному распределению образцов соответствующего вредоносного ПО.

МОНИТОРИНГ БОТНЕТ-УГРОЗ: АРХИТЕКТУРА

ОТ КОМАНДНОГО СЕРВЕРА



Предлагаются варианты подписки на сервисы «Лаборатории Касперского» Standard и Premium с различными условиями предоставления услуг и набором отслеживаемых URL-адресов. Обратитесь в «Лабораторию Касперского» или к партнеру, чтобы определить, какой вариант подходит вашей организации.

УРОВНИ ПОДПИСКИ И ПРЕДОСТАВЛЯЕМАЯ ИНФОРМАЦИЯ

PREMIUM

Уведомления по электронной почте или в формате JSON

10 отслеживаемых URL-адресов

- Расшифрованный конфигурационный файл соответствующего бота
- Образец соответствующего вредоносного ПО (по запросу)
- Географическое распределение обнаруженных образцов вредоносного ПО

STANDARD

Уведомления по электронной почте

5 отслеживаемых URL-адресов

- URL сайта-мишени (при посещении которого пользователем программа-бот начинает атаку)
- Тип ботнета (Zeus, SpyEye, Citadel, Kins и т. д.)
- Тип атаки
- Алгоритмы атаки: веб-инъекция, URL-ссылки, снимки экрана, запись видео и т. д.
- Адрес командного центра
- MD5-хэши соответствующего вредоносного ПО

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ

Детальные аналитические отчеты «Лаборатории Касперского» повысят осведомленность о масштабных кампаниях кибершпионажа, а также об угрозах, направленных против конкретных организаций.

Информация из этих отчетов и предоставляемые «Лабораторией Касперского» инструменты помогут быстро отреагировать на новые угрозы и уязвимости: заблокировать атаки с известных направлений, уменьшить ущерб от комплексных атак и усовершенствовать стратегию безопасности как вашей организации, так и ваших клиентов.

ОТЧЕТЫ О КОМПЛЕКСНЫХ ТАРГЕТИРОВАННЫХ УГРОЗАХ

Иногда информация об обнаружении комплексных таргетированных угроз (Advanced Persistent Threat – APT) не становится публичной. Наши подробные отчеты позволят вам в числе первых получать эксклюзивные данные о новых APT-угрозах.

Подписчики на такие отчеты при первой возможности получают уникальный доступ к результатам расследования и техническим данным в различных форматах по каждой APT-угрозе – в том числе по тем угрозам, информация о которых никогда не будет опубликована.

Наши эксперты, профессиональные и успешные «охотники» на APT-угрозы, немедленно оповестят вас о любых обнаруженных изменениях в тактике киберпреступников и кибертеррористов. Вы также получите доступ к полной базе отчетов «Лаборатории Касперского» о комплексных таргетированных угрозах, которая дополнит ваш арсенал для борьбы с киберугрозами.

ОТЧЕТЫ «ЛАБОРАТОРИИ КАСПЕРСКОГО» ОБ APT-УГРОЗАХ ПРЕДОСТАВЛЯЮТ:

- **Эксклюзивный доступ** к техническим описаниям новейших угроз уже в ходе их расследования, еще до публичного объявления.
- **Непубличные APT-отчеты**. Не обо всех масштабных угрозах сообщается публично. Некоторые угрозы так и остаются тайной из-за специфики своих жертв, конфиденциальности данных, самой природы устранения уязвимости или привлечения правоохранительных органов. Однако наши клиенты получают доступ к таким отчетам.
- **Подробные** технические данные, образцы и инструменты, в том числе расширенный список индикаторов компрометации (Indicators of Compromise – IOC), доступные в стандартных форматах, включая openIOC и STIX, и Yara Rules.
- **Непрерывный мониторинг APT-кампаний**. Доступ к ценным аналитическим данным в ходе расследования (информация о распространении APT-угрозы, индикаторы компрометации, инфраструктура командных центров).
- **Ретроспективный анализ**. В течение всего периода подписки предоставляется доступ ко всем ранее выпущенным закрытым отчетам.

ПРИМЕЧАНИЕ ОБ ОГРАНИЧЕНИИ ПОДПИСКИ

Отчеты, предоставляемые данным сервисом, содержат конфиденциальную информацию, и мы вынуждены ограничить подписку, предоставляя ее только доверенным правительственным, общественным и частным организациям.

Как лучше всего атаковать любую организацию? Какие векторы атаки и какие сведения доступны злоумышленнику, который решил атаковать ту или иную компанию? Возможно, атака уже организована, но об этом никто не знает?

КАСТОМИЗИРОВАННЫЕ АНАЛИТИЧЕСКИЕ ОТЧЕТЫ ОБ УГРОЗАХ

Кастомизированные аналитические отчеты «Лаборатории Касперского» отвечают на эти и многие другие вопросы. Наши эксперты составляют детальную картину текущей ситуации с угрозами, выявляют уязвимые места в защите вашей организации и обнаруживают признаки прошедших, текущих и планируемых атак.

Эти уникальные данные позволят вам сконцентрироваться на уязвимостях, которые больше всего интересуют киберпреступников, и действовать быстро и точно, чтобы отразить вторжение и свести к минимуму риск успешной атаки.

Кастомизированные отчеты составляются с использованием общедоступных источников для сбора и анализа информации (OSINT), мощных экспертных систем и баз «Лаборатории Касперского» и наших данных о подпольных преступных сетях. В отчетах рассматриваются следующие вопросы.

- **Определение векторов угроз**. Выявление и анализ состояния критических компонентов сети, доступных извне, включая банкоматы, системы видеонаблюдения, телекоммуникационное оборудование и другие виды систем, а также профили сотрудников в социальных сетях и учетные записи электронной почты. Все эти компоненты являются уязвимыми для потенциальной атаки.
- **Анализ отслеживания вредоносных программ и кибератак**. Выявление, мониторинг и анализ активных и неактивных образцов вредоносного ПО, нацеленного именно на исследуемую организацию, а также исторических данных и текущей активности ботнетов и любой другой подозрительной сетевой активности.
- **Атаки на третьи стороны**. Признаки угроз и активности ботнетов, направленной на ваших клиентов, партнеров и абонентов. Их зараженные системы могут стать источником атаки уже на вашу компанию.
- **Утечка информации**. Ведя скрытое наблюдение за обсуждениями на подпольных интернет-форумах и в сообществах, мы можем распознать планы атаки на вашу компанию, а также выявить нечистоплотных сотрудников, которые могут продавать злоумышленникам ценную информацию.
- **Текущее состояние атаки**. APT-угрозы могут оставаться незамеченными в течение многих лет. Если мы обнаруживаем, что вашу инфраструктуру уже атакуют, то даем рекомендации по эффективному реагированию на атаку.

БЫСТРО. УДОБНО. БЕЗ ДОПОЛНИТЕЛЬНЫХ РЕСУРСОВ

Определив параметры специализированных отчетов и предпочтительных форматов данных, вы сможете пользоваться этим сервисом «Лаборатории Касперского», не прибегая к созданию дополнительной инфраструктуры.

Для подготовки аналитических отчетов «Лаборатории Касперского» не используются активные методы анализа, таким образом, сервис не влияет на целостность и доступность ресурсов исследуемой компании.

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для бизнеса:
www.kaspersky.ru/enterprise

+7 (495) 737-34-12
sales@kaspersky.com

© АО «Лаборатория Касперского», 2016. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей. Splunk – зарегистрированный товарный знак Splunk, Inc в США и других странах. QRadar – зарегистрированный товарный знак International Business Machines Corporation.