kaspersky

Потоки данных «Лаборатории Касперского»

Краткое руководство администратора

kaspersky

СОДЕРЖАНИЕ

Введение

Попытки взломать защиту организаций предпринимаются все чаще, сложность и скрытность киберугроз растет. Злоумышленники используют многоступенчатые атаки, кампании и специфические тактики, методы и процедуры, чтобы обойти средства контроля безопасности и нарушить работу бизнеса. «Лаборатория Касперского» предлагает постоянно обновляемые потоки данных для обнаружения вредоносных действий в корпоративной сети.

Данные собираются из множества надежных источников, включая Kaspersky Security Network (KSN), поисковых роботов, сервисов мониторинга ботнет-угроз, ловушек для спама, а также крупнейшей в индустрии базы легитимного ПО. Также источниками данных являются результаты расследований исследовательских групп и партнеров.

Вся собранная информация тщательно проверяется и корректируется в режиме реального времени при помощи различных методов предварительной обработки: машинного обучения, статистических критериев, инструментов экспертных систем «Лаборатории Касперского» («песочницы», средства эвристического анализа, определения сходства и профилирования моделей поведения), проверки аналитиками и сопоставления со списками разрешенного программного обеспечения. В результате потоки данных об угрозах содержат тщательно проверенные данные индикаторов угроз, полученные из реального мира в режиме реального времени.
Получить дополнительную информацию о потоках данных об угрозах вы можете на официальном сайте «Лаборатории Касперского» или в документе.

Потоки данных «Лаборатории Касперского»

«Лаборатория Касперского» предоставляет следующие потоки данных:

Демонстрационные потоки

- Demo IP Reputation Data Feed — демоверсия IP Reputation Data Feed.

- Demo Botnet C&C URL Data Feed — демоверсия Botnet C&C URL Data Feed.
- Demo Malicious Hash Data Feed — демоверсия Malicious Hash Data Feed.
- Demo APT Hash Data Feed — демоверсия APT Hash Data Feed.
- Demo APT IP Data Feed — демоверсия APT IP Data Feed.
- Demo APT URL Data Feed — демоверсия APT URL Data Feed.
- Demo Crimeware Hash Data Feed — демоверсия Crimeware Hash Data Feed.
- Demo Crimeware URL Data Feed — демоверсия Crimeware URL Data Feed.
- Demo Suricata Rules Data Feed — демоверсия Suricata Rules Data Feed.
- Demo SIGMA Rules Data Feed – демоверсия SIGMA Rules Data Feed.
- Demo ICS Vulnerability Feed – демоверсия ICS Vulnerability Feed.
- Demo ICS Vulnerability Feed (OVAL) – демоверсия ICS Vulnerability Feed в формате OVAL.

Демонстрационные потоки можно скачать по ссылке (прямая загрузка архива).

Коммерческие потоки

- Malicious URL Data Feed — набор масок URL-адресов и дополнительной контекстной информации о веб-ресурсах, с которых распространяется вредоносное программное обеспечение. Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика или в виде динамически обновляемого списка URL-адресов для блокировки.
- Malicious URL Exact Data Feed — набор URL-адресов, хостов, доменов и дополнительной контекстной информации о веб-ресурсах, с которых распространяется вредоносное программное обеспечение. Поток предназначен для прямой интеграции в средства контроля безопасности (например, SIEM-решения, межсетевые экраны или безопасные почтовые и веб-шлюзы) и Threat Intelligence платформы, если использование масок и Kaspersky CyberTrace по каким-либо причинам невозможно.
- Ransomware URL Data Feed — набор URL-адресов, доменов и хостов с контекстными данными, относящихся к веб-ресурсам, с которых распространяются программы-вымогатели. Поток предназначен для прямой интеграции в средства контроля безопасности (например, SIEM-решения) либо интеграции с помощью Kaspersky CyberTrace, а также для интеграции в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика или в виде динамически обновляемого списка URL-адресов для блокировки.
- Phishing URL Data Feed — набор масок URL-адресов и дополнительной контекстной информации о фишинговых веб-ресурсах. Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика или в виде динамически обновляемого списка URL-адресов для блокировки.
- Phishing URL Exact Data Feed — набор URL-адресов, хостов, доменов и дополнительной контекстной информации о фишинговых веб-ресурсах. Поток предназначен для прямой интеграции в средства контроля безопасности (например, SIEM-решения, межсетевые экраны или безопасные почтовые и веб-

шлюзы) и Threat Intelligence платформы, если использование масок и Kaspersky CyberTrace по каким-либо причинам невозможно.

- Botnet C&C URL Data Feed — набор масок URL-адресов и дополнительной контекстной информации о C&C-серверах ботнетов и связанных с ними вредоносных объектах (ботах). Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика или в виде динамически обновляемого списка URL-адресов для блокировки.
- Botnet C&C URL Exact Data Feed — набор URL-адресов, хостов, доменов и дополнительной контекстной информации о C&C-серверах ботнетов и связанных с ними вредоносных объектах (ботах). Поток предназначен для прямой интеграции в средства контроля безопасности (например, SIEM-решения, межсетевые экраны или безопасные почтовые и веб-шлюзы) и Threat Intelligence платформы, если использование масок и Kaspersky CyberTrace по каким-либо причинам невозможно.
- Mobile Botnet C&C URL Data Feed — набор масок URL-адресов и дополнительной контекстной информации о C&C серверах мобильных ботнетов и связанных с ними вредоносных объектов (ботов). Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика.
- Malicious Hash Data Feed — набор хешей и дополнительной контекстной информации, относящихся к распространенным вредоносным файлам. Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика.
- Mobile Malicious Hash Data Feed — набор хешей и дополнительной контекстной информации, относящихся к распространенным вредоносным файлам для мобильных операционных систем (Android и iOS). Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика.
- IP Reputation Data Feed — набор IP-адресов и дополнительной контекстной информации, относящихся к различным категориям подозрительных и вредоносных хостов. Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика либо в виде динамически обновляемого списка IP адресов для блокировки.
- IoT URL Data Feed — набор масок URL-адресов и дополнительной контекстной информации о веб-ресурсах, с которых распространяется вредоносное программное обеспечение для IoT-устройств (IP-камер, умных пылесосов, чайников и пр.). Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика.
- Vulnerability Data Feed — набор уязвимостей корпоративного программного обеспечения с дополнительной контекстной информацией (хеши уязвимых

приложений или эксплойтов, временные метки, CVE, исправления и пр.). Поток предназначен для интеграции в Threat Intelligence платформы и SIEM-системы с целью поиска уязвимого программного обеспечения посредством сопоставления данных из потока с данными реестра используемого программного обеспечения (например, список активов в SIEM-системе).

- ICS Vulnerability Data Feed — набор уязвимостей корпоративного программного обеспечения и программного обеспечения АСУ ТП с дополнительной контекстной информацией (хеши уязвимых приложений или эксплойтов, временные метки, CVE, исправления и пр.). Поток предназначен для интеграции в Threat Intelligence платформы с целью агрегации информации об известных и релевантных для организации уязвимостях. Также поток может быть использован для интеграции в SIEM-системы с целью поиска уязвимого программного обеспечения посредством сопоставления данных из потока с данными реестра используемого программного обеспечения (например, список активов в SIEM-системе).
- ICS Vulnerability Data Feed в формате OVAL — набор правил для поиска уязвимостей программного обеспечения АСУ ТП. Поток предназначен для сканирования файлов в операционных системах Microsoft Windows с помощью популярных сканеров уязвимостей программного обеспечения с целью обнаружения уязвимого программного обеспечения АСУ ТП.
- ICS Hash Data Feed — набор хешей и дополнительной контекстной информации, относящихся к распространенным вредоносным файлам, представляющим угрозу для АСУ ТП. Поток предназначен для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace, либо в межсетевые экраны нового поколения или безопасные почтовые и веб-шлюзы посредством интеграции потока в подсистему анализа трафика.
- pDNS Data Feed — набор записей, содержащих результаты DNS преобразований для доменов в соответствующие IP-адреса за период времени. Поток предназначен для расследования киберинцидентов.
- Suricata Rules Data Feed — правила обнаружения различных категорий угроз в сетевом трафике, таких как APT, Botnet C&C, Ransomware и др. Поток предназначен для интеграции в IDS решения.
- Sigma Rules Data Feed — логика обнаружения вредоносных действий, описанная в формате SIGMA-правил. Поток предназначен для специалистов центров мониторинга событий информационной безопасности (Security Operation Centers) с целью формирования на его основе детектирующих правил систем класса SIEM и EDR.
- Cloud Access Security Broker (CASB) Data Feed — набор доменов и хостов, а также дополнительной контекстной информации, относящихся к популярным облачным сервисам. Поток предназначен для построения CASB решения, в частности, для настройки политик доступа к облачным сервисам.
- APT Hash Data Feed — набор хешей и дополнительной контекстной информации, относящихся к файлам, используемым участниками APT-группировок для проведения целевых атак. Поток предназначен для расследования киберинцидентов, а также для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace.
- APT IP Data Feed — набор IP-адресов, принадлежащих инфраструктуре, которая используется в целевых атаках. Поток предназначен для расследования киберинцидентов, а также для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace.
- APT URL Data Feed — набор доменов, принадлежащих инфраструктуре, которая используется в целевых атаках. Поток предназначен для расследования

киберинцидентов, а также для интеграции в средства контроля безопасности (например, SIEM-решения) с помощью Kaspersky CyberTrace.

- APT Yara Data Feed — набор YARA правил для идентификации файлов, используемых в целевых атаках. Поток предназначен для проактивного поиска признаков целевых атак в локальной сети организации, а также для расследования киберинцидентов.
- Open Source Software Threats Data Feed — список названий, версий и дополнительной контекстной информации о программных пакетах с открытым исходным кодом (open source), содержащих уязвимости, вредоносную функциональность либо политически мотивированную компрометацию функциональности (блокировку в определенных регионах, политические лозунги). Поток предназначен для компонентного анализа разрабатываемого программного обеспечения в рамках процесса безопасной разработки (DevSecOps) с целью защиты программного продукта от атак на цепочку поставок (supply chain attack), раннего обнаружения и устранения уязвимостей, а также предотвращения использования пакетов, содержащих политически ориентированные недекларированные возможности (НДВ).
- Crimeware Hash Data Feed — набор хешей и дополнительной контекстной информации, относящихся к файлам, используемым в мошеннических кампаниях, описанных в Crimeware отчетах «Лаборатории Касперского». Поток предназначен для расследования киберинцидентов.
- Crimeware URL Data Feed — набор доменов и дополнительной контекстной информации, используемых в мошеннических кампаниях, описанных в Crimeware отчетах «Лаборатории Касперского». Поток предназначен для расследования киберинцидентов.
- Crimeware Yara Data Feed — набор YARA правил, которые идентифицируют файлы, используемые в мошеннических кампаниях, описанных в Crimeware отчетах «Лаборатории Касперского». Поток предназначен для поиска признаков мошеннических кампаний в локальной сети организации и расследования киберинцидентов.
- Whitelisting Data Feed — набор хэшей популярных файлов легитимного ПО. Предназначен для использования в качестве фильтра для снижения нагрузки на антивирусное ПО и «песочницы», а также для реализации политики «запрещено все, что не разрешено».

Содержание потоков

Записи в потоках данных, предоставляемых «Лабораторией Касперского», содержат индикаторы компрометации и контекстные данные, которые позволяют быстро подтвердить и приоритизировать угрозы:

- установленные IP-адреса и доменные имена вредоносных веб-ресурсов;
- хеши вредоносных файлов;
- идентификаторы уязвимых и скомпрометированных объектов;
- имена угроз;
- метки времени;
- географическое положение;
- популярность и прочее.

Эти данные вы можете использовать, чтобы составить общее представление о событии или провести дополнительные проверки.

kaspersky

Частота обновления потоков

Потоки обновляются со следующей периодичностью:

- APT Hash Data Feed в формате JSON — каждые 60 минут.
- APT IP Data Feed в формате JSON — каждые 60 минут.
- APT URL Data Feed в формате JSON — каждые 60 минут.
- APT Yara Data Feed — каждые 60 минут.
- Botnet C&C URL Data Feed в формате JSON — каждые 60 минут.
- Botnet C&C URL Exact Data Feed в формате JSON — каждые 60 минут.
- Cloud Access Security Broker (CASB) Data Feed — каждые 6 часов.
- Crimeware Hash Data Feed в формате JSON — каждые 3 часа, но новые данные появляются в зависимости от обновлений отчетов Crimeware.
- Crimeware URL Data Feed — каждые 3 часа, но новые данные появляются в зависимости от обновлений отчетов Crimeware.
- Crimeware YARA Data Feed — каждые 3 часа, но новые данные появляются в зависимости от обновлений отчетов Crimeware.
- Demo Botnet C&C URL Data Feed — каждые 24 часа.
- Demo ICS Vulnerability Data Feed в формате JSON — статичный, не обновляется.
- Demo IP Reputation Data Feed — каждые 24 часа.
- Demo Malicious Hash Data Feed — каждые 24 часа.
- Demo SIGMA Rules Data Feed — статичный, не обновляется.
- Demo Suricata Rules Data Feed — каждые 24 часа.
- ICS Hash Data Feed в формате JSON — каждые 60 минут.
- ICS Vulnerability Data Feed в формате JSON — каждые 60 минут.
- ICS Vulnerability Data Feed в формате OVAL — каждые 60 минут.
- IoT URL Data Feed в формате JSON — каждые 60 минут.
- IP Reputation Data Feed в формате JSON — каждые 20 минут.
- Malicious Hash Data Feed в формате JSON — каждые 20 минут.
- Malicious URL Data Feed в формате JSON — каждые 20 минут.
- Malicious URL Exact Data Feed в формате JSON — каждые 10 минут.
- Mobile Botnet C&C URL Data Feed в формате JSON — каждые 60 минут.
- Mobile Malicious Hash Data Feed в формате JSON — каждые 20 минут.
- Open Source Software Threats Data Feed — каждые 4 часа.
- pDNS Data Feed в формате JSON — каждые 60 минут.
- Phishing URL Data Feed в формате JSON — каждые 20 минут.
- Phishing URL Exact Data Feed в формате JSON — каждые 30 минут.
- Ransomware URL Data Feed в формате JSON — каждые 20 минут.
- SIGMA Rules Data Feed — каждый квартал.
- Suricata Rules Data Feed — каждые 24 часа.
- Vulnerability Data Feed в формате JSON — каждые 6 часов.
- Whitelisting Data Feed – каждый час.

Протоколы доставки потоков

Потоки данных доступны для получения по протоколу HTTPS. Для этого необходимо использовать утилиту автоматизации скачивания потоков и сертификат «Лаборатории Касперского». Для получения утилиты и сертификата отправьте запрос на intelligence@kaspersky.com.

kaspersky

Наиболее популярные потоки также доступны по протоколу TAXII с аутентификацией по токену. Для получения токена и инструкции, отправьте запрос на intelligence@kaspersky.com.

При необходимости возможно использование другого протокола доставки потоков.

Форматы потоков

Потоки данных доступны в формате JSON. Потоки данных без контекста доступны в формате CSV.

По запросу может быть предоставлена утилита конвертации из формата JSON в форматы STIX, OpenIOC, Suricata, CSV и Plain-text. Конвертация в другой формат может быть добавлена по запросу.

Использование потоков

Рекомендуемый способ использования потоков «Лаборатории Касперского» - использование Threat Intelligence платформы CyberTrace.

Список поддерживаемых CyberTrace потоков указан в документации.

Использование потоков «Лаборатории Касперского», не поддерживаемых платформой CyberTrace, возможно путем скачивания и интеграции в стороннюю систему. Для получения подробной информации и консультаций отправьте запрос на intelligence@kaspersky.com.