Kaspersky Threat Attribution Engine

Важная роль атрибуции угроз

kaspersky

Крупнейшее киберограбление в истории

В феврале 2016 г. группа киберпреступников попыталась вывести из Центрального банка Бангладеш на свои счета около 851 млн долларов США и ей удалось заполучить 81 миллион.

Организатор этой атаки – печально известная команда Lazarus. Она уже провела несколько кампаний по кибершпионажу и саботажу, некоторые из которых имели разрушительные последствия. Lazarus с 2009 года атакует финансовые учреждения, казино, разработчиков программного обеспечения для инвестиционных компаний и криптовалютные компании по меньшей мере в 18 странах.

Как правило, злоумышленники действуют в соответствии с определенной тактикой, техниками и процедурами. Изучив их, эксперты по кибербезопасности могут определить кто стоит за атакой.

Профилактика – лучшая защита

Современный изменчивый мир связан компьютерными сетями, которые служат основными инструментами для общения, работы с данными и контроля критических важных инфраструктур. К сожалению, через те же сети и цифровые каналы связи по миру за считаные минуты распространяются киберугрозы. Правительственные организации и крупные предприятия подвергаются атакам гораздо чаще, чем хотелось бы.

Преступники обычно покушаются на денежные средства и нематериальные активы или на интеллектуальную собственность и другую ценную информацию, которую можно продать в теневом интернете или конкурирующим фирмам. Правительственные организации оказываются заложниками геополитической ситуации или региональных конфликтов и часто становятся жертвами шпионажа.

Киберпреступники все чаще умело проводят целевые атаки, их методы становятся все изощреннее, в их арсенале все больше ресурсов. Теперь, как никогда раньше, ИБ-специалистам нужны новые методы и инструменты для прогнозирования, отслеживания и предотвращения киберугроз и шпионажа. Также необходимы меры, позволяющие минимизировать последствия атак для бизнеса. Изменилась и общая стратегия IT-безопасности: теперь она должна включать в себя цифровую криминалистику, чтобы определить причины инциденты, закрыть существующие «бреши» и предотвратить подобные инциденты в будущем

Сегодня многие организации имеют специальное подразделение по управлению инцидентами кибербезопасности или пользуются услугами внешнего центра мониторинга и реагирования (SOC). Кибербезопасность для многих компаний стала приоритетом: крупные корпорации и государственные учреждения снабжают ИБ-отделы самыми современными защитными сервисами и решениями.

«Лаборатория Касперского» сотрудничает с крупными центрами реагирования на инциденты (CERT), правительственными и правоохранительными организациями по всему миру, предоставляя актуальную информацию о новейших киберугрозах и помогая внедрить подходящие защитные механизмы.

Более 20 лет работы в области кибербезопасности, эксперты мирового уровня, широкий ряд сервисов для анализа угроз, несколько петабайт непрерывно обновляемых данных о ландшафте киберугроз — «Лаборатория Касперского» поможет вам всегда оставаться на шаг впереди киберпреступников.

Почему важна атрибуция угроз?

В августе 2016 года «Лаборатория Касперского» предотвратила попытку Lazarus атаковать банк в Юго-Восточной Азии. Расследуя нападения группировки на финансовые фирмы, наши эксперты смогли идентифицировать более 150 различных экземпляров вредоносных программ, которые использовали преступники.

Киберугрозы постоянно эволюционируют. Наблюдать за ними, анализировать, вовремя реагировать на атаки и сводить к минимуму их последстви — чрезвычайно трудоемкий процесс.

Аналитика угроз (Threat Intelligence) — не просто модное направление в информационной безопасности, это важный инструмент защиты. Он включает ряд сервисов для защиты организаций, информирования в области кибербезопасности и расследования инцидентов.

В сфере аналитики угроз атрибуция, вероятно, самая обсуждаемая и спорная тема, и на то есть ряд причин.

Сложные методы расследования и обратной разработки замедляют реагирование на продвинутые угрозы. Однако в эпоху цифровизации организациям необходимо оперативно расследовать и приоритизировать оповещения систем безопасности и сокращать время реакции. Корректная и своевременная атрибуция сокращает время реагирования на инцидент с нескольких часов до нескольких минут, а также снижает количество ложноположительных срабатываний.

Атрибуция целевых атак – эффективный инструмент, который действует в нескольких направлениях:

- Оценка риска для организации: конечная цель атаки или случайная жертва.
- Предоставление аналитических данных о преступниках, совершивших атаку, и их мотивах.
- Эффективное расследование и сдерживание угроз, а также реагирование на них благодаря знанию тактик, методов и процедур злоумышленников.

Искусство атрибуции угроз

Нередко замечание «Атрибуция — это сложно» произносится шутливым или извиняющимся тоном. Конечно, это проще, чем подробно описывать процесс и объяснять, что суть атрибуции – в сочетании технических индикаторов, ошибок хакеров, совпадений и порой просто удачи. Процесс осложняет еще и то, что киберпреступники умеют искусно заметать следы. Так что атрибуция киберугроз — это искусство, которое требует вложений.

При классическом подходе к атрибуции проводится анализ каждого отдельного случая на основе выявленных индикаторов, которые необходимо интерпретировать на каждом шаге процесса.. Сопоставив эти индикаторы, мы можем опознать авторов атаки. Давайте рассмотрим несколько основных.

Метки времени

Формат Portable Execution (PE) всегда содержит данные о времени компиляции,. Эту информацию легко изменить, но во многих экземплярах все же остаются исходные метки времени. Они позволяют исследователям узнать некоторые важные сведения. По меткам времени можно не только узнать, как давно этот экземпляр был написан, но и отследить эволюциюинструментария злоумышленников. Если у исследователей будет сравнительно большое число экземпляров вредоносного ПО, разработанного одной и той же группировкой, они смогут определить часовой пояс, в котором она находится, по пикам активности.

Строки, пути к файлам отладки и метаданные

Имплантированный двоичный код может многое рассказать о своих авторах. По нему можно, например, определить предпочитаемый язык или просмотреть пути к файлам отладки, которые часто содержат имя пользователя, а также узнать внутренние правила именования инструментов, проектов или кампаний. Язык редко раскрывает происхождение автора, но неправильное сочетание слов и машинный перевод на английский могут указывать на отвлекающий маневр. Еще один источник информации – метаданные, которые могут рассказать о конфигурации системы разработчика.

Хороший пример – код вредоносного ПО, который мы нашли в ходе расследования атак Lazarus. Преступники начали вставлять ключевые слова на русском (рисунок 1), чтобы запутать исследователей. Поскольку слова использовались странным образом, легко было понять, что это автоматический перевод.

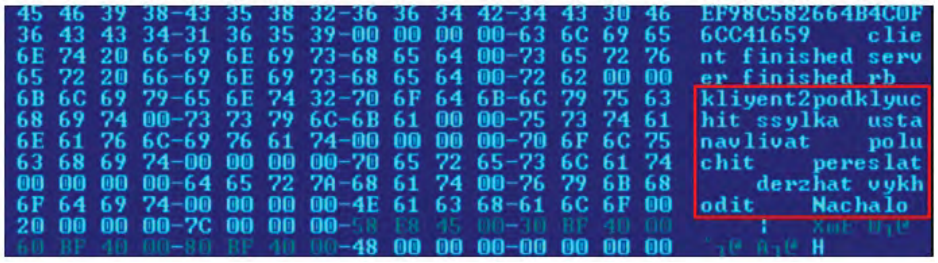


Рисунок 1. Строки на русском языке в коде Lazarus

Инфраструктура серверов

Инфраструктура командных серверов обычно стоит дорого, и ее сложно обслуживать. К тому же доступ к ней в случае обнаружения могут закрыть правоохранительные органы или бдительный системный администратор.

Поэтому даже хорошо оснащенные преступники обычно повторно используют инфраструктуру командных и фишинговых серверов. Для аналитиков угроз, пополняющих базы данных для атрибуции, повторное использование инфраструктуры будет самым ярким признаком, указывающим на конкретную группировку. Киберпреступники почти всегда используют сервисы анонимизации, когда подготавливают вспомогательные и фишинговые серверы, проверяют доступность взломанного домена или извлекают данные из учетной записи электронной почты через сервер эксфильтрации. Но они часто делают ошибки.

Происхождение угрозы можно узнать, просмотрев, например, журналы взломанного сервера. Иногда преступники не используют VPN, и их IP-адрес легко найти, как это показано на рисунке 2. Все знают, что в Северной Корее VPN не работает. Поэтому вероятность того, что атакующий находится в Северной Корее, составляет почти 100%.

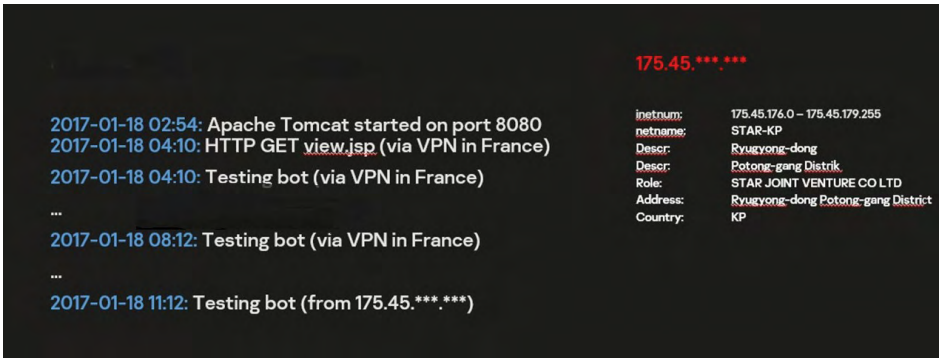


Рисунок 2. Журналы командного сервера в Европе

Эксплойты

Эксплойты нулевого дня – хороший источник информации об организаторах кибератаки. Атаки на уязвимость нулевого дня проводят более искушенные преступники, так что усердие исследователей приносит свои плоды. Когда реализация уязвимости нулевого дня наблюдается в нескольких несвязанных атаках в течение определенного срока (даже спустя долгое время после обнаружения и исправления бреши), это означает, что используется один и тот же код и, скорее всего, угроза исходит от одной и той же группировки или из одного и того же кластера активности.

Инструментарий, вредоносный код и пароль

Даже самый продвинутый киберпреступник может использовать общедоступные инструменты. Однако в большинстве случаев злоумышленники сами разрабатывают вредоносные программы, бэкдоры, средства распространения и эксплойты. Бывает, что преступникам нужно полностью сменить свой арсенал (если их раскрыли, например). При этом они, скорее всего, не будут изобретать велосипед: программисты не любят лишних усилий. Так что, даже если потребуется заменить все, злоумышленник будет повторно использовать конкретные функции или фрагменты кода, хорошо работавшие в прошлом. Дотошный исследователь сможет пройти по этим следам и найти связь новой компании с прошлыми атаками. Преступники также могут повторно использовать пароли и жестко прописанные ключи шифрования при создании разных семейств зловредов или в новых кампаниях.

Жертва целевой атаки

Многие индикаторы можно подделать или замаскировать. Отношения между атакующим и жертвой труднее скрыть, так как в них замешаны некоторые обстоятельства, которые известны многим, или геополитические конфликты. Команда умелых аналитиков может использовать эти данные для создания профилей атакующих. В результате вполне возможно сопоставить кампанию с геополитической или региональной ситуацией, которая может указать на атакующую организацию или страну.

В 2015 году специалисты «Лаборатории Касперского» заметили, что группировка Equation использовала те же два эксплойта нулевого дня, что и создатели червя Stuxnet. Два одинаковых эксплойта в двух разных червях примерно в одно и то же время: это говорит о том, что Equation и разработчики Stuxnet – одни и те же люди или же тесно сотрудничают.

Более свежий пример – внедрение дропперов через ресурсы, защищенные паролем. Вредоносное ПО содержало полезную нагрузку, которая помогала обмануть песочницу и автоматические системы обнаружения угроз. Жестко прописанный пароль, защищающий ресурс, был одним и тем же, даже если используемые дропперы, на первый взгляд, не были связаны друг с другом. Это позволило исследователям «Лаборатории Касперского» связать два семейства зловредов с одной и той же группировкой.

Атрибуция угроз требует времени и терпения

Идентификация целевой атаки, создание профиля преступников и разработка факторов атрибуции для различных угроз – эта работа требует тщательного подхода и может длиться годами. Эффективная атрибуция всегда требует больших объемов данных, собранных на протяжении многих лет, а также участия квалифицированных исследователей с опытом цифровой криминалистики и расследования инцидентов.

Хороший пример атрибуции – исследование семейства вредоносных программ Lambert «Лабораторией Касперского».

Lambert – семейство сложных инструментов, которые одна или несколько киберпреступных организаций использовали для атаки на крупные компании по меньшей мере с 2008 года. Впервые информация о зловреде из этого семейства, получившем имя Black Lambert, была опубликована в октябре 2014 года. За следующие три года было обнаружено еще 9 имплантов. Последним был Brown Lambert, найденный в октябре 2017.

В арсенале создателей семейства – сетевые бэкдоры, несколько поколений модульных бэкдоров, инструменты сбора данных и вайперы. На данный момент известны версии Lambert для Windows и для OSX. Последние экземпляры были созданы в 2016 году.

Два варианта каждой обнаруженной вредоносной программы имеют по крайней мере один общий индикатор: это может быть версия и описание ToolType, кодовые имена, структура, стиль программирования или формат конфигурации (рисунок 3).

То есть, во время атрибуции угроз исследователи «Лаборатории Касперского» терпеливо отслеживают деятельность киберпреступников и постепенно пополняют базу данных. Такая база данных становится ценными ресурсом, который организации впоследствии могут использовать для предотвращения атак.

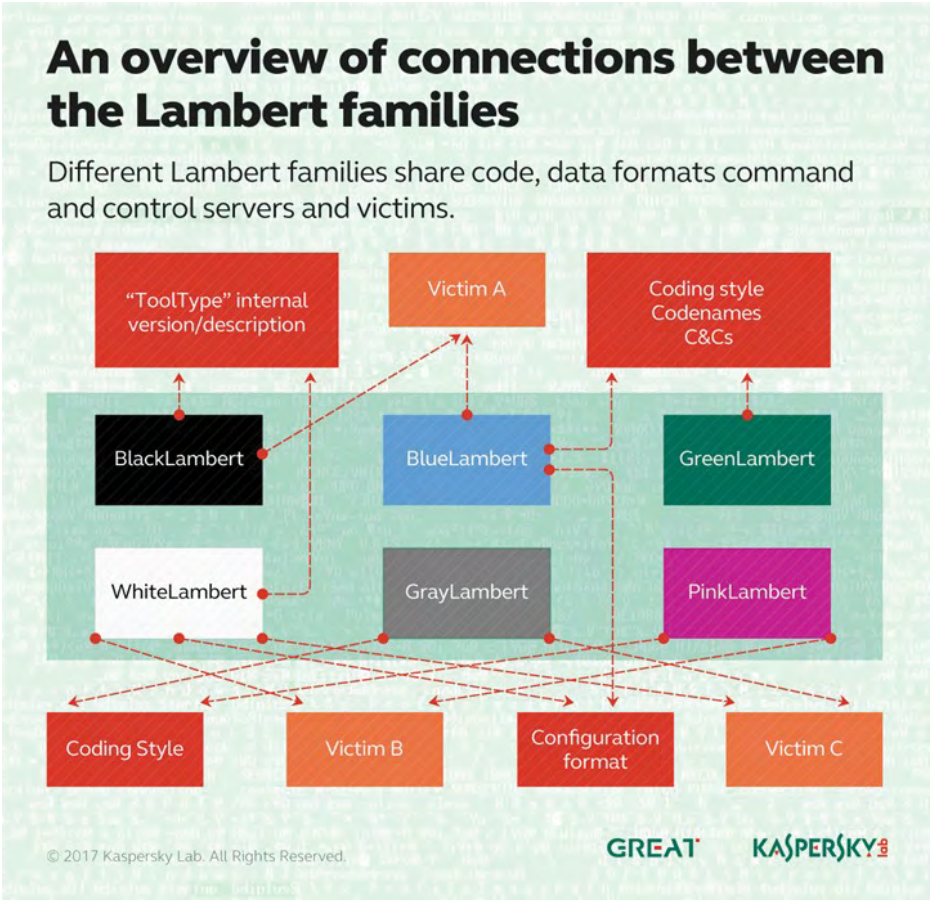


Рисунок 3. Связи между зловредами семейства Lambert

- 22 года наблюдений
- Около 3 млрд экземпляров в базе данных «Лаборатории Касперского»
- Около 4 млн новых экземпляров, обрабатываемых ежедневно
- Более 60 тысяч экземпляров APT-угрозами в базе данных «Лаборатории Касперского»
- Более 600 APT-группировок и кампаний, отслеживаемых «Лабораторией Касперского»
- Более 120 аналитических отчетов об APT-угрозах, публикуемых ежегодно

Что такое Kaspersky Threat Attribution Engine

С помощью готового кода можно быстро создавать программы, так как в нем уже решены возможные конфликты и технические проблемы. Именно поэтому повторное использование кода так часто встречается в разработке программного обеспечения: как легального, так и вредоносного. Это означает, что почти каждая новая атака содержит экземпляры предыдущих, и основная задача – найти общие элементы.

Атрибуция целевых атак на основе данных из базы с экземплярами вредоносных программ остается самым надежным методом на данный момент. При наличии неограниченных серверных мощностей для проверки петабайтов данных атрибуция работает наиболее эффективно. Однако это не только чрезмерно затратное, но и нереализуемое решение для большинства организаций.

Kaspersky Threat Attribution Engine – инструмент, база данных которого содержит экземпляры APT-угроз и чистые файлы, собранные экспертами «Лаборатории Касперского» за 22 года. Уникальный метод сравнения экземпляров и выявления сходств между ними обеспечивает высокую точность атрибуции и минимизирует количество ложноположительных срабатываний.

Kaspersky Threat Attribution Engine может быстро сопоставить новые атаки с известными APT-угрозами, предыдущими целевыми атаками, киберпреступными группировками и кампаниями, позволяя отличить серьезные инциденты от незначительных и вовремя скорректировать защитные механизмы. Автоматизация обратной разработки кода значительно повышает эффективность анализа вредоносных программ, а также ускоряет приоритизацию угроз и реагирование на инциденты. Благодаря Kaspersky Threat Attribution Engine атрибуция угроз занимает считаные секунды, а не годы, как это было раньше.

«Лаборатория Касперского» отслеживает более 600 APT-группировок и кампаний и ежегодно выпускает свыше 120 аналитических отчетов. Непрерывные исследования помогают поддерживать коллекцию APT-угроз в актуальном состоянии. В настоящий момент она содержит более 60 тысяч файлов. Данные исследований APT-атак и автоматизированные инструменты вместе обеспечивают максимально точную атрибуцию.

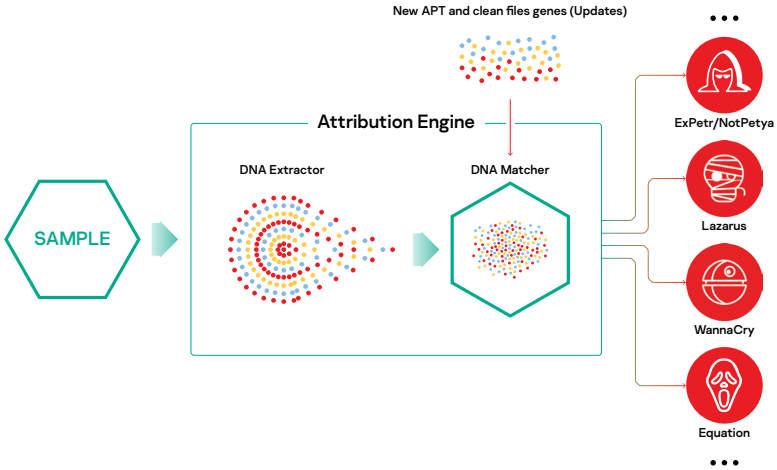
Обучение системы атрибуции на отдельных экземплярах

- Пользователь создает новую запись киберпреступника или кампании для своего образца или коллекции образцов
- Далее пользователь загружает образцы и ассоциирует их с вновь заведённой записью
- Kaspersky Threat Attribution Engine обрабатывает загруженные экземпляры файлов и извлекает их «гены»
- Kaspersky Threat Attribution Engine записывает генотип отдельного экземпляра в собственную базу данных организации
- Теперь Kaspersky Threat Attribution Engine может связывать файлы с этим генотипом и группировкой

Принцип работы Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine автоматически извлекает и анализирует «гены» вредоносных программ: система ищет сходства с экземплярами расследованных APT-атак и сопоставляет с данными о киберпреступниках. Извлеченные «гены» (небольшие фрагменты двоичного кода из декомпилированных файлов) проверяются по базе экземпляров APT-угроз, после чего определяется репутационный скоринг файла. Выявляя генотип файла и принадлежность кода, **Kaspersky Threat Attribution Engine** быстро предоставляет аналитические данные о происхождении вредоносной программы и ее возможных разработчиках.

Kaspersky Threat Attribution Engine можно развернуть в изолированной среде, защищенной от доступа сторонних лиц к обрабатываемой информации и отправляемым в нее объектам. Интерфейс API позволяет подключить продукт к другим системам и фреймворкам, чтобы внедрить атрибуцию в существующую инфраструктуру и автоматизированные процессы.



Picture 4. Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine входит в портфель продуктов «Лаборатории Касперского» для SOC и государственных служб IT-безопасности

Kaspersky Threat Attribution Engine мощное решение для эффективного управления инцидентами. Оно дополняет портфель продуктов «Лаборатории Касперского» для государственных ведомств и коммерческих центров мониторинга и реагирования (SOC).

На каждом шаге процесса управления инцидентами требуются технические возможности и специальные знания, чтобы ответить на вопросы, представленные на рисунке 4.

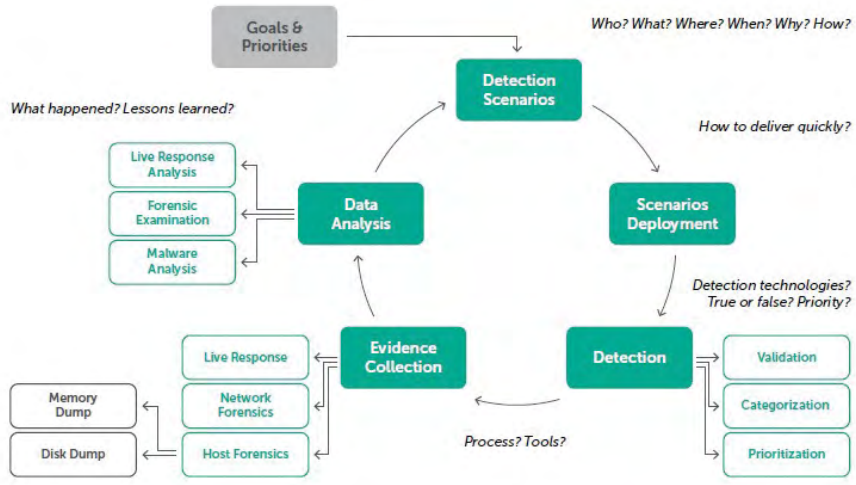


Рисунок 4. Процесс управления инцидентами и связанные вопросы

«Лаборатория Касперского» помогает государственным организациям и центрам мониторинга и реагирования отвечать на эти вопросы, предоставляя доступ к экспертам мирового уровня и современным защитные технологиям:

Вопросы	Вопросы	Решения
Кто? Когда? Зачем? Что? Как?	Кто потенциальные киберпреступники? Когда они были замечены в последний раз? Какие цели они преследовали? Какие возможности у них были? Как они использовали эти возможности	Имея представление о поверхности атаки, а также о текущих тенденциях распространения вредоносных программ и кибератак против конкретной организации или страны, компания сможет сосредоточиться на уязвимостях, которые больше всего интересуют киберпреступников. Таким образом можно быстро и точно отражать вторжения и свести к минимуму риск успешной атаки. **Аналитические отчеты об APT-угрозах и угрозах для конкретных стран или организаций** содержат подробные данные об угрозах,, полученные различными способами: от обработки общедоступных данных (Open Source Intelligence, OSINT) до сбора и углубленного анализа информации с помощью распределенных по всему миру сетей «Лаборатории Касперского» и доступа к самым закрытым подпольным киберпреступным сообществам. **Сервисы тестирования на проникновения и оценки безопасности «Лаборатории Касперского»** позволяют получить информацию об уязвимостях ключевых служб и компонентов, понять возможные последствия их эксплуатации, оценить эффективность текущих средств управления защитой и запланировать дальнейшие действия для исправления обнаруженных недостатков и усиления защиты.

Вопросы	Развернутые вопросы	Решения
Как быстро реализовать сценарии? Как оперативно распространить логику обнаружения в крупных IT-сетях?	Киберпреступники быстро меняют свои инструменты и командные центры (срок жизни сервера, распространяющего вредоносное ПО, может составлять лишь несколько минут), поэтому скорость крайне важна.	Технологии и сервисы «Лаборатории Касперского» обеспечивают быстрое распространение логики обнаружения: ▪ **Kaspersky Security Network (KSN)** – глобальная репутационная база данных угроз «Лаборатории Касперского». ▪ **Kaspersky Private Security Network** – локальная копия KSN, разворачиваемая на предприятии клиента. ▪ **Kaspersky Security Center** – централизованная консоль управления продуктами «Лаборатории Касперского». ▪ **Потоки данных «Лаборатории Касперского» об угрозах** – актуальные данные об угрозах, интегрированные в текущие средства управления защитой. Они помогают эффективнее бороться с угрозами и заранее принимать защитные меры.
Какие технологии обнаружения использовать? Как расставить приоритеты? Как определить истинное или ложное срабатывание? Уникальная и распространённая угроза?	Какие технологии использовать для обнаружения? Отслеживать атаки нужно на рабочих местах или в сети? Какие события следует анализировать? Как определить, действительно ли была обнаружена угроза, или это ложноположительное срабатывание? Соответствует ли решение потребностям нашей организации?	**Kaspersky Sandbox** дополняет решение Kaspersky Security для бизнеса и помогает крупным организациям с распределенными сетями и подразделениями CERT не прибегать к услугам ИБ-аналитиков. Оно усиливает защиту против неизвестных и маскирующихся угроз и существенно повышает количество угроз, блокируемых автоматически. **Kaspersky Research Sandbox** – инструмент, который используют государственные лаборатории цифровой криминалистики для обнаружения и анализа неизвестных угроз без раскрытия конфиденциальной информации за пределами организации. В основе решения **Kaspersky Threat Attribution Engine** – обширная база данных APT-угроз. С ее помощью исследователи быстро устанавливают связь новой атаки с известными APT-угрозами, предыдущими целевыми атаками и киберпреступными организациями, для быстрого и эффективного реагирования. **Kaspersky Anti Targeted Attack Platform** – специализированная платформа, разработанная для проактивного обнаружения известных и новых целевых угроз. Она включает такие технологии, как веб-анализ, анализ почтового трафика, анализ событий на рабочих местах и песочницу. **Kaspersky Endpoint Detection and Response** обеспечивает полный обзор всех рабочих мест в корпоративной сети, расширенное обнаружение сложных угроз, автоматическое реагирование и централизованное управление инцидентами. Сервис **Kaspersky Managed Protection** позволяет заранее отслеживать угрозы в изолированных сетях с односторонним входящим потоком данных с помощью экспертизы «Лаборатории Касперского», обеспечивая абсолютную целостность систем и соблюдение требований.
Как собирать улики? Какие инструменты следует использовать	Для эффективного расследования инцидентов необходимо правильно организовать процесс и использовать подходящие инструменты. Ошибка может привести к крайне нежелательным последствиям и серьезному ущербу, а неправильные выводы – к ошибкам адаптации, в том числе к выбору неправильных приоритетов и ложным ожиданиям.	**Программа тренингов по кибербезопасности «Лаборатории Касперского»** охватывает множество тем и подходов, связанных с обеспечением кибербезопасности. Это единый блок знаний, в который входит широкий спектр специальных навыков, методик и компетенций. Программа разработана признанными экспертами «Лаборатории Касперского», которые участвовали в построении нашей антивирусной лаборатории, а теперь готовят новое поколение экспертов мирового уровня. Платформа K**aspersky Threat Lookup** помогает отследить связи между артефактами (хеши, IP-адреса, URL-адреса) и ускорить реагирование на инциденты и повысить эффективность проактивного поиска угроз. **Cloud Sandbox** позволяет моментально определить природу любого файла и выявить ранее неизвестное вредоносное ПО. Сервис реагирования на инциденты **Kaspersky Incident Response** помогает быстро разрешить инцидент кибербезопасности и минимизировать его последствия.

«Лаборатория Касперского» сотрудничает с международными правоохранительными организациями, включая Интерпол и государственные подразделения CERT. Аналитические агентства Gartner, Forrester и IDC признают «Лабораторию Касперского» и ее продукты одними из лучших на рынке. Благодаря команде экспертов по кибербезопасности мирового уровня, широкому выбору решений для аналитики угроз и облачным инструментам для глобального мониторинга в режиме реального времени «Лаборатория Касперского» имеет все возможности для точной и своевременной атрибуции угроз.

www.kaspersky.ru