KASPERSKY lab

Kaspersky Security для бизнеса: Технологии защиты рабочих мест

www.kaspersky.ru
#ИстиннаяБезопасность

Kaspersky Security для бизнеса: технологии защиты рабочих мест

В этом материале мы расскажем о современных технологиях обнаружения угроз, используемых в Kaspersky Endpoint Security для бизнеса — решении «Лаборатории Касперского» для защиты рабочих мест.

Защита конечных узлов: история развития

Раньше к конечным узлам относили только рабочие станции и серверы, но сегодня это понятие расширилось. Теперь оно включает в себя еще и мобильные устройства, а также виртуальные среды. В целом ИТ-инфраструктура в последние годы усложнилась, а ее значимость в обеспечении работы непрерывных процессов многократно возросла. Анализ больших данных, распределенное хранение, автоматизация процессов требуют современных подходов в обеспечении безопасности. Одновременно с этим отмечается растущий интерес со стороны злоумышленников к закрытым данным и финансовым активам. Большинство современных угроз представляют собой инструмент по зарабатыванию денег, приводящий жертву к крупным финансовым и репутационным потерям.

Сложные атаки служат новым вызовом разработчикам решений информационной безопасности и требуют значительного экспертного ресурса в создании эффективной защиты.

Рабочая станция продолжает оставаться точкой входа угроз и потребность в ее качественной защите усиливается.

Приведем характеристики, которыми должна обладать современная защита конечного узла:

- минимальная загрузка целевой системы — результат сбалансированной работы применяемых технологий;
- скорость детектирования: применение продвинутых методов выявления аномальной активности, в том числе с использованием экспертных облачных сервисов;
- автоматизированное расследование выявленных инцидентов;
- автоматический откат вредоносных действий в системе;
- передача информации об инцидентах в систему корреляции событий SIEM и другие решения;
- легкость в управлении — интуитивно понятный интерфейс с преднастроенным функционалом;
- централизованное управление;
- контроль целостности собственных технологий защиты;
- эффективные сервисы: поддержка продукта, расследование инцидентов, обучение и другое.

Из перечисленного видно, что современная защита это уже далеко не простой механизм сигнатурного детектирования, а целый комплекс сложных технологий, в котором особую важность приобретает— легкий в управлении.

При выборе средства защиты важно руководствоваться не только составом функциональных требований. Необходимо понимать, какие технологии применяются внутри решения и как они связаны между собой. Не менее важно оценивать уровень экспертных знаний и опыта компании и ее способность развивать технологии в дальнейшем.

Технологии с использованием машинного обучения

Техники Feature инжиниринга – процесс применения экспертных знаний для определения признаков, которые будут использоваться в алгоритмах машинного обучения.

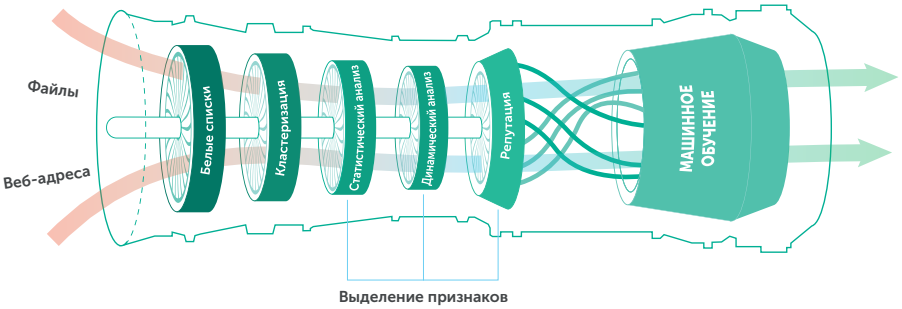
В настоящее время огромное развитие получили методы машинного обучения (machine learning, ML), успешно применяемые к большим объемам данных. Однако эффективное использование ML в целях детектирования угроз возможно

только при наличии обширного опыта и знаний в области информационной безопасности в сочетании с техниками feature-инжиниринга.

Существует заблуждение, что в задачах выявления угроз ML можно применять на сырых данных. Это не совсем так. Среди специалистов хорошо известна истина: «Мусор на входе — мусор на выходе». Для построения процесса обучения крайне важна грамотная предобработка данных и дополнение их экспертными знаниями (feature-инжиниринг). Наивно думать, что без вирусных аналитиков и глубоких экспертных знаний можно построить эффективно работающие алгоритмы. По сути аналитики выполняют надзорную роль, обеспечивая контроль работы алгоритмов и их улучшение, принимая точечное участие в верификации самых сложных угроз, где не всегда достаточно автоматического анализа.

Двадцатилетний опыт развития собственных исследовательских подразделений, анализа и накопления экспертных данных, позволил «Лаборатории Касперского» выявлять подавляющее большинство угроз автоматически, благодаря применению методов машинного обучения.

Автоматизированный центр обработки а анализа угроз



Сам центр обработки и анализа угроз можно представить в виде «турбины», где на вход подаются объекты, которые проходят уровни обработки и анализа различными технологиями, в том числе алгоритмами машинного обучения. В результате анализа на выходе получаются сформированные правила детектирования угроз, которые становятся доступны в Kaspersky Security Network.

Алгоритмы ML позволяют ежедневно обнаруживать и описывать более 310 000 уникальных угроз, большая часть которых благодаря работе облачного сервиса Kaspersky Security Network становится моментально доступной для технологий защиты конечного узла.

При этом огромное внимание уделяется недопущению ложных срабатываний. Для этого новые правила детектирования угроз проверяются по обширной базе данных чистых файлов.

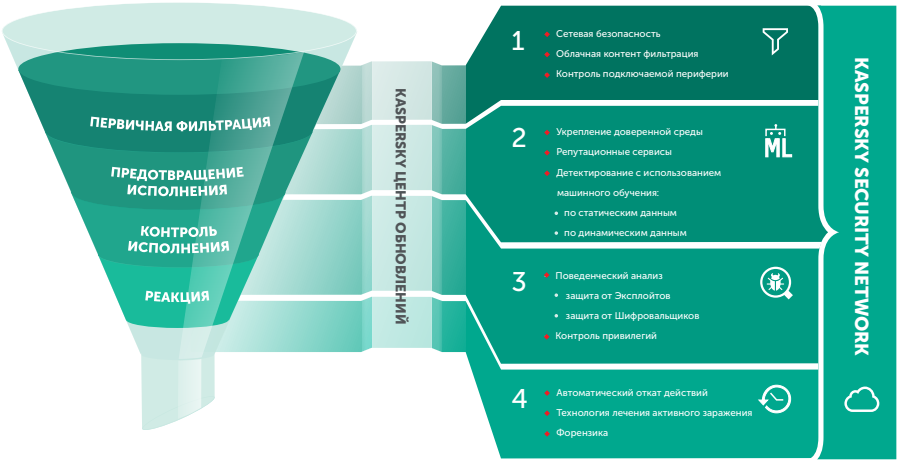
Kaspersky Security для бизнеса

Развитие угроз для бизнеса обусловило создание нового поколения защиты рабочих мест. Силами «Лаборатории Касперского» были разработаны и внедрены различные технологии защиты, в том числе использующие методы машинного обучения. Благодаря этому удалось значительно ускорить процесс обнаружения угроз и одновременно снизить общую нагрузку на целевую систему. На сегодняшний день Kaspersky Security для бизнеса (KESB) представляет собой высокоэффективный комплекс безопасности конечных узлов корпоративной сети.

Последовательность технологий защиты

Логику работы KESB можно условно разделить на четыре этапа:

Последовательность технологий защиты Kaspersky Security для бизнеса

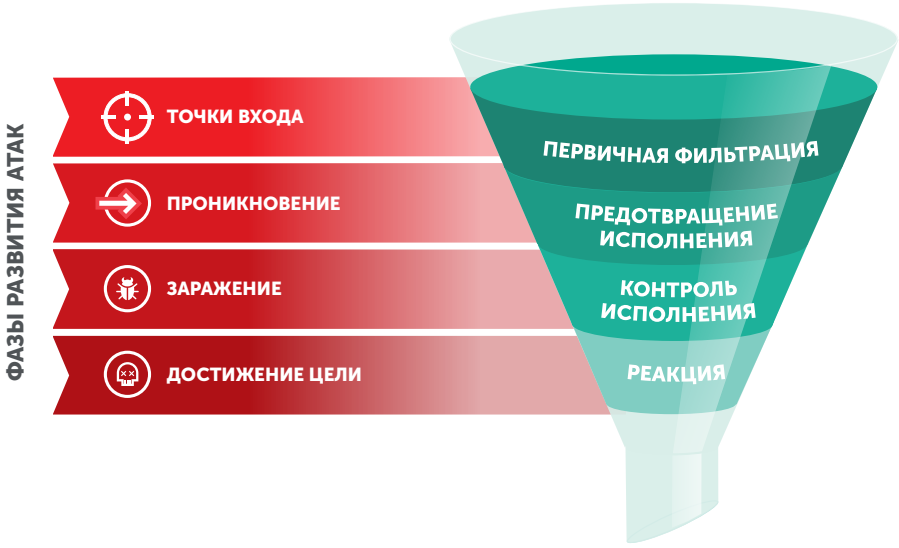


Каждый этап представлен группой самостоятельных технологий защиты. Это означает, что любая из технологий в рамках своей компетенции способна обнаружить и остановить угрозу самостоятельно, а приведенная последовательность этапов демонстрирует потенциал решения в целом. Также наряду с технологиями безопасности существуют два облачных сервиса экспертного обеспечения.

- **Центр обновлений** содержит своевременные инкрементальные обновления компонентов защиты, включая локальные экспертные базы (сигнатурная, эвристическая, база сценариев поведения и т. д.). Также в центр попадают оперативные изменения параметров всех используемых алгоритмов машинного обучения, что придает большую гибкость в обеспечении защиты.

- **Kaspersky Security Network** — облачная инфраструктура, которая обеспечивает оперативный доступ к различным статистическим данным (репутационным, контентным, поведенческим и т. д.). Благодаря этому сокращается не только время обнаружения угроз, но и экономятся вычислительные ресурсы защищаемого узла.

Приведенная последовательность технологий защиты стала ответом на фазы развития атак: на каждом из этапов обеспечивается свой уровень безопасности, необходимый для предотвращения угрозы.



Рассмотрим технологии защиты каждого этапа в отдельности.

1. Этап первичной фильтрации

Сегодня, когда угрозы распространяются через любые возможные каналы передачи информации, чрезвычайно важно обеспечить надежную защиту периметра защищаемого узла.

Первый этап – фильтр для всей входящей информации. Благодаря применению превентивных блокирующих технологий обеспечивается мониторинг основной активности защищаемого узла, позволяющий выполнять раннее обнаружение и блокирование известных угроз. Рассмотрим блокирующие технологии первого этапа.

1.1 Защита от сетевых атак

Безопасность сетевых соединений контролируется системой обнаружения вторжений (Intrusion Detection System, IDS), которая представляет собой сетевой сигнатурный сенсор. В процессе работы IDS применяет технологию глубокого инспектирования пакетов (Deep Packet Inspection, DPI), позволяя сетевому сенсору контролировать весь проходящий трафик. Благодаря этому он способен оперативно выявлять множество подозрительных и опасных сетевых событий.

Пример сетевых событий:

- активное сканирование портов;
- попытки подключения к различным портам операционной системы;
- обнаружение внештатной сетевой коммуникации, например, применения инструментов удаленного управления, команд от центров управления (в случаях с ботнетами).

При выявлении опасного события сенсор блокирует соединение, используя функционал сетевого экрана.

Сетевой экран – блокирующая технология, фильтрующая сетевую активность защищаемого узла с учетом заданных правил:

- фильтрация сетевых пакетов и потоков данных;
- активность программного обеспечения при работе с сетью.

Параметры задаются администратором в политике сетевых соединений.

1.2 Веб-фильтрация

Веб-ресурсы — одни из источников распространения угроз. Компрометация доверенного веб-узла и размещение на нем вредоносного скрипта либо эксплойта с угрозой нулевого дня делают каждодневную работу небезопасной. Для обеспечения комфортной и безопасной работы с веб-ресурсами сети в KESB применяется технология веб-фильтрации, состоящая из двух уровней защиты.

Первый уровень относится к облачному сервису **KSN** (Kaspersky Security Network) и отвечает за пассивную фильтрацию, то есть предоставляет оперативный доступ к категоризации веб-ресурсов и их репутации непосредственно перед тем, как веб-браузер начнет выполнять загрузку контента.

Категории веб-адресов, содержащиеся в репутационной базе данных KSN:

- **вредоносный** — несет опасность заражения;
- **фишинговый** — используется в целях хищения личной информации;
- **неизвестный** — отсутствует репутационная информация;
- **безопасный** — безопасный веб-ресурс.

Фильтрация позволяет значительно обезопасить работу, блокируя большую часть известных опасных веб-ресурсов и экономя вычислительные ресурсы защищаемого узла.

Второй уровень основан на технологии динамического анализа и контролирует непосредственно загружаемый контент с любых неизвестных веб-ресурсов. О нем мы расскажем во время описания технологий защиты второго этапа.

1.3 Контроль подключаемой периферии

Портативная электроника также представляет потенциальную угрозу для защищаемого узла. Контроль периферии позволяет определить тип подключенного устройства и одновременно подтвердить легитимность операции от пользователя с помощью символьного ключа. Контроль позволяет выявить случаи подмены: к примеру, когда флеш-карта пытается выдать себя за клавиатуру, чтобы избежать сканирования. Такой метод злоумышленники используют для того, чтобы усыпить бдительность технологий контроля и проникнуть внутрь защищаемого периметра. Контроль периферии тесно связан с технологиями этапа предотвращения исполнения, на котором непосредственно выполняется анализ неизвестных объектов.

2. Этап предотвращение исполнения

Для киберпреступников важно не только пройти первичную фильтрацию, но и суметь обмануть детектирующие технологии, обеспечивающие раннее обнаружение вредоносного ПО. Заражение можно считать успешным только тогда, когда вредоносному коду будет доступно исполнение внутри доверенной среды. Для этого киберпреступники непрерывно совершенствуют свои техники обхода детектирующих технологий. Перечислим основные из них:

- **упаковщик** — содержит вредоносное тело в упакованном виде, усложняя его обнаружение;
- **обфускация кода** — запутывание кода на уровне алгоритма при помощи специальных компиляторов;
- **полиморфизм** — видоизменение программного кода вируса во время каждого заражения;
- **серверный полиморфизм** — генерация вредоносным сервером нового экземпляра вредоноса при каждом обращении к серверу;
- **шифрование** — многоуровневое шифрование применяется для сокрытия части кода от детектирующих механизмов. Часто применяется вместе с обфускацией;
- **уязвимости, в том числе нулевого дня** — отдельно стоит отметить эксплуатацию уязвимостей в программном обеспечении, являющуюся эффективным механизмом заражения;
- **обход эмулятора** — антивирусный эмулятор проверяет исполняемый файл в изолированной среде, анализируя логику его работы. Обнаружение вредоносного кода происходит сигнатурным либо эвристическим методом. Хакеры используют различные практики по изменению алгоритма кода, не позволяя эмулятору определить логику выполнения зловредной программы

Комбинирование приведенных техник обхода — мощный инструмент, широко применяемый для проникновения в среду конечного узла. Противостоять ему способна лишь комплексная и технологичная защита, вооруженная современными методами контроля и анализа исполняемых объектов.

Предотвращение исполнения – это один из самых нагруженных этапов, на котором непрерывно анализируется большое количество объектов.

Рассмотрим в деталях технологии, на которых он строится, и задачи, которые выполняет.

2.1 Укрепление доверенной среды

В первую очередь осуществляется контроль доверенной среды. Это делается для снижения потенциальных угроз путем локализации и устранения уязвимостей в компонентах операционной системы и стороннего программного обеспечения.

Для этого применяется поиск уязвимостей (Vulnerability Assessment), использующий глобальную базу уязвимостей CVE (Common Vulnerabilities and Exposures). Это автоматизированный процесс, централизованно управляемый компонентом Kaspersky Systems Management. Он позволяет оперативно сообщать о выявленных угрозах в программном обеспечении и так же оперативно устранять их при помощи технологии обновления ПО (патч-менеджмент).

Технология обновления ПО способствует поддержанию актуальных версий используемых программных продуктов. В комплексе обе технологии укрепляют защищаемую среду, существенно снижая возможную эксплуатацию уязвимостей.

Для повышения качества обнаружения угроз и минимизации ложных срабатываний «Лаборатория Касперского», развивает «Технологический альянс», который включает как представителей ТОП-500 из списка производителей программного обеспечения, так и независимых разработчиков свободно распространяемого ПО. Это позволяет активно формировать белые списки в том числе для применения в технологии «Запрет по умолчанию» (Default Deny).

Отдельно важно выделить дополнительную блокирующую технологию **Default Deny** («запрет по умолчанию»). В ней реализован альтернативный подход к контролю запуска программного обеспечения в режиме, что не разрешено то запрещено.

Такой подход предоставляет возможность администратору определять необходимые и достаточные программные продукты для выполнения бизнес-задач компании.

К основным преимуществам Default Deny относятся:

- блокирование неизвестных приложений, включая новые разновидности вредоносных программ;
- возможность блокировать установку и запуск нелегитимного/нелицензионного ПО, не связанного с рабочими задачами.

Технология включает широкий набор категорий, которые администратор может присвоить ПО (доверенные производители / доверенные аккаунты, добавленные вручную / запрещенное либо нелицензированное программное обеспечение и т. д.). Списки формируются и обновляются автоматически центром обработки и анализа угроз и не требуют внимания со стороны.

2.2 Репутационные сервисы

Эта часть Kaspersky Security Network обеспечивает высочайшую скорость обнаружения угроз за счет репутационных онлайн-баз с детализированной информацией по объектам. Базы непрерывно пополняются экспертной информацией, в том числе и от детектирующих технологий других участников инфраструктуры KSN, использующих экспертное облако для защиты. Главные достоинства репутационных сервисов:

- мгновенный вердикт по объекту;
- независимость от вычислительных ресурсов конечного узла.

В результате проверки каждому файлу присваивается своя категория:

- **зловредный** — содержит вредоносный код;
- **чистый** — прошел анализ и признан безопасным;
- **неизвестный** — новый, ранее не был анализирован, потенциально опасен.

Каждый файл из категории «Неизвестный» автоматически передается на анализ технологиям детектирования с использованием машинного обучения, которые мы рассмотрим далее.

2.3 Многоуровневая защита

Заключительная задача второго этапа — выявление сложных угроз с использованием различных технологий анализа. Для этого применяется компонент многоуровневой защиты, состоящий из набора сценариев, предопределенных по типам точек входа информации.

Сценарии работы многоуровневой защиты:

Каждый сценарий обладает своим набором детектирующих технологий, но при необходимости технологии могут комбинироваться, тем самым обеспечивая требуемый уровень защиты.

Веб-фильтрация — динамическая защита

Начнем с технологии, являющейся продолжением работы «Веб-фильтрации» (этап первичной фильтрации). Она отвечает за активную фазу детектирования угроз непосредственно в загружаемом контенте. Если на первом уровне выполняется статический контроль URL, определяющий принадлежность веб-ресурса к конкретной категории, то на втором осуществляется динамический анализ неизвестного HTML-кода в момент его контролируемой загрузки.

- **Эвристический анализ скриптов**
  Особое внимание уделяется анализу скриптов, присутствующих в HTML-документе. Для этого дополнительно применяется эмулятор, способный обнаруживать сложные угрозы в различных скриптовых языках. Среди скриптовых языков, подлежащих эвристическому анализу.
  Таким образом пассивный (уровень первичной фильтрации) и активный (предотвращение вторжения) уровни «**Веб-фильтрации»** в совокупности обеспечивают безопасную работу с веб-ресурсами.

  Также технологии **«Веб-фильтрации»** применяются для контроля безопасности при работе с любыми другими точками входа информации, где может присутствовать веб-адрес: к примеру, в электронной почте или при переписке в **мессенджере**.

Электронная почта

При работе с электронной почтой, помимо анализа URL, применяются дополнительные технологии, позволяющие анализировать файловые вложения.

Дело в том, что электронная почта — одна из самых распространенных точек входа для злоумышленников. Существует целое направление социальной инженерии (Spear phishing) как инструмента направленного подготовленного воздействия, где помимо вложенного эксплойта могут содержаться закрытые архивные вложения с указанным паролем от них в теле письма либо в графическом виде. Это накладывает определенные требования к защите, а именно: умение автоматически открывать и анализировать закрытые архивы.

Перейдем к технологиям анализа файлов.

- **Сигнатурный анализ файлов**
  Технология сигнатурного анализа применяется в различных сценариях защиты, где требуется быстрая идентификация объекта на наличие угрозы. В сценарии электронной почты она необходима для проверки вложенных файлов.

  Сам сигнатурный метод детектирования обладает рядом преимуществ, благодаря которым при анализе файлов он применяется первым. Вот основные из них:
  - высокая скорость детектирования;
- - минимальный уровень ложных срабатываний;
- - нетребовательность к вычислительным ресурсам защищаемого узла.
  Такой метод детектирования ограничен количеством сигнатур, находящихся в пополняемой базе данных. По этой причине сигнатурный анализ работает в паре с анализом эвристическим.

- **Детектирование с использованием методов машинного обучения**
  Непосредственно анализ файлов с использованием машинного обучения мы детально рассмотрим далее. А в сценарии защиты электронной почты машинное обучение играет следующую роль: оно обеспечивает уникальную возможность распаковывать защищенные паролем архивные вложения путем извлечения оставленного в теле письма пароля (в графическом, либо текстовом виде). Этот метод злоумышленники используют как одну из техник обхода детектирующих технологий, где защищенный архив играет роль «сейфа», недоступного для анализа. Для распознавания пароля в графическом виде применяется алгоритм машинного обучения. После этого пароль используется для извлечения содержимого из защищенного паролем архива.

Сигнатура – это фрагмент кода, который позволяет обнаружить вредоносный объект.

Устройства хранения

Каждый **неизвестный** файл представляет собой потенциальную угрозу для защищаемого узла и требует отдельного внимания со стороны технологий защиты.

Для таких случаев в многоуровневой защите предусмотрен продвинутый сценарий, в котором обеспечивается глубокий анализ с применением методов машинного обучения.

Существует несколько технологий анализа файлов.

- **Сигнатурный анализ файлов,**
  основные преимущества которого были приведены в сценарии электронной почты. В этом сценарии технология выполняет задачу грубого фильтра, оставляя только неизвестные файлы для анализа с использованием методов машинного обучения. Благодаря сигнатурному анализу также экономятся вычислительные ресурсы защищаемого узла.

- **Детектирование с использованием методов машинного обучения**
  Самая продвинутая технология многоуровневой защиты. Выполняет глубокий анализ файлов в целях раннего обнаружения угроз. Технология основывается на выполнении двух параллельных процессов, обеспечивающих детектирование по статическим и динамическим данным.

Оба процесса делятся на три этапа, состоящие из своих групп технологий. Статический и динамический подходы дополняют друг друга, компенсируя возможные недостатки:
- При обучении модели на статических признаках вредоносов могут встретиться файлы, слабо отличающихся от чистых;
- При обучении модели на динамических признаках не каждая зловредная программа проявит свое поведение. Для этого может потребоваться специфическое окружение, либо специальная командная строка для запуска.

Далее мы подробно рассмотрим особенности работы каждого из процессов.

Детектирование по статическим данным

Статические данные – собранная информация об объекте без его исполнения. Технология обладает высокой обобщающей способностью и производительностью.

Препроцессор, подготовительные технологии:

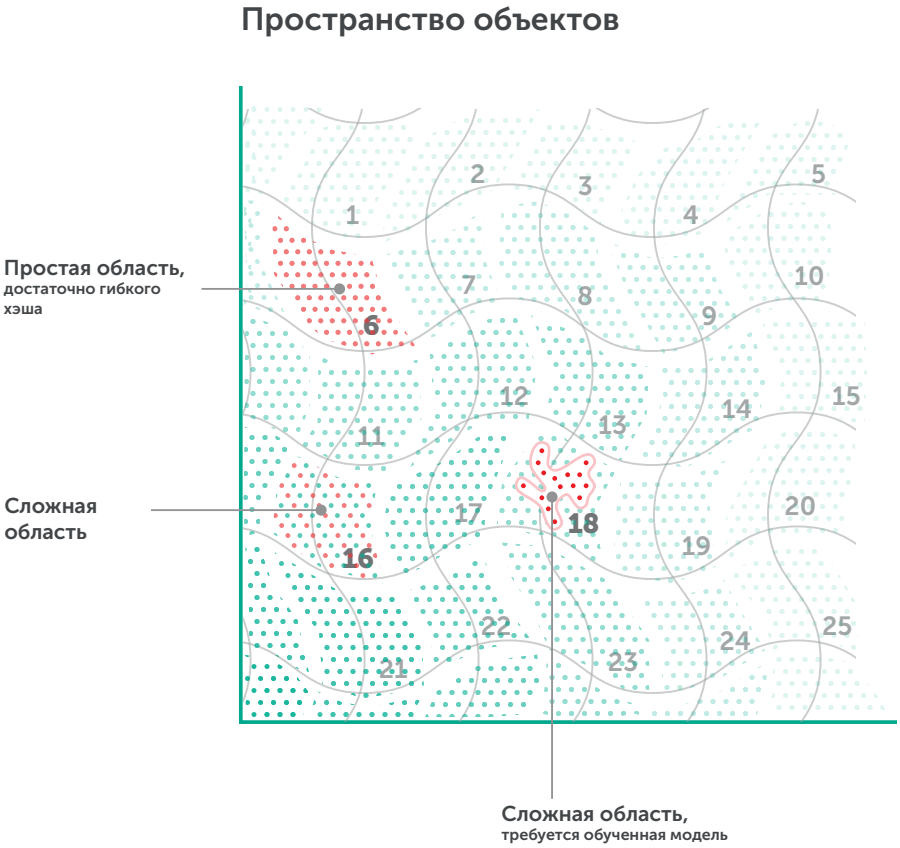
- **распаковщики** извлекают упакованный код, обеспечивая возможность извлечения метаданных парсерами (упаковщик, обфускация, шифрование – стандартные методы обхода, применяемые злоумышленниками);

- **парсеры** — инструменты извлечения различных наборов метаданных.

Разнообразие метаданных напрямую влияет на качество детектирования, поэтому препроцессор содержит большую библиотеку различных парсеров. Они поставляют информативные признаковые описания (структуры исполняемых файлов, статистические характеристики данных и кода, строки и т. д.).

Детектор выносит решение о вредоносности объектов, анализируя признаковые описания. Работа детектора происходит в два этапа.

На первом вычисляется гибкий хеш, позволяющий эффективно проверить, находится ли проверяемый объект в «грязной» области. Если область простая (то есть в ней встречаются объекты одного класса: только «чистые» либо только «грязные»), на этом этапе может быть выдан детект. Преимущество гибкого хеша — устойчивость к полиморфизму и обфускации, что позволяет существенно экономить вычислительные ресурсы защищаемого узла.



Гибкий хэш строится на основе признаков таким образом, чтобы он был одинаков у группы файлов.

Область – часть пространства объектов, которой соответствует гибкий хеш, либо обученная модель.

Если область сложная (в ней встречаются как «грязные», так и «чистые» объекты), объект передается на второй этап. На нем признаковые описания объекта оцениваются классификатором, в задачи которого входят поиск и применение подходящей обученной модели (специализирующейся на этой области) из числа многих, содержащихся в базе данных. Обученная модель выдает окончательное решение о том, является ли объект вредоносным.

Детектирование по динамическим данным

Препроцессор собирает динамическую информацию: поведение объекта, области памяти с исполняемым кодом и другие.

Динамические данные – информация об объекте, собираемая в момент его исполнения или эмуляции, в том числе о его поведении.

Эмулятор позволяет запустить исполняемый файл в контролируемой среде, частично имитирующей реальную систему. К его достоинствам относятся низкие требования к вычислительным ресурсам и безопасность (так как исключено воздействие анализируемого кода на доверенную среду). В результате работы динамического анализа мы получаем записанную последовательность действий исполняемого файла, а также дамп памяти и другие объекты, которые были порождены в результате его исполнения (например, созданные файлы). Все перечисленные данные представляют собой базовые поведенческие признаки.

Дамп памяти позволяет получить доступ к оригинальному (неупакованному) коду, а также обнаружить данные, которые указывают на вредоносное предназначение.

Детектор выносит решение о вредосности объектов, выявляя вредоносные поведенческие сценарии.

В работе детектор использует библиотеку вредоносных сценариев, которая формируется автоматизированным центром «Лаборатории Касперского» для обработки и анализа угроз.

Вредоносный сценарий – последовательность действий, реализующих атаку.

Центр, обладая большими коллекциями вредоносных и чистых (незараженных) файлов, непрерывно обрабатывает их, извлекая базовые поведенческие признаки, на которых обучает модели. Те преобразуются в сценарии поведения и поставляются детектору в режиме инкрементальных обновлений. Такой подход значительно сокращает время и размер самого обновления, позволяя оперативно поддерживать эффективность работы детектора.

Ложное срабатывание – ошибочное заключение детектора, о том, что чистый объект является вредоносным.

Минимизация ложный срабатываний

Каждое решение, вынесенное детектором, дополнительно проверяется на предмет ложного срабатывания.

Ложные срабатывания имеют крайне низкую вероятность, но могут повлечь за собой серьезные негативные последствия.

В целях минимизации ложных срабатываний при срабатывании детекта выполняются как минимум следующие проверки:

- запрос в облачный сервис KSN с номером обученной модели или сценария поведения, принявших решение об угрозе (KSN содержит информацию об актуальных моделях и сценариях поведения, тем самым предоставляя возможность проверить, не отозваны ли они);
- запрос к **белым спискам** облачного сервиса KSN, которые позволяют исключить ложные срабатывания детектора (Белые списки – это большая коллекция достоверно «чистых» файлов, непрерывно обновляемая автоматизированным центром «Лаборатории Касперского»);
- запрос в облачную систему классификации сертификатов для проверки репутации сертификата, подписывающего файл.

Говоря о втором этапе, важно отметить наличие локального кеша KSN, позволяющего избежать повторных запросов на уже проверенные объекты и тем самым сэкономить вычислительные ресурсы защищаемого узла.

3. Контроль исполнения

Несмотря на то, что на втором этапе производится статический и динамический анализ, часть угроз может пройти дальше. Например, многокомпонентные шифровальщики, использующие легитимное ПО с функцией шифрования, могут не вызвать подозрений, так как каждый компонент по отдельности не представляет угрозы.

Задача третьего этапа заключается в обнаружении вредоносного поведения внутри доверенной среды. В ходе анализа учитывается суммарное поведение всех активных компонентов, включая доверенные и недоверенные приложения, а также системные компоненты. Такой анализ позволяет выявлять сложные многокомпонентные угрозы.

Уязвимость нулевого дня – допущенные ошибки в коде, позволяющие злоумышленнику использовать недокументированные возможности исполнения программы для компрометации системы, при этом для исправления ошибок еще недоступен патч.

Поведенческий анализ видит реальное поведение, а не предполагаемую (эмулируемую) картину действий, которая анализируется на этапе предотвращения вторжения.

Другой пример — предотвращение эксплойтов. В этом случае происходит обнаружение вредоносного поведения внутри доверенного приложения.

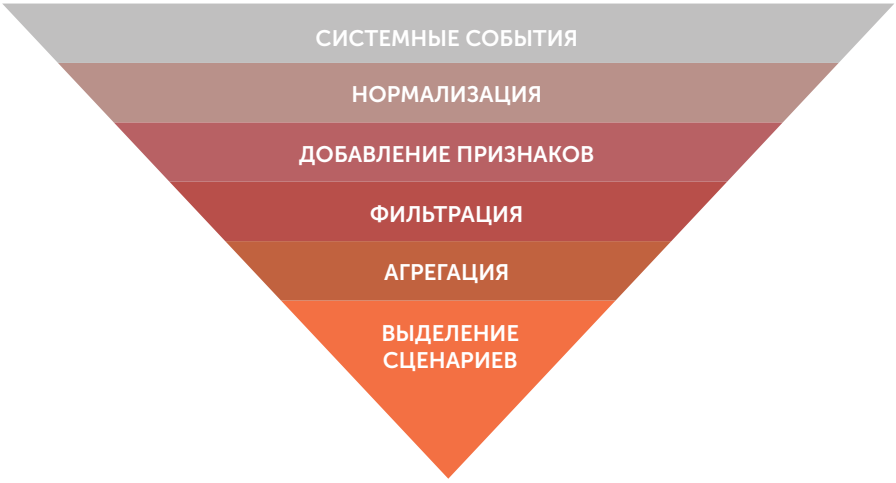
Например, при открытии документа Word, содержащего эксплойт, технология Автоматической защиты от эксплойтов (Automatic Exploit Prevention, AEP) обнаружит вредоносное поведение и заблокирует его. Технология эффективна и позволяет блокировать сложные угрозы, в том числе эксплоиты для уязвимостей нулевого дня.

3.1 Поведенческий анализ

Эта технология анализирует поведение всех активных компонентов внутри доверенной среды защищаемого узла. Выделяются следующие уровни анализа:

- **системные события** — мониторинг ключевых системных событий (создание процессов, изменение ключевых значений реестра, изменение файлов и т. д.);
- **нормализация** — приведение всех получаемых событий к общему виду для последующей обработки;
- **добавление признаков** — получение дополнительной информации для части событий: например, является ли измененный файл исполняемым;
- **фильтрация, агрегация, выделение сценария** — на этих этапах выделяются значащие комбинации и последовательности событий, которые складываются в сценарий поведения. Библиотека вредоносных сценариев формируется автоматизированным центром «Лаборатории Касперского» для обработки и анализа угроз.

Поведенческий анализ



3.2 Контроль привилегий

Параллельно с поведенческим анализом выполняется контроль привилегий, основанный на политиках и категоризации приложений.

Контроль заключается в мониторинге активности приложений и накладывании ограничений, исходя из тех свойств, которыми они обладают: известность в мире, доверие издателю, наличие детекта и т. д. Благодаря этому программа не может бесконтрольно выполнять действия внутри защищаемой среды, например, осуществлять сетевой обмен или другие действия.

Базовые ограничения для разных категорий приложений создаются технологиями автоматизированного центра обработки и анализа угроз «Лаборатории Касперского».

Например, к приложениям Microsoft или другим широко известным приложениям будет применена слабая политика контроля. С другой стороны, для малоизвестных или noname приложений система контроля привилегий сформирует политику, по строгости соответствующую той опасности и рискам, которые это приложение может вызвать.

Контроль привилегий работает в паре со списками доверенных программ Default Deny, если этот режим активирован, обеспечивая безопасность в режиме реального времени. Ограничениями можно управлять централизованно на уровне корпоративной сети или настраивать защиту персональных данных индивидуально.

4. Процесс исправления

Заражение – это исполнение вредоносного кода внутри доверенной среды. В этом случае исполняемый процесс находится на пути к достижению намеченных злоумышленниками целей, порождая своей активностью цепь различных событий. Обычно такие ситуации происходят в случае установки защитного решения на заведомо инфицированный узел, либо в случае выявления потенциально опасной активности уровнем поведенческого анализа. К примеру, когда шифрование файлов запускается легитимным процессом на локальном диске защищаемого узла.

В таких случаях начинается четвертый этап защиты, отвечающий за экстренное реагирование на угрозу.

4.1 Реакция

В каждом случае блокирования потенциально опасной активности технологиями защиты поведенческого анализа требуется выполнить комплекс мер, направленных на возврат к прежнему состоянию доверенной среды.

Автоматический откат действий отменяет выполненные изменения, следуя по шагам заблокированного процесса. Фактически он «раскручивает» цепочку событий, возвращая структуру к исходному состоянию. В этом ей способствует технологии этапа **поведенческого анализа,** предоставляющие детальную историю действий по конкретному процессу.

Цепь событий может включать в себя:

- ветки реестра операционной системы;
- созданные процессом исполняемые файлы (скрипты или бинарные файлы);
- измененные файлы, например, те, которые успел зашифровать шифровальщик.

В ряде сложных случаев (например, когда зловредный код внедрил себя в системный процесс, на который невозможно повлиять, не затронув стабильность операционной системы) подключается технология, отвечающая за лечение активного заражения. Этот инструмент способен безопасно восстановить зараженные файлы, в том числе компоненты операционной системы. В случае активного лечения происходит перезагрузка защищаемого. При этом выполняется замена зараженных системных компонентов методом замещения. Для этого технология обладает широким функционалом поиска оригинальных файлов для восстановления. Таким образом система приводится к стабильному состоянию.

4.2 Цифровая криминалистика

Каждый инцидент информационный безопасности при анализе требует своей доказательной базы. Благодаря тому, что технологии защиты собирают расширенные данные, предоставляется возможность изучить выявленный инцидент для принятия мер профилактики информационной безопасности.

Меры собственной безопасности

Для гарантированно надежной работы решение обладает средствами контроля собственной безопасности. Это обеспечивает целостность защиты, в том числе и от попыток отключения ее самим пользователем.

Самозащита перехватывает и запрещает небезопасные операции с ресурсами внутри доверенной среды вне зависимости от прав и привилегий пользователя. Таким образом решается вопрос с уязвимостями, позволяющими завладеть привилегированным доступом администратора.

Управление

Для гибкого централизованного управления защитой был разработан компонент Kaspersky Security Center. Центр управления позволяет получить доступ к детальной информации об уровне защищенности конечных узлов, централизованной политике безопасности. Таким образом центр становится единой точкой агрегации всех угроз и управления защитой корпоративной сети.

Отдельно важно сказать о его расширенном функционале, доступном в компоненте Kaspersky System Management. Он повышает защищенность корпоративной сети за счет следующих возможностей:

- мониторинг уязвимостей и управление установкой обновлений;
- учет аппаратного и программного обеспечения;
- гибкое развертывание операционных систем и приложений;
- распространение ПО;
- интеграция с SIEM-системами;
- разделение прав доступа в сложных корпоративных сетях.

www.kaspersky.ru

#ИстиннаяБезопасность