KASPERSKY lab

KASPERSKY SECURITY ДЛЯ БИЗНЕСА: ТЕХНОЛОГИИ В ДЕЙСТВИИ

Эффективная борьба с известными, неизвестными и сложными угрозами

kaspersky.ru/business

СОДЕРЖАНИЕ

В течение года 98% предприятий столкнулись с инцидентами кибер-безопасности, источники которых находились за пределами компании

Отчет Информационная безопасность бизнеса, 2014 г.

БИЗНЕС ПОД УГРОЗОЙ

В последние годы количество кибератак на предприятия малого и среднего бизнеса значительно возросло.

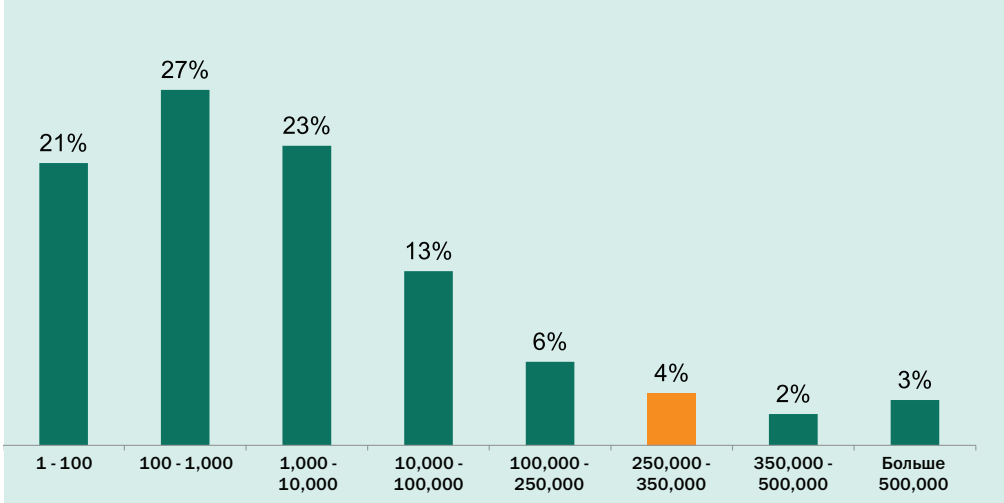
НЕЗНАНИЕ УГРОЗ НЕ ОСВОБОЖДАЕТ ОТ УЩЕРБА

По данным исследования «Информационная безопасность бизнеса», проведенного «Лабораторией Касперского» и B2B International в 2014 г., 98,5% российских предприятий среднего и малого бизнеса в течение года как минимум раз подвергались внешней атаке, а 82% – испытали на себе действие внутренних угроз. Наиболее распространенной мерой обеспечения информационной безопасности является антивирусное ПО, однако при этом лишь 60% опрошенных сообщили, что своевременно обновляют установленную в организации защиту. Возможно, вы полагаете, что ваш бизнес слишком скромен, чтобы представлять интерес для киберпреступников? Но именно на такое отношение они и рассчитывают!

ЗНАТЬ ВРАГА В ЛИЦО

Допустим, вы принадлежите к 60% предприятий, где установлено то или иное решение для обеспечения IT-безопасности рабочих станций. Однако это еще не гарантия полноценной защиты. К сожалению, большинство бизнес-пользователей недооценивают масштаб угроз. Так, лишь 4% опрошенных более или менее точно назвали количество угроз, обнаруживаемых каждый день.[1]

ОЦЕНКА КОЛИЧЕСТВА ЕЖЕДНЕВНО ПОЯВЛЯЮЩЕГОСЯ ВРЕДОНОСНОГО ПО



Многие также недооценивают важность средств для обеспечения IT-безопасности и не видят особой разницы между различными вариантами защиты. Это очень опасное заблуждение! Даже 1% разницы в уровне обнаружения у разных решений может обернуться проникновением тысяч вредоносных объектов. Откуда мы это знаем?

- «Лаборатория Касперского» ежедневно обнаруживает около 325 000 новых образцов вредоносного ПО.
- За второй квартал 2015 г. наши защитные решения выявили 379 972 834 вирусные атаки на системы конечных пользователей, обнаружив при этом 110 731 713 уникальных вредоносных объектов.[2]

Наибольшую опасность представляют неизвестные угрозы. Эксперты «Лаборатории Касперского» каждый день следят за появлением новых угроз, анализируют их и разрабатывают меры противодействия. Кроме того, наш огромный экспертный опыт в области анализа угроз позволяет обеспечить дополнительную защиту от самых сложных угроз, так называемых APT (Advanced Persistant Threats, или комплексных таргетированных атак).

Мы наблюдаем значительный разрыв между представлением организаций о масштабах и характере угроз и реальным положением дел. Мы назвали эту ситуацию разрывом восприятия. Компании любого размера катастрофически недооценивают как объем угроз, так и их серьезность.

Костин Райю, директор глобального центра исследования и анализа угроз, «Лаборатория Касперского»

[1] Информационная безопасность бизнеса, 2014 г.
[2] «Лаборатория Касперского», отчет о развитии информационных угроз во втором квартале 2015 г.

ПРОАКТИВНАЯ, РЕАКТИВНАЯ И ИНТЕЛЛЕКТУАЛЬНАЯ ЗАЩИТА

Специалисты «Лаборатории Касперского» первыми обнаружили многие наиболее опасные угрозы, такие как Carbanak (вирус, ответственный за крупнейшее в мире киберхищение денег из банка), Darkhotel, The Mask, Icefog и Red October. Более трети наших сотрудников трудятся в департаменте исследований и разработки (R&D). Они проектируют и создают технологии для выявления и нейтрализации постоянно развивающихся угроз, которые ежедневно изучаются нашими аналитическими и исследовательскими группами. Все это позволило нам разработать эффективную многоуровневую платформу безопасности для борьбы с известными, неизвестными и сложными угрозами.

Как она действует? Давайте подробно рассмотрим работу технологий «Лаборатории Касперского» для обнаружения угроз и защиты от вредоносного ПО с момента загрузки файла.

ОБНАРУЖЕНИЕ ИЗВЕСТНЫХ УГРОЗ

Непосредственно перед загрузкой файла, открытием веб-страницы или запуском приложения антивирусное ядро «Лаборатории Касперского» проверяет их на наличие вирусов, троянцев, руткитов, червей, шпионских программ, вредоносных скриптов и других известных вредоносных и нежелательных объектов, и обеспечивает надежную защиту от них.

ЗАЩИТА ОТ СЕТЕВЫХ АТАК

Проверяет сетевой трафик, выявляя и блокируя сетевые атаки: сканирование портов, атаки типа «отказ в обслуживании», атаки через переполнение буфера и другие удаленно запускаемые вредоносные действия.

ФИЛЬТРАЦИЯ URL-АДРЕСОВ

Сканирует входящий и исходящий трафик, проверяя обнаруженные в нем URL-адреса по базе «Лаборатории Касперского», содержащей данные об известных на сегодняшний день вредоносных и фишинговых сайтах. Это позволяет эффективно блокировать интернет-атаки, полиморфное серверное вредоносное ПО и командные серверы ботнетов (C&C).

ЧЕРНЫЕ СПИСКИ

Базы «Лаборатории Касперского» регулярно обновляются и пополняются сигнатурами новейших образцов вредоносного ПО и другими актуальными данными. Это позволяет автоматически блокировать все известные на текущий момент вредоносные программы.

СЕТЕВОЙ ЭКРАН

Анализирует каждый пакет данных, поступающий в локальную сеть или покидающий ее, и блокирует либо пропускает его в зависимости от наличия угроз безопасности. Несанкционированные подключения блокируются, чтобы сократить зону возможной атаки и снизить вероятность заражения. Сетевая активность зараженных компьютеров ограничивается, чтобы помешать распространению вредоносного ПО и уменьшить ущерб, вызванный нарушением политик безопасности.

Сигнатурные методы «Лаборатории Касперского» разработаны с учетом многолетнего опыта и знаний наших экспертов. Все перечисленные выше технологии построены на использовании сигнатур и отлично справляются с блокированием известного вредоносного ПО. Однако остаются еще неизвестные и сложные угрозы. Как быть с ними? Читайте дальше, и вы об этом узнаете.

ОБНАРУЖЕНИЕ НЕИЗВЕСТНЫХ УГРОЗ

Если файл прошел проверку по сигнатурным базам известных угроз, это еще не означает, что он безопасный. Необходимо выяснить, что происходит в момент его запуска. Многоуровневые проактивные технологии «Лаборатории Касперского» анализируют и проверяют файлы во время их выполнения, выявляя подозрительную или вредоносную активность, которая свидетельствует о наличии неизвестной угрозы.

ЭВРИСТИЧЕСКИЕ МЕТОДЫ

Эвристический анализ обеспечивает проактивную защиту от угроз, которые не удается обнаружить с помощью традиционных антивирусных баз. К таким угрозам относится новое вредоносное ПО или неизвестные модификации известного вредоносного ПО. Статический анализ сканирует код запускаемой программы на наличие признаков подозрительных команд. Динамический анализ изучает возможные действия файла, эмулируя их в безопасной среде, и в случае обнаружения подозрительной активности блокирует его выполнение.

ЭВРИСТИЧЕСКИЙ АНТИФИШИНГ

В случае новейших фишинговых атак, от которых пока пострадало лишь небольшое число пользователей, технология «Лаборатории Касперского» выявляет дополнительные признаки подозрительной активности, анализируя различные параметры открываемой страницы, включая используемую лексику, формы для ввода данных и трудночитаемые последовательности символов. Эта технология дополняет традиционную проверку по базе фишинговых ссылок.

Многие из недавних наиболее опасных угроз начинались именно с фишинговых атак.

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (HIPS)

Система предотвращения вторжений (HIPS), разработанная «Лабораторией Касперского», обеспечивает дополнительный уровень защиты, выявляя подозрительные приложения и ограничивая их активность, чтобы предотвратить запуск вредоносного кода. Принцип работы HIPS заключается в присвоении каждому приложению после его первоначального анализа определенной степени доверия. Эта характеристика определяет, какие ресурсы может использовать приложение, какие данные считывать или изменять и т.д. Система HIPS блокирует выполнение потенциально опасных программ, не снижая производительность безопасных приложений. Недоверенным приложениям не разрешаются никакие действия, в том числе запуск.

КОНТРОЛЬ ПРОГРАММ И БЕЛЫЕ СПИСКИ

Контроль программ блокирует или разрешает выполнение указанных администратором программ. «Лаборатория Касперского» использует динамические белые списки – постоянно обновляемые списки безопасных приложений и категорий ПО, которое разрешается запускать в соответствии с заданными правилами и политиками. В компании работает специализированная Whitelisting-лаборатория, сотрудники которой регулярно обновляют и пополняют базу белых списков. В настоящее время база насчитывает более миллиарда файлов и ежедневно пополняется миллионом новых.

Контроль программ с поддержкой динамических белых списков значительно снижает риски, связанные с активностью еще не известных угроз. Большинство вредоносных программ представляют собой исполняемые файлы, которых нет ни в одном белом списке. Это значит, что организации, следующие такой модели защиты (и применяющие соответствующие технологии), могут предотвратить выполнение вредоносного файла без точного определения его особенностей.

KASPERSKY SECURITY NETWORK

Kaspersky Security Network – это глобальная облачная сеть безопасности, которая за считаные секунды обнаруживает, анализирует и помогает нейтрализовать известные, неизвестные и новые угрозы и источники кибератак, передавая последние данные о них непосредственно на компьютеры клиентов «Лаборатории Касперского».

Таким образом, каждый файл, проходящий через системы, находящиеся под защитой «Лаборатории Касперского», анализируется при помощи самой актуальной информации об угрозах. Эти сведения собираются в режиме реального времени с компьютеров миллионов пользователей, разрешивших сбор подобных данных. В сочетании с другими защитными технологиями облачная сеть KSN позволяет обеспечить защиту от неизвестных угроз еще до получения их сигнатур. На подготовку традиционного сигнатурного ответа на новую угрозу могут уйти часы, а Kaspersky Security Network позволяет реагировать почти мгновенно.

ОБНАРУЖЕНИЕ СЛОЖНЫХ УГРОЗ

Итак, файл загружен и запущен. Технологии «Лаборатории Касперского» просканировали его, проанализировали с использованием самых актуальных данных и запретили или разрешили его исполнение по итогам проверки на наличие известных и неизвестных угроз.

А как быть с так называемыми сложными угрозами?

Технологии обнаружения сложных угроз разработаны «Лабораторией Касперского» для выявления и блокирования самых изощренных вредоносных атак. Проактивные технологии отслеживают поведение программ, выявляя подозрительную активность, блокируют вредоносные действия и выполняют отмену опасных изменений, в том числе вызванных программами-шифровальщиками.

МОНИТОРИНГ СИСТЕМЫ

Отслеживает активность приложений и других важных системных процессов, собирая данные и выявляя закономерности в их поведении. Полученная информация передается в описанные выше защитные компоненты «Лаборатории Касперского». Подозрительная активность обрабатывается в соответствии с заданными администратором политиками. Вредоносные процессы по умолчанию блокируются и помещаются в карантин для дальнейшего анализа.

Данный компонент также осуществляет мониторинг вносимых в реестр изменений, а сетевой экран собирает данные о сетевой активности приложений. Все это позволяет реагировать на сложные системные события, такие как установка драйверов.

Все вредоносные и подозрительные действия, говорящие о возможном наличии вредоносного кода, блокируются.

АВТОМАТИЧЕСКАЯ ЗАЩИТА ОТ ЭКСПЛОЙТОВ (AEP)

Эта технология противодействует вредоносному ПО, которое использует уязвимости в программном обеспечении. Технология AEP разработана с учетом углубленного анализа особенностей наиболее широко распространенных эксплойтов. Она позволяет выявлять характерные для них поведенческие закономерности и блокировать их выполнение. Автоматическая защита от эксплойтов работает в связке с компонентом «Мониторинг системы» и служит эффективным дополнением к другим защитным технологиям «Лаборатории Касперского».

ОТМЕНА (ОТКАТ) ВРЕДОНОСНЫХ ДЕЙСТВИЙ

Постоянный тщательный мониторинг системы делает возможной пошаговую отмену вредоносных действий, что позволяет свести к минимуму последствия заражения, вернув систему к первоначальным безопасным параметрам.

РЕЖИМ «ЗАПРЕТ ПО УМОЛЧАНИЮ»

Эта политика все чаще признается наиболее эффективной в борьбе с постоянно развивающимися сложными угрозами. В этом случае на рабочих местах блокируется выполнение любых приложений, кроме разрешенных администратором.

В режиме «Запрет по умолчанию» автоматически блокируются все разновидности нового вредоносного ПО, в том числе используемого в ходе целевых атак.

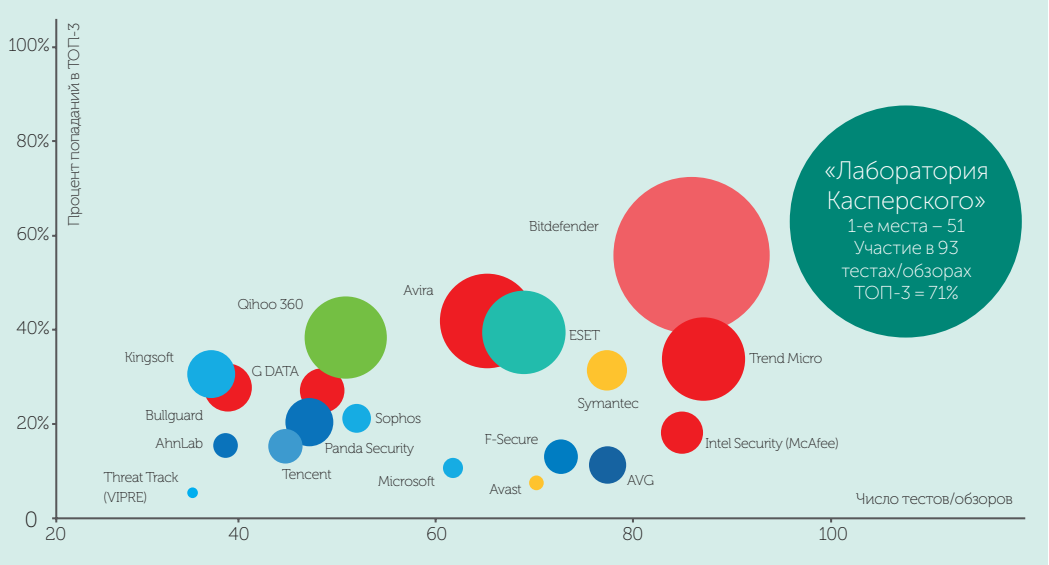
ИНОГДА НЕБОЛЬШИЕ ОТЛИЧИЯ ОЧЕНЬ ВАЖНЫ

Даже 1% разницы в уровне обнаружения у разных решений может обернуться проникновением тысяч вредоносных объектов. Теперь вы знаете, каким образом уникальные технологии обнаружения, анализа и нейтрализации угроз, разработанные «Лабораторией Касперского», позволяют эффективно выявлять и блокировать известные, неизвестные и даже самые сложные угрозы – до того, как они успеют нанести вам серьезный ущерб.

ПОЧЕМУ «ЛАБОРАТОРИЯ КАСПЕРСКОГО»?

*Потому что «Лаборатория Касперского» обеспечивает лучшую защиту**

Эффективность продуктов «Лаборатории Касперского» регулярно подтверждается результатами независимых тестов. В 2014 году компания заняла первое место среди производителей защитных решений по показателю ТОП-3. По итогам 93 различных испытаний, проведенных авторитетными тестовыми организациями разных стран, решения «Лаборатории Касперского» вошли в тройку лидеров в 71% случаев и 51 раз занимали первое место. Это неоспоримое доказательство того, что «Лаборатория Каперского» предоставляет лучшую в отрасли защиту.



** Примечание*

- *Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2014 год*
- *В обзор включены тесты, проведенные следующими независимыми тестовыми лабораториями и изданиями: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs; Virus Bulletin*
- *Диаметр круга соответствует числу занятых первых мест*

Подробнее: kaspersky.ru/top3

О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

+7 (495) 737-34-12
sales@kaspersky.com
www.kaspersky.ru/business