KASPERSKY lab

УГРОЗЫ БУДУЩЕГО: БУДЬТЕ К НИМ ГОТОВЫ

Специальный отчет о стратегиях борьбы со сложными угрозами

kaspersky.ru/corporate

СОДЕРЖАНИЕ

АТАКИ КЛАССА APT И ОБЩЕЕ ПОЛОЖЕНИЕ ДЕЛ

Кибербезопасность – это не игра, где можно рассчитывать на удачу. Поскольку всего одна вредоносная программа может нанести серьезный ущерб бизнесу, то обычной системы безопасности, которая защищает от большинства атак, будет явно недостаточно.

Поэтому разумно сосредоточить усилия и на более опасных угрозах, а не только на тех, которые встречаются повсеместно.

Все вредоносное ПО можно разделить на **известные** (70%), **неизвестные** (29%) и **сложные** угрозы (1%).

Известные угрозы - это те, от которых сравнительно легко защититься. Если вредоносный код удалось распознать, то его можно заблокировать. С этим, как правило, справляются традиционные сигнатурные методы.

Для борьбы с неизвестными угрозами требуются интеллектуальные методы, применяемые сегодня в индустрии ИБ. Помимо сигнатурного анализа, появившегося раньше остальных технологий защиты, среди них можно назвать эвристический анализ и динамические белые списки.

К сложным угрозам относятся атаки класса APT (Advanced Persistent Threats), которые непрерывно ведутся по нескольким направлениям. Они проникают в сеть, незаметно собирают конфиденциальные данные и могут оставаться незамеченными на протяжении нескольких лет.

APT-атака, известная под именем Darkhotel, действовала через сети Wi-Fi в элитных отелях и похищала данные посетителей в течение семи лет. Данная угроза представляет особый интерес, поскольку она действовала весьма избирательно (охотясь преимущественно за данными высшего руководства компаний) и продемонстрировала, насколько важно обеспечить безопасность рабочих мест, в том числе ноутбуков и планшетов, даже когда те покидают защитный периметр корпоративной сети.

Атака класса APT, известная под именем Darkhotel, действовала через сети Wi-Fi в элитных отелях и похищала данные посетителей в течение семи лет.

Жертвами APT-атак стали несколько очень известных организаций, но чтобы попасть в сферу интересов киберпреступников, совершенно необязательно быть крупной и известной по всему миру корпорацией. Предприятиям нужно предотвратить проникновение в свою сеть таргетированных угроз и избежать возможных убытков, будь то потеря данных, продолжительный простой в работе или серьезный ущерб репутации. Профилактика целевых атак обходится намного дешевле, чем устранение их последствий (бывает, что атака началась несколько месяцев, а то и несколько лет назад и уже успела нанести серьезный или, что еще хуже, непоправимый ущерб).

Не существует какого-то одного универсального способа решения такой проблемы. Технологии, применяемые для борьбы с известными и новыми угрозами, полезны, но сами по себе не могут служить адекватным ответом на комплексные целевые атаки. В ситуации, когда угрозы становятся все более сложными и изощренными, требуется многоуровневая организация безопасности, где сочетание интегрированных технологий обеспечивает комплексное обнаружение и защиту от известных, неизвестных, сложных угроз и других типов вредоносного ПО.

Данный отчет поможет подготовиться к борьбе с комплексными целевыми атаками.

По результатам совместного опроса «Лаборатории Касперского» и B2B International средний ущерб от серьезного инцидента информационной безопасности составляет 780 тыс. рублей для российских компаний малого и среднего бизнеса и 20 млн рублей для крупных компаний[1].

Масштаб последствий APT-атак может быть очень велик. В 2014 году «Лаборатория Касперского» помогла обнаружить угрозу Carbanak. Эта комплексная атака позволила международной преступной группе похитить миллиард долларов США из различных финансовых учреждений. Заразив сеть банка, эта группа получила доступ к информации, отображавшейся на экранах сотрудников, и смогла подробно изучить процедуру перевода денег, оставаясь при этом полностью незамеченной.

[1] Отчет «Информационная безопасность бизнеса, 2014

ПОД ПРИЦЕЛОМ – КРУПНЫЕ ПРЕДПРИЯТИЯ

Крупные предприятия знают об актуальных угрозах IT-безопасности, которые становятся все более изощренными и целенаправленными.

1 Первым шагом в разработке подходящей стратегии борьбы с комплексными целевыми атаками становится понимание того, что ваша компания, как и любая другая, является потенциальной жертвой. Реальность такова, что у вашей организации есть информация, которая нужна преступникам: интеллектуальная собственность, контактные данные или финансовая информация. Даже если преступников не интересуют именно ваши данные, с помощью атаки на вас они могут добраться до ваших партнеров или клиентов, а вы в таком случае станете промежуточным звеном в цепочке атаки.
В случае с Darkhotel такими вспомогательными звеньями для атакующих были гостиницы. Злоумышленников интересовали не отели сами по себе, а только данные их постояльцев. Которые пострадали из-за недостаточной защищенности IT-инфраструктуры гостиниц.

2 Вторым шагом является распространение адекватной информации об уязвимостях. В организациях, где большое количество сотрудников работают в приложениях на разнообразных устройствах разных платформ, может быть трудно уследить за всеми рисками и потенциальными векторами атаки, которыми могут воспользоваться злоумышленники. Атаки класса APT используют уязвимости, будь то технические недочеты или человеческие слабости. Чем крупнее и чем сложнее организация, тем больше в ней существует потенциальных точек проникновения угрозы.

3 Распространение использования личных устройств для работы и работа вне периметра корпоративной сети лишь усложняют эту проблему. Телефоны и планшеты сами по себе достаточно уязвимы и к тому же часто используются для подключения к незащищенным сетям. Хуже того, во многих случаях очень трудно определить, заражено ли устройство (особенно если оно работает с довольно «закрытой» операционной системой). Сотрудники, работающие на выезде, фактически представляют собой подвижные цели. Устройства сложно контролировать за периметром корпоративной сети, а значит, важным компонентом стратегии безопасности должна стать защита мобильных рабочих мест.

4 Огромное количество способов заражения сети, к которым прибегают киберпреступники, на фоне разнообразия типов рабочих мест означает, что точечных мер защиты совершенно недостаточно. Требуется целый комплекс мер, включая анализ угроз, соблюдение политик безопасности и применение специализированной технологии, способной не только блокировать появляющиеся угрозы, которые удалось распознать, но также выявлять новые угрозы и использованием белых списков и аналогичных приемов предотвращать выполнение еще неизвестных угроз.

5 Для снижения риска необходимо пересмотреть подход к защите рабочих мест. Киберпреступники ищут уязвимые места, а самым слабым звеном на предприятии часто является рабочее место. Его безопасность часто нарушается не только из-за недостатков самого устройства, но из-за небрежности сотрудника или недостаточной защиты сети, в которой устройство используется.
Если рабочие места не оснащены многоуровневой защитой, то вся организация подвергается риску.

ВАЖНОСТЬ СНИЖЕНИЯ РИСКОВ

Снижение рисков становится первоочередной задачей предприятия, поскольку профилактика APT-атак обходится намного дешевле, чем устранение их последствий .

Разработчики атак класса APT – это специалисты с очень хорошей подготовкой, обычно располагающие обширными ресурсами. Однако подобно всем киберпреступникам, они тоже предпочитают идти по пути наименьшего сопротивления. Поэтому, хотя безусловный иммунитет к APT-атакам гарантировать нельзя, можно принять комплекс мер, которые сильно понизят вероятность успеха таких атак.

Поскольку комплексные целевые атаки имеют многоуровневую структуру, то и эффективный ответ на них должен быть многоуровневым. Простых привычных средств безопасности будет явно недостаточно.

Как же следует подходить к защите? Австралийское управление радиотехнической обороны (Australian Signals Directorate) разработало стратегию противодействия сложным угрозам; список мер, который составляет эту стратегию, «Лаборатория Касперского» считает исчерпывающим. Мы полагаем, что эти меры вполне применимы и к безопасности предприятий и послужат отличной отправной точкой в организации защиты.

Представленные в списке меры безопасности подразделяются на четыре основные категории:

1 ПОЛИТИКИ БЕЗОПАСНОСТИ И ПРОСВЕТИТЕЛЬСКАЯ РАБОТА

IT-безопасность касается не только сферы IT. Человеческие ошибки оказывают киберпреступникам неоценимую помощь. Регулярное распространение исчерпывающей информации о проблемах безопасности, выработка правильных привычек и применение адекватных и реалистичных политик безопасности помогают уменьшить шанс проникновения киберугроз в организацию.

2 СЕТЕВАЯ БЕЗОПАСНОСТЬ

Продуманная структура сети может значительно ограничить потенциальный ущерб от заражения. Возможны различные стратегии сетевой безопасности для снижения рисков и противодействия угрозам. Например, разделение сети на сегменты помогает сократить количество рабочих мест с доступом к конфиденциальным данным, в несколько раз снижая уровень риска.

3 СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Контроль и ограничение административных прав пользователей посредством политик безопасности может значительно сократить число уязвимостей. Кроме того, большую роль могут сыграть функции безопасности, встроенные в используемые программы. Если отключить ненужные функции, то программы будут полноценно работать, но целые направления возможных атак окажутся перекрыты.

Хорошим примером устранения уязвимостей в ресурсах, используемых сотрудниками, служит отключение исполнения JavaScript в браузере.

4 СПЕЦИАЛИЗИРОВАННЫЕ РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Помимо перечисленных действий, бесценный вклад в создание защиты могут внести отдельные возможности специализированного программного обеспечения. При этом интеграция решений вовсе не обязательно сопряжена с масштабными инвестициями и обширными трудозатратами. Следующие три специализированные решения в сочетании с ограничением административных прав (см. выше стратегию системного администрирования) позволяют предотвратить 85% угроз безопасности:

- использование белых списков, контроля программ в режиме «Запрет по умолчанию»;
- регулярная установка исправлений для приложений, чаще всего подвергающихся атакам;
- регулярная установка исправлений (патчей) для операционных систем и программного обеспечения.

ОСНОВНЫЕ СТРАТЕГИИ СНИЖЕНИЯ РИСКОВ

Ряд стратегий снижения рисков должен либо уже применяться на любом предприятии, либо по крайней мере серьезно рассматриваться.

КОНТРОЛЬ ПРОГРАММ И БЕЛЫЕ СПИСКИ

Белые списки служат мощным средством противодействия комплексным целевым атакам и другому вредоносному ПО. В динамических белых списках перечисляются разрешенные приложения, которые могут запускаться на машинах пользователей. Независимо от действий пользователя контроль за выполнением приложений остается в руках администратора. Составляется белый список из известных безопасных приложений и допускается запуск приложений только из этого списка. Вредоносное ПО часто имеет вид исполняемого файла того или иного типа, и данная стратегия позволяет заблокировать подобное ПО. Этот подход противоположен черным спискам традиционных антивирусов, которые разрешают выполнение всех приложений, кроме входящих в черные списки.

Для достижения максимальной безопасности администраторы могут настроить сценарий «Запрет по умолчанию», где разрешается только выполнение приложений, предварительно утвержденных администраторами. В этом случае вероятность заражения вредоносной программой сильно уменьшается. Это эффективный способ предотвратить проникновение угроз, однако в этом случае необходимо убедиться, что не блокируются полезные программы, которые служат для повышения продуктивности работы. Более детализированный контроль программ с динамическими белыми списками дает дополнительные средства контроля. Можно блокировать или ограничивать использование программ в зависимости от категорий ПО, подразделений организации, отдельных пользователей и других факторов.

Конечно, для эффективного использования белых списков нужно знать, какие программы уже работают на ваших компьютерах. Это значит, что совершенно необходимой становится инвентаризация установленного ПО.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: КОНТРОЛЬ ПРОГРАММ С ДИНАМИЧЕСКИМИ БЕЛЫМИ СПИСКАМИ

База динамических белых списков «Лаборатории Касперского» насчитывает более миллиарда надежных приложений, в том числе 97,5% всех программ, относящихся к корпоративному сектору. Мы постоянно ведем анализ угроз, и эта база непрерывно пополняется благодаря данным, поступающим в режиме реального времени из облачной сети Kaspersky Security Network. Наш Контроль программ работает не просто по принципу «включить/выключить». Когда происходит блокирование приложения, все компоненты операционной системы продолжают работать обычным образом. Это значит, что можно останавливать атаки, не препятствуя работе пользователей. «Лаборатория Касперского» реализовала «Запрет по умолчанию», предусмотрев его запуск и в тестовом режиме с той целью, чтобы можно было заблаговременно увидеть и просчитать все трудности, сопряженные с развертыванием такого режима.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: МОНИТОРИНГ УЯЗВИМОСТЕЙ И УПРАВЛЕНИЕ УСТАНОВКОЙ ИСПРАВЛЕНИЙ

Технологии, входящие в Kaspersky Security для бизнеса, проверяют наличие уязвимостей в ПО и операционных системах по обширной базе, автоматически находят и устанавливают обновления Microsoft, а также обновления и исправления для приложений других разработчиков. Все ваши приложения и операционные системы всегда будут обновлены до последней версии, и это не потребует больших трудозатрат.

«В режиме "Запрет по умолчанию" на компьютере разрешается запускать только надежные программы. Можете мне поверить, что подавляющее большинство вредоносных программ, используемых в APT-атаках, проникает через недоверенные приложения или приложения, для которых не установлены исправления».

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

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ В ПРИЛОЖЕНИЯХ И ОПЕРАЦИОННЫХ СИСТЕМАХ

В приложениях и операционных системах есть уязвимости, которыми могут воспользоваться преступники. Важно вовремя узнавать о подобных брешах в системе безопасности и устранять их до проникновения вредоносного кода. Уязвимости в популярных приложениях чаще всего остаются неустраненными.

Средства управления установкой исправлений являются важнейшим компонентом многоуровневой системы IT-безопасности, поскольку они автоматизируют задачу обновления приложений на множестве рабочих мест. Своевременно установленные исправления закроют потенциальные пути проникновения атак.

Как мы уже говорили, от комплексных целевых атак не может быть гарантированной защиты. Однако правильная реализация всех четырех стратегий (ограничение административных прав, контроль программ, управление установкой исправлений для программ и операционных систем) может предотвратить 85% нарушений безопасности, вызванных целевыми атаками.

Выстраивание подобной эшелонированной обороны крайне затрудняет выполнение вредоносного кода или по крайней мере позволяет его обнаружить.

За 2014 год 92% случаев проникновения вредоносного ПО пришлось на долю уязвимостей в Oracle Java, популярных браузерах и Adobe Reader[2].

[2] Kaspersky Security Bulletin 2014, «Лаборатория Касперского».

ДРУГИЕ ЭФФЕКТИВНЫЕ ПОДХОДЫ

Рассмотренные выше основные стратегии обеспечивают защиту от большинства видов вторжения, но к сожалению, этого мало.

Вот ряд дополнительных приемов, усиливающих надежность вашей защиты:

ПРОТИВОДЕЙСТВИЕ ЭКСПЛОЙТАМ ДЛЯ ОПЕРАЦИОННЫХ СИСТЕМ

Стандартные технологии довольно успешно противостоят попыткам использовать уязвимости в операционных системах, однако специализированные решения способны на большее, и тому есть веская причина. Например, даже если вы постоянно устанавливаете все доступные исправления для всех приложений и операционных систем, все же сохраняется возможность атаки, использующей уязвимость «нулевого дня».
Поэтому важно иметь решение, которое не только выявляет и нейтрализует известные угрозы, но также обнаруживает отклоняющееся и подозрительное поведение программ, обеспечивая таким образом защиту от новых угроз, даже тех, с которыми еще никто не сталкивался.

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Уже известно, что комплексные целевые атаки умеют хорошо скрывать себя и долгое время могут оставаться незамеченными. Поэтому защиты периметра извне оказывается недостаточно, ведь вредоносный код уже мог проникнуть в организацию. Нужна технология, которая будет распознавать и блокировать чересчур рискованные действия программ, даже если нельзя достоверно установить, что они вредоносные.
Системы предотвращения вторжений (Host-based Intrusion Prevention System, HIPS) ограничивают активность приложений в системе в зависимости от присвоенного каждому приложению уровня доверия. Система HIPS выявляет отклонения в выполнении приложений (когда оно выполняет функции или операции, не обусловленные контекстом и позволяющие предположить угрозу). Такую проверку лучше всего проводить сразу после установки приложений (то есть до того, как их может поразить скрытая вредоносная атака).

ТЕХНОЛОГИИ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: АВТОМАТИЧЕСКАЯ ЗАЩИТА ОТ ЭКСПЛОЙТОВ (AEP)

Модуль AEP проводит ряд проверок безопасности, особое внимание уделяя программам, которые часто становятся жертвой атак, таким как Internet Explorer, Microsoft Office и Adobe Reader. Постоянно отслеживая процессы в памяти, этот модуль может выявлять подозрительные действия, характерные для эксплойтов (количество таких признаков намного меньше, чем самих эксплойтов). Такой подход позволяет модулю AEP «Лаборатории Касперского» останавливать даже эксплойты «нулевого дня»[3].

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: МОНИТОРИНГ СИСТЕМЫ И КОНТРОЛЬ АКТИВНОСТИ ПРОГРАММ

Эти два компонента позволяют отслеживать и регистрировать события, происходящие в системах на компьютере, чтобы не позволить приложениям выполнять вредоносные действия. Заметив подозрительное поведение запущенного приложения, Мониторинг системы автоматически его блокирует и производит автоматический откат вредоносных действий на основании динамического журнала операционной системы и реестра. Контроль активности программ в свою очередь регулирует (разрешает или запрещает) действия уже запущенных программ, а именно доступ к файловой системе, системному реестру и взаимодействие с другими программами, в соответствии с определенным для каждой программы уровнем доверия.

[3] По результатам независимого тестирования, проведенного MRG Effitas, только модуль AEP, при других отключенных защитных технологиях, обеспечил защиту от эксплойтов в 95% случаев.

ДИНАМИЧЕСКИЙ АНАЛИЗ ЭЛЕКТРОННОЙ ПОЧТЫ И ВЕБ-КОНТЕНТА

Как сигнатурные методы защиты не в состоянии противостоять атакам «нулевого дня», так и традиционный «статический» анализ, в котором содержимое электронной почты и веб-страниц сравнивается с базой известного вредоносного ПО, не может защитить от новых угроз.

Поэтому так важен динамический анализ. Вам необходимо решение, которое будет отслеживать подозрительные особенности в коде веб-страниц и электронной почты (например, предписание найти и изменить исполняемые файлы) и блокировать соответствующий функционал еще до открытия страницы или письма.

Атакой «нулевого дня» называется использование ранее неизвестной уязвимости в операционной системе или в приложении. Такая атака проводится до того, как становится доступным исправление уязвимости.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: ВЕБ-КОНТРОЛЬ И ВЕБ-АНТИВИРУС

Наша технология Веб-контроля позволяет разрешать и запрещать доступ пользователей как к отдельным сайтам, так и к различным типам веб-сайтов (азартные игры и др.). Мониторинг HTTP- и HTTPS-трафика позволяет открывать на рабочем месте только те веб-ресурсы, которые входят в белый список.

Тем временем наш веб-антивирус с помощью динамического анализа выявляет вредоносный код, передаваемый по протоколам HTTP/HTTPS и FTP, обеспечивая защиту от сложных угроз, которые проникают в систему через загружаемые файлы или посредством drive-by загрузки.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: ПОЧТОВЫЙ АНТИВИРУС И ЗАЩИТА ПОЧТОВЫХ СЕРВЕРОВ

Используя статический и динамический анализ в сочетании с эвристическими методами, решение Kaspersky Endpoint Security для бизнеса помогает блокировать угрозы, распространяющиеся по электронной почте. Наша технология моделирует возможное поведение вложений и может обнаруживать эксплойты во вложениях электронной почты.

Kaspersky Security для почтовых серверов с модулем DLP для защиты от утечки данных также предотвращает несанкционированное распространение важной информации. Файлы можно пометить как запрещенные к распространению, и их нельзя будет отправить за пределы компании по электронной почте.

ПОДХОД «ЛАБОРАТОРИИ КАСПЕРСКОГО»: МНОГОУРОВНЕВАЯ ЗАЩИТА

Мир угроз отличается высокой сложностью и быстро меняется. Специалисты «Лаборатории Касперского» сотрудничают с крупными организациями в рамках многоуровневой стратегии, куда входят и меры по снижению рисков, и аналитика в области безопасности.

Для нашей компании главным приоритетом является развитие технологий, и мы уже разработали инструменты, необходимые для создания всеобъемлющей стратегии борьбы с угрозами. Поскольку все инструменты созданы на основе единой кодовой базы, они легко интегрируются и позволяют реализовать комплексную стратегию безопасности, не имеющую слабых мест «на стыке».

В основе нашего решения находится собственная технология «Лаборатории Касперского» защиты от вредоносного ПО и персональный сетевой экран, удостоенные множества наград. Они блокируют **известные** угрозы, то есть 70% всех угроз. **Расширенные** средства, такие как проактивная защита, эвристический анализ, контроль программ с динамическими белыми списками и веб-контроль, обеспечивают защиту от **неизвестных** угроз. Для борьбы со **сложными** угрозами требуется другой уровень защиты, в который входят такие технологии «Лаборатории Касперского», как автоматическая защита от эксплойтов и мониторинг системы.

МЕТОДЫ АНАЛИЗА И ОБНАРУЖЕНИЯ ДЛЯ БЫСТРОГО ВЫЯВЛЕНИЯ РЕАЛЬНЫХ АТАК

Хотя детально проработанный подход к снижению рисков безусловно необходим, стратегия противодействия комплексным целевым атакам должна предусматривать технологии, которые могут быстро блокировать атаки и сводить к минимуму причиняемый бизнесу ущерб, а также обеспечивать отсутствие ложных срабатываний, которые могут создать весьма серьезные неудобства.

Рекомендуемый подход «Лаборатории Касперского» предусматривает меры обнаружения на уровне рабочих мест и уровне сети, интеллектуальную «песочницу» и подробный журнал событий.

Последнее время некоторые IT-вендоры фокусировали свое внимание на детектировании вредоносного ПО на сетевом уровне – и сегодня они предлагают специализированные решения для осуществления такого подхода. Однако мы полагаем, что альтернативное решение, в котором используется распределенная архитектура датчиков, обладает существенными преимуществами.

Размещение в ключевых точках сети датчиков, передающих данные в центральный пункт, поможет повысить уровень обнаружения.
Кроме того, такая архитектура обладает повышенной масштабируемостью и помогает снизить затраты на защиту сложных сетей корпоративного уровня.

НЕ ТОЛЬКО ТЕХНОЛОГИИ: АНАЛИЗ УГРОЗ

Принятие комплекса профилактических мер значительно снижает риски для любой организации, но никакое решение для обеспечения кибербезопасности не может гарантировать 100%-ную защиту.

Если атака окажется успешной, будет необходимо определить:

- какие именно данные были похищены - чтобы принять меры по ограничению ущерба;
- каким образом атака стала возможной - чтобы устранить уязвимости и недостатки в системе безопасности.

Поэтому важно иметь доступ к услугам квалифицированных экспертов, готовых быстро провести анализ инцидента информационной безопасности.

«Лаборатория Касперского» предлагает ряд аналитических услуг, позволяя выбрать подходящий уровень для каждой организации:

- Анализ вредоносного ПО – для клиентов с собственной группой экспертов.
- Расследование инцидентов информационной безопасности, включая анализ вредоносного ПО.
- Полный комплекс услуг реагирования на инциденты информационной безопасности, включая их расследование.

ПОЧЕМУ ИМЕННО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»?

«Лаборатория Касперского» наряду с другими организациями сражается с атаками класса APT на передовом рубеже. Наш глобальный центр исследования и анализа угроз (GReAT) участвовал в обнаружении многих из наиболее сложных и опасных угроз мирового уровня, начиная Red October и заканчивая недавно обнаруженной группировкой, занимающейся кибершпионажем и получившей название Equation.

При этом киберпреступников совершенно не смущают масштабы задач. Современное кибероружие несложно «перенацелить» на жертвы в мире бизнеса, и даже оружие, секретно разрабатываемое службами государственной безопасности, может попасть в руки преступных группировок.

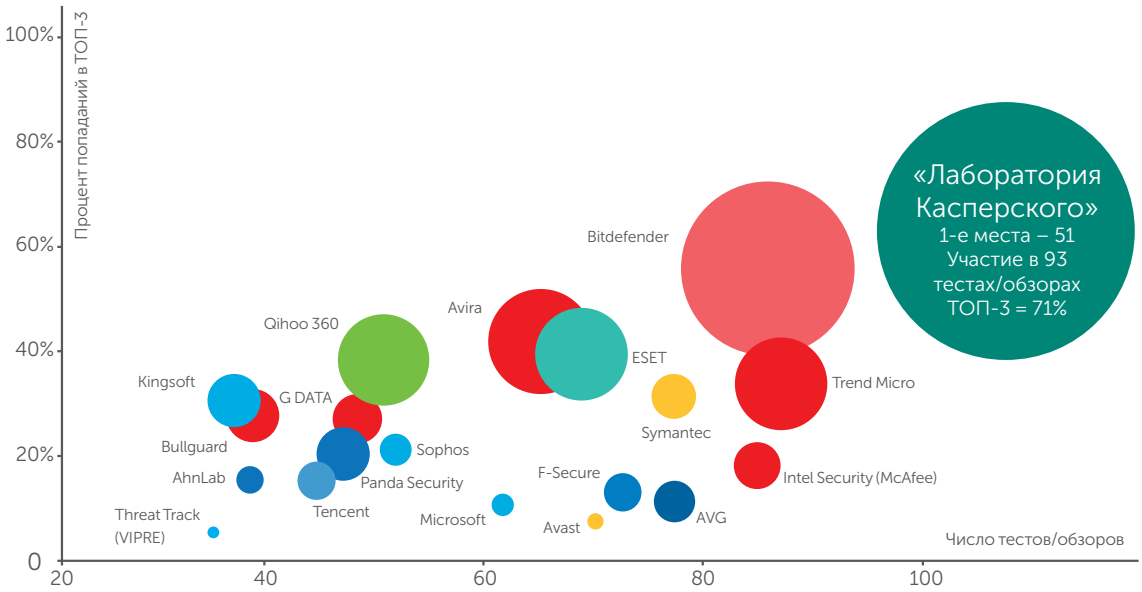
Мы хорошо понимаем это и стремимся выравнять шансы в борьбе. По итогам расследования атак класса APT мы даем правительственным организациям рекомендации по защите от кибератак, но это лишь начало. Весь наш опыт мы применяем при создании новых решений, которые будут одновременно эффективны и практичны в работе на уровне предприятия.

Для этого мы дополняем инновационными технологиями непревзойденные аналитические результаты в области безопасности. Процент сотрудников, занятых в нашей компании научно-исследовательской разработкой, значительно выше, чем у любого из конкурентов.

В результате разработан многоуровневый подход к организации корпоративной системы безопасности, который является базой для построения стратегии противодействия комплексным целевым атакам на любом предприятии.

Мы добились уровня обнаружения вредоносного ПО выше 99% и в 93 независимых тестах за 2014 год 66 раз финишировали в тройке лидеров, причем 51 раз[4] – на первом месте. Такой результат недостижим для других компаний. Кроме того, более 130 OEM-партнеров доверяют технологиям «Лаборатории Касперского» и используют их в своих продуктах. Возможно, вы уже пользуетесь нашими разработками.

«ЛАБОРАТОРИЯ КАСПЕРСКОГО» ОБЕСПЕЧИВАЕТ ЛУЧШУЮ ЗАЩИТУ*



* Примечание

Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2014 год

В обзор включены тесты, проведенные следующими независимыми организациями и изданиями: тестовые лаборатории 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

[4] Результаты ТОП-3 независимых тестов

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.

KASPERSKY lab

ЗАЩИТА СЕГОДНЯ — ШАГ В БЕЗОПАСНОЕ ЗАВТРА

Стратегические решения в сфере IT-безопасности

+7 (495) 737-34-12

sales@kaspersky.com

kaspersky.ru/corporate