Принципы прозрачности ведения бизнеса «Лаборатории Касперского»

«Мы считаем, что каждый – от пользователя домашнего компьютера до крупной компании и правительства – должен иметь возможность защитить то, что дорого для него. Неважно, идет ли речь о частной жизни, семье, финансах, бизнесе или критической инфраструктуре, мы работаем над тем, чтобы обеспечить защиту всего. И мы преуспели в этом благодаря нашему опыту и экспертным знаниям, благодаря сотрудничеству с международными организациями и правоохранительными органами, а также благодаря нашим технологиям, решениям и сервисам, которые помогают вам оставаться в безопасности несмотря на все киберугрозы».

Евгений Касперский, генеральный директор «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира. У нас 37 офисов в 32 странах. По всему миру мы защищаем более 400 миллионов пользователей и свыше 270 тысяч корпоративных клиентов, среди которых компании малого и среднего бизнеса, а также крупные правительственные и коммерческие организации. Наш бизнес строится на доверии. Надежность компании является одним из ключевых активов в глазах наших клиентов. Именно поэтому мы придерживаемся деловой этики и высочайших стандартов прозрачности бизнеса во всех сферах своей деятельности.

В этом документе изложены наши принципы прозрачности ведения бизнеса: чем мы руководствуемся и как мы работаем. Эти принципы отражают нашу позицию в борьбе с киберугрозами, во взаимодействии с правительствами и правоохранительными органами, в обработке данных и т.д.

1. Наши принципы противодействия киберугрозам

Киберугрозы стали проблемой общемирового характера. Как эксперт в области информационной безопасности «Лаборатория Касперского» видит свою задачу в обнаружении и нейтрализации всех форм вредоносных программ независимо от их происхождения и предназначения.

Одним из важнейших подразделений «Лаборатории Касперского» является глобальный центр исследований и анализа угроз, в котором работают ведущие эксперты в области кибербезопасности из России, Европы, Северной и Южной Америки, Азии и Ближнего Востока.

Мы придерживаемся в своей работе простого и открытого принципа: детектировать и устранять любую вредоносную атаку. Для нас не существует понятий «хорошего» и «плохого» вредоносного ПО. Команда наших экспертов принимала активное участие в расследовании множества атак, за организацией которых в той или иной мере стояли правительства и госорганы. За последние годы мы опубликовали ряд детальных исследований кибершпионских кампаний массового характера: Flame, Gauss, «Маска», Regin, Equation, Duqu 2.0, ProjectSauron, Sofacy (Fancy Bear), CozyDuke (Cozy Bear), Black Energy (Sand Worm). Объединив усилия с Интерполом, Европолом и властями разных стран, мы смогли раскрыть большое банковское киберограбление Carbanak. Кроме того, наши эксперты помогали расследовать атаки группировки Lurk и таким образом способствовали задержанию киберпреступников.

Мы извещаем мир обо всех угрозах, которые исследуем, вне зависимости от того, на каком языке говорят стоящие за ними люди – на русском, китайском, испанском, немецком или

английском. А о разнообразии используемых языков свидетельствует, к примеру, следующий список атак, анализ которых публиковала команда экспертов «Лаборатории Касперского»:

русский: «Красный октябрь», Cloud Atlas, MiniDuke, CosmicDuke, Epic Turla, Penquin Turla, Black Energy, Agent.BTZ, TeamSpy, Lurk, GCMAN, Metel, Carbanak, Sofacy;

английский: Regin, Equation, Duqu 2.0, ProjectSauron;

китайский: Icefog, SabPub, NetTraveler, Danti;

испанский: «Маска», El Machete;

корейский: Darkhotel, Kimsuky, Lazarus;

французский: Animal Farm;

арабский: Desert Falcons.

Однако наличие определенного языка во вредоносном коде не позволяет приписывать происхождение атаки конкретной стране. Языковые маркеры не могут считаться достаточными доказательствами, поскольку они могут быть подделаны и намеренно внедрены в код с целью пустить исследователей по ложному следу. Именно по этой причине мы не говорим, что за какой-либо атакой стоит определенная страна.

В настоящее время глобальный центр исследований и анализа угроз «Лаборатории Касперского» продолжает отслеживать активность свыше 100 кибергруппировок, стоящих за сложными атаками и вредоносными операциями, жертвами которых являются коммерческие и правительственные организации в более чем 80 странах.

2. Принципы честной разработки технологий и решений

С каждым годом IT-индустрия становится все более динамичной. Так же быстро развивается и киберпреступность. Для того чтобы эффективно противодействовать киберугрозам, компания должна реагировать даже на самые незначительные изменения в онлайн-среде и IT-индустрии. Вот почему мы инвестируем в лучших специалистов, обучение и исследования и разрабатываем новые решения, обеспечивающие передовую защиту.

«Лаборатория Касперского» уделяла повышенное внимание качеству разрабатываемых решений с самого начала своей деятельности, с тех пор, как в 1994 году Гамбургский университет признал наш продукт лучшим в мире. Мы неоднократно завоевывали первые места в многочисленных независимых тестах (проводимых в частности AV-TEST, AV-Comparatives, MRG Effitas и другими лабораториями), получали престижные международные награды, занимали верхние строчки в различных рейтингах и обзорах[i].

Технологиям «Лаборатории Касперского» доверяют более 120 партнеров по всему миру, включая такие компании, как Microsoft, Amazon Web Services, Cisco, ZyXel, Parallels, Lenovo, Facebook и Check Point.

В случае если того требует местное законодательство, продукты «Лаборатории Касперского» проходят обязательную государственную сертификацию. Кроме того, в отдельных случаях, также предусмотренных законодательством конкретной страны, программный код передается соответствующим сертификационным органам – эта проверка служит подтверждением того, что программное обеспечение «Лаборатории Касперского» соответствует законодательным

нормам и может быть использовано в государственных организациях и правительственных учреждениях.

3. Наши принципы взаимодействия с индустрией IT-безопасности

Мы уверены, что объединение усилий – это наиболее эффективный способ противодействия киберпреступникам. Мы делимся своим опытом и техническими открытиями с мировым сообществом по кибербезопасности, а также обнародуем результаты своих исследований с целью содействовать развитию совместных практик защиты от киберугроз и объединению участников сообщества на международном уровне.

«Лаборатория Касперского» исследует киберугрозы совместно с другими компаниями и организациями, в частности с Adobe, AlienVault Labs, Dell Secureworks, Crowdstrike, OpenDNS Security Research Team, GoDaddy Network Abuse Department, Seculert, SurfNET, Kyrus Tech Inc. и Honeynet Project. Мы также активно взаимодействуем с крупнейшими мировыми IT-вендорами, включая Google и Microsoft, с целью координации действий для устранения недавно обнаруженных уязвимостей в программном обеспечении.

В случае нахождения бреши в том или ином программном продукте мы передаем данные соответствующему вендору и оказываем ему дальнейшую поддержку. Вся работа в таких случаях ведется конфиденциально в соответствии с политикой неразглашения информации, что дает производителю ПО время для разработки и распространения обновлений, закрывающих обнаруженные уязвимости.

В дополнение к регулярному взаимодействию с другими участниками индустрии информационной безопасности с целью распространения сведений о новых угрозах, «Лаборатория Касперского» проводит ежегодную конференцию Security Analyst Summit, в рамках которой лучшие мировые эксперты обмениваются своими знаниями и открытиями. В списке участников присутствуют международные организации, правоохранительные органы и технологические компании. В частности, в саммитах «Лаборатории Касперского» принимали участие Adobe, Arbor, Barracuda, BlackBerry, Boeing, Google, HB Gary, Интерпол, ISEC Partners, Lockheed Martin и Microsoft.

4. Наши принципы взаимодействия с правительствами и правоохранительными органами

Как частная компания мы не имеем никаких политических связей с каким бы то ни было правительством, однако мы гордимся своим партнерством и сотрудничеством в сфере борьбы с киберпреступностью с властями разных стран и международными правоохранительными организациями. Взаимодействие такого уровня ведется в интересах международной кибербезопасности. Мы осуществляем консультации технического характера, а также проводим анализ вредоносных программ в рамках совместных расследований.

То же самое делают и другие компании, работающие в области информационной безопасности. Успешное завершение операций правоохранительных органов по расследованию киберпрестпулений без экспертных знаний, которыми обладают игроки рынка информационной безопасности, было бы несбыточной мечтой. В случае если киберпреступления носят локальный характер, IT-компании сотрудничают с внутренними

правоохранительными органами той страны, в которой произошел инцидент. Если же вредоносные атаки вышли на международный уровень, вендоры взаимодействуют с соответствующими организациями в пострадавших странах. Такое сотрудничество критически важно для противодействия киберпреступности во всем мире.

Мы работаем совместно с другими участниками мирового IT-сообщества, международными организациями, национальными и региональными правоохранительными органами. В частности, мы сотрудничаем с Интерполом, Европолом, подразделением Microsoft по борьбе с киберпреступлениями (Microsoft Digital Crimes Unit), Национальным центром по борьбе с преступлениями в сфере высоких технологий (NHTCU) полиции Нидерландов, а также с полицией Лондона и командами CERT по всему миру. В ходе совместных расследований специалисты «Лаборатории Касперского» проводят техническую экспертизу, анализируя вредоносное ПО.

В октябре 2014 года «Лаборатория Касперского» и Европол подписали меморандум, который открыл путь к более плотному сотрудничеству двух организаций. Кроме того, «Лаборатория Касперского» оказала поддержку Интерполу в открытии в Сингапуре Центра исследования компьютерных преступлений (Digital Crime Center) в составе специального подразделения IGCI (Global Complex for Innovation), занимающегося расследованием киберпреступлений. В этом центре осуществляется техническая часть расследований, проводимых Интерполом. «Лаборатория Касперского» предоставляет международной полиции свое программное обеспечение для анализа вредоносных программ, а также делится наработками в области расследования киберинцидентов.

Помимо прочего, на регулярной основе мы проводим специальные обучающие курсы для полицейских ведомств разных стран, а также для Интерпола и Европола.

5. Принципы защиты тайны частной жизни

Уважение и защита частной жизни пользователей – фундаментальный принцип, на котором строится бизнес «Лаборатории Касперского», и одна из основных задач компании. Тайна личной жизни – базовое право человека, но сегодня оно нарушается все чаще. Именно поэтому «Лаборатория Касперского» прилагает массу усилий для его защиты. Мы расследуем сложные кампании кибершпионажа и слежки, например, с использованием «легальных» инструментов вроде HackingTeam или Computrace, которые нарушают права людей. Часто наши расследования приводят к остановке подобной киберпреступной деятельности.

Помимо этого, «Лаборатория Касперского» обеспечивает конфиденциальность жизни пользователей при помощи специальных функций в своих защитных продуктах. К примеру, владельцы устройств на базе Android могут скрывать входящие звонки и SMS от определенных людей, а пользователи операционной системы Windows могут быть уверены в том, что за ними никто не следит через веб-камеру. Наконец, люди могут окончательно удалять документы при помощи средства уничтожения файлов, а также стирать следы своей активности на устройстве, включая историю в браузере, открытые документы и т.д., при помощи функции защиты приватности.

Миллионы людей по всему миру доверяют «Лаборатории Касперского» защиту своих цифровых ценностей, в том числе и личные данные. Мы относимся к этому очень серьезно, вот почему наши продукты и технологии не обрабатывают личную информацию. Решения «Лаборатории

Касперского» получают лишь обезличенные данные об угрозах с тех устройств, владельцы которых согласились передавать информацию в облачную инфраструктуру Kaspersky Security Network. Обработка такого рода данных помогает быстрее и точнее распознавать новые и еще неизвестные угрозы. Схожие технологии используют и другие производители защитных решений.

Участники Kaspersky Security Network (KSN) не отправляют никаких данных, которые могли бы считаться персональными в соответствии с законодательством большинства стран. «Лаборатория Касперского» не определяет и не следит за передвижениями конкретного человека и не имеет намерений делать это. Правоохранительные органы тех стран, в которых работает компания, могут запрашивать информацию для проведения расследования, однако в силу своей анонимности данные из KSN не могут им в этом помочь.

Более того, как социально ответственная компания «Лаборатория Касперского» всецело осознает, что антивирусное решение, будучи базовой мерой киберзащиты, в некоторых случаях не может обеспечить должный уровень конфиденциальности. В связи с этим компания информирует пользователей о новейших технологиях защиты приватности, имеющихся в Интернете.

Что клиенты и партнеры говорят о «Лаборатории Касперского»

Витторио Боэро (Vittorio Boero), IT-директор Ferrari:

«Для защиты нашей основной ценности – интеллектуальной собственности – мы нуждались в надежном технологическом партнере, способном предложить комплексное, передовое защитное решение. И в качестве такого партнера мы выбрали «Лабораторию Касперского». Способность компании противодействовать киберугрозам, которые еще не были обнаружены другими вендорами, и гибкость ее решений, позволяющая настраивать систему защиты в соответствии с индивидуальными потребностями Ferrari, служат залогом инновационного партнерства в будущем».

Джо Салливан (Joe Sullivan), бывший директор по безопасности Facebook:

«Будучи инновационной компанией мы разделяем общие ценности с «Лабораторией Касперского». Этот вендор – лидер в своей индустрии. Компания постоянно следит за глобальными тенденциями в сфере информационных угроз, разрабатывает надежную защиту и предоставляет нам самую свежую информацию об актуальных опасностях».

Нобору Нактани (Noboru Nakatani), исполнительный директор Глобального комплекса инноваций Интерпола (Global Complex for Innovation):

«Интерпол сотрудничает с «Лабораторией Касперского» в сфере информационной безопасности с апреля 2013 года, и в течение всего этого времени наше взаимодействие было очень плодотворным. Компания оказала нам содействие в запуске Глобального комплекса инноваций (IGCI) в Сингапуре и организовала обучающие курсы для наших сотрудников. Помимо этого, компания предоставляет Интерполу свои результаты исследований киберугроз, а также принимает участие в расследовании ряда компьютерных инцидентов. Я убежден, что

«Лаборатория Касперского» внесла значимый вклад в обеспечение информационной безопасности на международном уровне. Своими действиями компания демонстрирует свое желание сделать цифровой мир безопасным пространством без ущерба для его открытости».

Рональд Ноубл (Ronald Noble), бывший генеральный секретарь Интерпола:

«Сложные и постоянно эволюционирующие киберугрозы требуют высокого уровня технической подготовки, знаний и опыта. Поэтому для эффективного противодействия киберпреступности правоохранительным органам крайне важно заручиться поддержкой специалистов из разных секторов. Соглашение между Интерполом и «Лабораторией Касперского» – серьезный шаг в сторону глобального объединения усилий в борьбе с киберпреступностью и достижения уверенности в том, что мы предлагаем нашим странам-участницам самые современные средства обеспечения безопасности».

Эдриан Леппард (Adrian Leppard), комиссар полиции Лондона:

«Полиция Лондона – национальное полицейское подразделение Великобритании по борьбе с мошенничеством и экономическими преступлениями – сотрудничает с лидером в индустрии IT-безопасности «Лабораторией Касперского», пользуясь ее учебными программами и сервисами по расследованию киберинцидентов, для того чтобы добиться снижения уровня киберпреступности и онлайн-угроз».

Римма Перельмутер (Rimma Perelmuter), генеральный директор MEF:

«Лидерство «Лаборатории Касперского» в вопросах информационной безопасности в сочетании с глубоким пониманием угроз для мобильных устройств делает эту компанию надежным партнером для всех, кто работает в столь динамичной сфере, как защита от мобильных угроз».

Источники:

---

[i] Компания заняла четвертое место в рейтинге IDC ‘Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind Vendors’ report (IDC # US41867116, 2015 - Nov 2016)

Gartner, Magic Quadrant for Endpoint Protection Platforms, 30 January 2017. Данные, публикуемые компанией Gartner, не являются рекомендацией в отношении каких бы то ни было производителей, продуктов или услуг и не могут рассматриваться в качестве совета выбирать поставщиков с наибольшим рейтингом. Аналитические публикации Gartner основаны на мнениях экспертов компании и не могут считаться констатацией фактов. Gartner не дает никаких гарантий, выраженных в явной или подразумеваемой форме, в отношении публикуемых данных, в том числе гарантий коммерческого качества или пригодности для определенных целей.

Суммарные результаты независимых тестирований продуктов для корпоративных и домашних пользователей, а также для мобильных устройств за 2016 год. Результаты включают в себя независимые тесты, проведенные лабораториями AV-Comparatives, AV-TEST, SELabs, MRG Effitas, VirusBulletin, ICSA Labs.