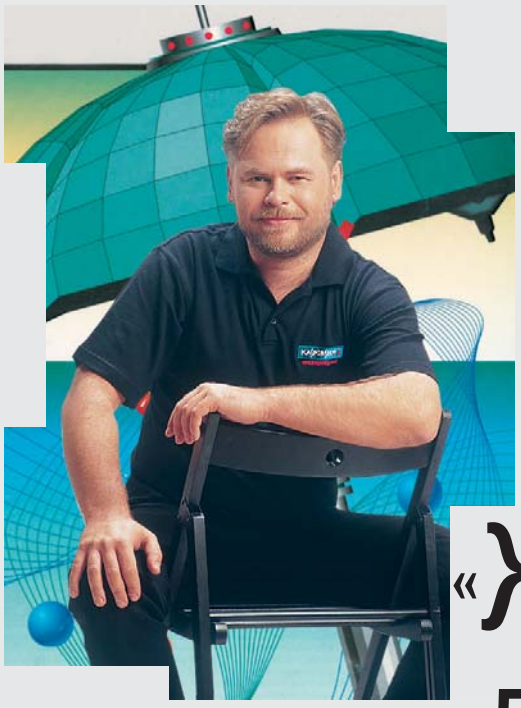

Евгений Касперский,
руководитель и основатель
«Лаборатории Касперского»:

«Жизнь длинная — цели большие»

За спинами у специалистов «Лаборатории Касперского» не один год напряженной работы и исследований. Я решил не упускать возможности получить ответы на интересующие меня вопросы из первых рук и договорился о встрече с Евгением Касперским — руководителем антивирусных исследований компании.

Евгений, как физически происходит излечение зараженных файлов, и в каких случаях оно невозможно?
Обнаружение вируса происходит несколькими методами. Первый и самый простой из них — последовательная проверка всего жесткого диска компьютера. Другой способ — это проверка всех используемых файлов резидентным монитором. Последняя версия «Антивируса Касперского» при старте компьютера также проверяет ключи автозапуска реестра и определяет файлы, в которых могут содержаться вирусы.

У простейших вирусов есть «маска» — последовательность данных, которая, собственно, и является вирусом. Для восстановления файла мы находим в нем эту маску и извлекаем ее, одновременно восстанавливая нарушенные связи между частями зараженной программы. Бывают и сложные случаи. Например, существуют так называемые полиморфные вирусы, их тело в каждом зараженном файле шифруется уникальным алгоритмом и выглядит по-разному. Для борьбы с такими вирусами применяются более сложные приемы.

Нам приходится бороться с несколькими разновидностями вредоносных программ. В последнее время широкое распространение получили трояны и черви, которые с технологической точки зрения вирусами не являются. То есть вредоносной программой от первого до последнего байта является сам файл. Таким образом, для излечения компьютера достаточно просто удалить этот файл. Функция антивируса в данном случае заключается в том, чтобы указать на него.

В случае с вирусами ситуация менее однозначна. Если вирус грамотно написан, и не портит файлы при заражении, к примеру, как печально известный «Чернобыль», то файлы лечатся просто изумительно. Ког- »

да вирус написан криво, изымая его, мы не можем гарантировать того, что файл будет впоследствии работоспособен. И поэтому в некоторых случаях мы отказываемся от лечения таких файлов, а пользователю проще будет воспользоваться резервной копией.

Часто пользователи пренебрегают антивирусной защитой, и в последнее время все чаще к нам попадают файлы, содержащие сразу несколько вирусов. В таких случаях мы не гарантируем, что нам удастся угадать их последовательность, так как не всегда очевидно, который из них следует лечить первым.

А по какому куску кода вирус идентифицируется антивирусом?

По подходящему. Многие антивирусы грешат ложными срабатываниями, когда маска выбрана неправильно. У меня даже есть коллекция ложных срабатываний различных антивирусов. Panda, к примеру, ругалась на русифицированный Windows.

Я считаю, что корректнее на полдня отложить обновление антивирусных баз, чем ошибочно «вылечить» чистое ПО. Это чревато потерями более серьезными, чем может нанести сам вирус: пользователь начинает нервничать и способен причинить компьютеру даже больший вред. У нас обновления тестируются на ложные срабатывания на нескольких сотнях гигабайт наиболее распространенного ПО. Там есть все: различные операционные системы, базы данных, прикладные программы…

Почему же Ваш антивирус ругался на Panda?

До сих пор ругается, и будет ругаться. Просто у них в коде зашит кусок трояна. У нас с ними уже был разговор по этому поводу; но что нам остается делать, если в программе присутствует строка «format c: /q /autotest…» В данном случае, конечно, этот вирус не попадет в систему, но держать внутри программы код трояна целиком и в нешифрованном виде — это безобразие.

А возможно ли создать ОС, которая вообще не будет подвержена заражению?

Да, такую операционную систему разработать можно, но с ней никто не будет работать.

В каком смысле?

Для того чтобы закрыть операционную систему от вирусов, необходим жесткий контроль за тем, что в ней происходит, и она должна иметь «разрешительные» правила работы, в ней все должно быть запрещено. Новую программу придется ставить, вручную преодолевая многочисленные точки контроля. Выход в Интернет — исключительно в текстовом режиме.

Однако даже если сеть защищена грамотно стандартными средствами, поместить в нее шпиона очень сложно и дорого. Гораздо дешевле сыграть на человеческом факторе, и какая-нибудь новенькая секретарша-блондинка может учудить такое, что все потом будут бегать с выпученными глазами.

Какие компании на сегодняшний день являются лидерами в области вирусологии?

В мире сейчас около 20 более-менее заметных антивирусных компании (в России их всего две: мы и «Диалог-Наука»), и их условно можно разделить на 3 категории. Лидерами на рынке являются американцы McAfee и Symantec и китайская Trend Micro. Следом идут Computer Associates, Command Software; в Европе это Sophos, F-Secure, Norman. Мелкие антивирусы — H+BEDV (Германия), VirusBuster (Венгрия), AVG (Чехия), RAV (Румыния). Мы перекочевали из локальных, в мировом масштабе, компаний в середнячки где-то год-два назад. В остальном жизнь длинная — цели большие.

А что на сегодняшний день было бы целесообразно привнести в законодательную базу?

Менять нужно не следствие, менять нужно причину. Кардинальная перестройка сети Интернет смогла бы снизить количество компьютерных преступлений (я имею в виду написание вирусов и их распространение и т. п.) в десятки раз. Нужно уходить от того бардака стандартов, который сейчас имеет место. Я считаю, что в будущем должны существовать строгие правила входа в Сеть, то есть оказавшийся в ней должен предъявлять свой ID, и на всем, что пользователь делает, должна стоять его подпись.

Что бы Вы сказали вирусописателям?

Я бы им порекомендовал поскорее взрослеть и начинать заниматься чем-нибудь более полезным.

Беседовал Дмитрий Асауленко

Вирусы для мобильников

Количество разновидностей вредоносных программ на сегодняшний день огромно, а численность вирусных инцидентов растет в последние годы в геометрической прогрессии. Я посчитал своим долгом выяснить, что же ждет пользователей в ближайшем будущем.

Евгений, как Вы думаете, появятся ли в ближайшем будущем новые типы вирусов?

Программы для современных ОС стали настолько сложными, что они сами стали операционными системами. Пример — Microsoft Office для макросов, которые там работают. Очень многие приложения сегодня поддерживают жизнь внутри себя, естественно, могут появиться и паразиты. Поэтому типов вирусов, которые могут появиться, очень много.

Проясните, пожалуйста, ситуацию с вирусами для мобильных телефонов…

Да, они будут существовать!

А для каких моделей?

Кому больше повезет: для самых популярных и незащищенных.

Для того чтобы существовали вирусы, от среды требуются три вещи. Первое — она должна быть очень популярной среди пользователей. Второе — среда должна быть документирована. Третье — среда должна быть незащищенной (в данном случае разграничение прав доступа защитой не является).

Мобильников много везде. Скоро для них появятся программы, сегодня уже выпущено несколько утилит для их разработки. Следующий шаг — программы для мобильных телефонов начнут писать все, включая школьников. Что они будут писать — очевидно.

Если компании-производители мобильных телефонов не будут уделять защите должного внимания, если программа, написанная не ими, сможет получить доступ, скажем, к адресной книге мобильного телефона… Ждем. Мы к этому готовы.

Кстати, та же судьба ждет системы «интеллектуальный дом». Если эти системы станут популярными, то вашим домом через некоторое время смогут управлять совершенно посторонние люди.

да вирус написан криво, изымая его, мы не можем гарантировать того, что файл будет впоследствии работоспособен. И поэтому в некоторых случаях мы отказываемся от лечения таких файлов, а пользователю проще будет воспользоваться резервной копией.

Часто пользователи пренебрегают антивирусной защитой, и в последнее время все чаще к нам попадают файлы, содержащие сразу несколько вирусов. В таких случаях мы не гарантируем, что нам удастся угадать их последовательность, так как не всегда очевидно, который из них следует лечить первым.

А по какому куску кода вирус идентифицируется антивирусом?

По подходящему. Многие антивирусы грешат ложными срабатываниями, когда маска выбрана неправильно. У меня даже есть коллекция ложных срабатываний различных антивирусов. Panda, к примеру, ругалась на русифицированный Windows.

Я считаю, что корректнее на полдня отложить обновление антивирусных баз, чем ошибочно «вылечить» чистое ПО. Это чревато потерями более серьезными, чем может нанести сам вирус: пользователь начинает нервничать и способен причинить компьютеру даже больший вред. У нас обновления тестируются на ложные срабатывания на нескольких сотнях гигабайт наиболее распространенного ПО. Там есть все: различные операционные системы, базы данных, прикладные программы…

Почему же Ваш антивирус ругался на Panda?

До сих пор ругается, и будет ругаться. Просто у них в коде зашит кусок трояна. У нас с ними уже был разговор по этому поводу; но что нам остается делать, если в программе присутствует строка «format c: /q /autotest…» В данном случае, конечно, этот вирус не попадет в систему, но держать внутри программы код трояна целиком и в нешифрованном виде — это безобразие.

А возможно ли создать ОС, которая вообще не будет подвержена заражению?

Да, такую операционную систему разработать можно, но с ней никто не будет работать.

В каком смысле?

Для того чтобы закрыть операционную систему от вирусов, необходим жесткий контроль за тем, что в ней происходит, и она должна иметь «разрешительные» правила работы, в ней все должно быть запрещено. Новую программу придется ставить, вручную преодолевая многочисленные точки контроля. Выход в Интернет — исключительно в текстовом режиме.

Однако даже если сеть защищена грамотно стандартными средствами, поместить в нее шпиона очень сложно и дорого. Гораздо дешевле сыграть на человеческом факторе, и какая-нибудь новенькая секретарша-блондинка может учудить такое, что все потом будут бегать с выпученными глазами.

Какие компании на сегодняшний день являются лидерами в области вирусологии?

В мире сейчас около 20 более-менее заметных антивирусных компании (в России их всего две: мы и «Диалог-Наука»), и их условно можно разделить на 3 категории. Лидерами на рынке являются американцы McAfee и Symantec и китайская Trend Micro. Следом идут Computer Associates, Command Software; в Европе это Sophos, F-Secure, Norman. Мелкие антивирусы — H+BEDV (Германия), VirusBuster (Венгрия), AVG (Чехия), RAV (Румыния). Мы перекочевали из локальных, в мировом масштабе, компаний в середнячки где-то год-два назад. В остальном жизнь длинная — цели большие.

А что на сегодняшний день было бы целесообразно привнести в законодательную базу?

Менять нужно не следствие, менять нужно причину. Кардинальная перестройка сети Интернет смогла бы снизить количество компьютерных преступлений (я имею в виду написание вирусов и их распространение и т. п.) в десятки раз. Нужно уходить от того бардака стандартов, который сейчас имеет место. Я считаю, что в будущем должны существовать строгие правила входа в Сеть, то есть оказавшийся в ней должен предъявлять свой ID, и на всем, что пользователь делает, должна стоять его подпись.

Что бы Вы сказали вирусописателям?

Я бы им порекомендовал поскорее взрослеть и начинать заниматься чем-нибудь более полезным.

Беседовал Дмитрий Асауленко

Вирусы для мобильников

Количество разновидностей вредоносных программ на сегодняшний день огромно, а численность вирусных инцидентов растет в последние годы в геометрической прогрессии. Я посчитал своим долгом выяснить, что же ждет пользователей в ближайшем будущем.

Евгений, как Вы думаете, появятся ли в ближайшем будущем новые типы вирусов?

Программы для современных ОС стали настолько сложными, что они сами стали операционными системами. Пример — Microsoft Office для макросов, которые там работают. Очень многие приложения сегодня поддерживают жизнь внутри себя, естественно, могут появиться и паразиты. Поэтому типов вирусов, которые могут появиться, очень много.

Проясните, пожалуйста, ситуацию с вирусами для мобильных телефонов…

Да, они будут существовать!

А для каких моделей?

Кому больше повезет: для самых популярных и незащищенных.

Для того чтобы существовали вирусы, от среды требуются три вещи. Первое — она должна быть очень популярной среди пользователей. Второе — среда должна быть документирована. Третье — среда должна быть незащищенной (в данном случае разграничение прав доступа защитой не является).

Мобильников много везде. Скоро для них появятся программы, сегодня уже выпущено несколько утилит для их разработки. Следующий шаг — программы для мобильных телефонов начнут писать все, включая школьников. Что они будут писать — очевидно.

Если компании-производители мобильных телефонов не будут уделять защите должного внимания, если программа, написанная не ими, сможет получить доступ, скажем, к адресной книге мобильного телефона… Ждем. Мы к этому готовы.

Кстати, та же судьба ждет системы «интеллектуальный дом». Если эти системы станут популярными, то вашим домом через некоторое время смогут управлять совершенно посторонние люди.