IDC
Analyze the Future

WHITE PAPER

Понимание рисков, связанных с использованием нелегального ПО домашними пользователями

При поддержке Microsoft

Сентябрь 2010

РЕЗЮМЕ

В последние годы достигнут существенный прогресс в ограничении использования нелицензионного программного обеспечения (ПО) предприятиями и организациями. При этом большинство корпоративных пользователей осознают не только юридические риски, связанные с использованием нелицензионного ПО, но и в определенной степени осведомлены об экономических и технологических факторах риска и дополнительных затратах, возникающих при использовании нелицензионного ПО.

Несколько иная ситуация характерна для сегмента домашних пользователей. Ежегодные исследования IDC свидетельствуют о том, что, хотя уровень компьютерного пиратства в России из года в год неуклонно снижается, он все еще значительно выше среднемирового. Согласно данным IDC, в 2009 году уровень компьютерного пиратства в России составил 67%, против 43% в среднем по миру. При этом необходимо понимать, что это средние цифры и что уровень пиратства сильно варьируется в разных сегментах пользователей: в крупном бизнесе он значительно ниже среднего, а в домашнем сегменте, наоборот, выше. Это справедливо и для разных категорий ПО. Для каких-то видов программных продуктов уровень пиратства снижается медленнее, для каких-то быстрее. Например, компания Microsoft за последние годы добилась очень больших успехов в деле снижения уровня пиратства для своей операционной системы Windows. Однако, поскольку эта ОС устанавливается на подавляющее большинство персональных компьютеров в стране, в абсолютных величинах, т.е. по числу установленных копий, уровень пиратства для Windows, в особенности в домашнем сегменте, остается чрезвычайно высоким. Это создает очень благоприятную среду не только для распространителей нелицензионного ПО, ведь чем более популярна программа, пиратская копия которой распространяется, тем больше потенциальная аудитория зараженных вредоносным ПО. В итоге, Windows становится наиболее привлекательной мишенью для преступников, которым зачастую даже нет необходимости использовать уязвимости в пиратских версиях для заражения их через интернет, когда можно встроить вредоносный код сразу в нелегальную копию до того, как она попадет к пользователю.

Все большее проникновение персональных компьютеров в нашу жизнь приводит к тому, что растет и серьезность рисков, связанных с их использованием. Достаточно сказать, что, по данным МВД РФ, число мошенничеств с использованием интернет-технологий в 2009 году возросло на 30%, а размер украденных сумм увеличился в три раза.

IDC Moscow, Timiryazevskaya Street 1, Building 5, Moscow 127422 www.idc.com/russia

Данное исследование было инициировано российским представительством Microsoft в связи с острой необходимостью понимания и разъяснения домашним пользователям тех рисков, с которыми сопряжено нелицензионное использование программных продуктов. При этом исследование сфокусировано на двух основных вопросах:

- Какие риски сопутствуют использованию нелицензионного ПО?
- Какой ущерб наносит домашнему пользователю использование нелицензионного ПО?

Исследование IDC позволяет выделить семь ключевых рисков для домашнего пользователя ПК, связанных с использованием нелицензионного ПО:

1. Потеря важных данных из-за нестабильности системы
2. Несанкционированный доступ к логину и паролям пользователя систем онлайн-банкинга или к данным кредитных карт
3. Использование чужого ПК в качестве шлюза для рассылки нелицензионного контента или проведения хакерских атак
4. Использование персонального компьютера жертвы в качестве шлюза для рассылки нелегального контента
5. Кража чужих идентификационных данных в социальных сетях или других персонализированных системах с целью совершения незаконных операций от имени жертв кражи
6. Похищение конфиденциальных данных с последующей их публикацией на общедоступных вебсайтах
7. Похищение конфиденциальных документов, связанных с работой жертвы, которые зачастую хранятся на домашнем ПК

Только прямой финансовый ущерб от использования нелицензионного ПО может составлять несколько тысяч рублей, т.е. многократно превосходить стоимость легальных копий ПО для домашнего пользователя, не говоря уже о проблемах, связанных с вероятной потерей репутации или уголовным преследованием.

Потеря важных данных из-за нестабильности системы

Ущерб: затраты на восстановление данных на жестком диске, потеря невосстановимых данных

Результаты опросов, проводимых IDC, свидетельствуют о том, что пользователи нелицензионного программного обеспечения сталкиваются со сбоями своих компьютеров значительно чаще, чем пользователи легального ПО. Тому можно найти несколько объяснений:

- Нелицензионное ПО нередко не дает пользователю возможности своевременно получать обновления, направленные на исправления ошибок в коде, ведущих к сбоям.

- Отсутствие лицензии также может служить препятствием к скачиванию обновлений, направленных на устранение уязвимостей ПО, что, в конечном итоге, также часто ведет к сбоям систем.

- Само по себе вмешательство в код программных продуктов распространителями пиратского ПО может служить причиной некорректной или нестабильной работы этого ПО.

- Использование нелегального ПО часто ведет к созданию на домашнем ПК "зоопарка" продуктов, многие из которых практически не используются, но засоряют систему, снижая ее стабильность и производительность.

- Наконец, очень часто Web-сайты, через которые распространяется пиратское ПО, а также диски, на которых оно распространяется, содержат троянов и другой вредоносный код, который устанавливается на компьютер пользователя вместе с новыми нелицензионными программными продуктами.

Все это так или иначе значительно снижает надежность системы, что, помимо серьезных неудобств, связанных с недоступностью данных, практически всегда выливается во вполне ощутимые потери для пользователя домашнего ПК:

- Большинство пользователей ПК не обладают знаниями и опытом, достаточными для восстановления системы, и вынуждены обращаться в фирмы либо к частным специалистам, оказывающим подобные услуги. Стоимость этих услуг может варьироваться от 1 500 рублей за простую переустановку системы и основных приложений до нескольких тысяч за восстановление информации на жестком диске.

- Даже если пользователь обладает достаточной квалификацией для самостоятельного восстановления системы, восстановление системы и данных – это достаточно длительный процесс, занимающий не один час времени, которое можно было бы потратить на что-то более полезное.

- Наконец, нередки случаи, когда в результате сбоя системы данные теряются частично или полностью и не подлежат восстановлению, ведь мало кто из домашних пользователей делает резервные копии личных архивов, содержащих семейные фотографии, документы и другие личные данные.

В любом случае, важно понимать, что затраты на восстановление системы либо сопоставимы, либо даже многократно превосходят стоимость основного лицензионного ПО для домашнего пользователя. Безвозвратная же утрата личного архива для многих может оказаться вообще несравнимой с затратами на легальное ПО.

Несанкционированный доступ к логину и паролям пользователя систем онлайн-банкинга или к данным кредитных карт

Ущерб: кража денег со счета жертвы

По данным МВД РФ, число мошенничеств с использованием интернет-технологий в 2009 году возросло на 30%. Размер украденных сумм увеличился в три раза, то есть каждое мошенничество стало в несколько раз эффективнее. Число привлеченных к уголовной ответственности по этим случаям, к сожалению, в процентном соотношении к количеству мошенничеств продолжает падать, так как профессиональные преступники изобретают все новые способы ухода от ответственности.

К сожалению, невозможно создать идеальный во всех отношениях продукт. Производители ПО постоянно совершенствуют пользовательские интерфейсы, расширяют функционал, что неизбежно приводит к появлению все новых уязвимостей в казалось бы уже отлаженных продуктах, и на их обнаружение и устранение уходит время. Естественно, угрозам, связанным с наличием уязвимостей в приложениях, подвержены как пользователи нелицензионных программных продуктов, так и обладатели лицензий. Однако пользователи пиратского ПО как правило не имеют возможности оперативно скачивать обновления программ, выпускаемые их производителями для устранения этих уязвимостей, что критически важно в наше время, когда между обнаружением новой уязвимости и появлением вируса, использующего ее, проходит меньше одного дня.

Проникнув на домашний компьютер пользователя через имеющиеся в его пиратском ПО "дыры", вредоносное ПО может оставаться на нем сколь угодно долго, ничем не выдавая своего присутствия. Сегодняшние вирусописатели очень редко создают свои программы для нанесения заметного вреда компьютерам своих жертв. Их основная задача – сбор конфиденциальной информации с зараженных компьютеров, поэтому вредоносные программы тщательно маскируются на компьютерах пользователей, постоянно передавая своим создателям информацию о логинах и паролях, номерах кредитных карт и другие персональные данные. Пользователь может находиться в неведении о том, что с его компьютером что-то не так до тех самых пор, пока с его банковского счета не пропадут деньги, и отнюдь не факт, что жертва киберпреступников сможет доказать банку свою непричастность к исчезновению и вернуть деньги.

Использование чужого ПК в качестве шлюза для рассылки нелицензионного контента или проведения хакерских атак

Ущерб: дополнительные затраты на "чужой" интернет-трафик.

Целью киберпреступников может быть не только кража персональных данных жертв, но и использование их компьютеров для создания ботнетов, т.е. сетей, состоящих из большого числа зараженных компьютеров и используемых для совершения противоправных действий, таких как:

- *Рассылка пиратского ПО.* Правообладатели и правоохранительные органы, конечно, стараются выявлять и закрывать Web-сайты, содержащие нелицензионное ПО, музыку и фильмы, а распространители пиратских продуктов стараются затруднить им эту задачу, используя вместо физических серверов распределенные сети зараженных компьютеров.

- *Рассылка спама,* т.е. массовая рассылка коммерческой и иной рекламы лицам, не выражавшим желания ее получать. Поскольку в большинстве случаев такая рассылка является незаконной, то, как и в случае с рассылкой пиратского ПО, для спама используются распределенные сети зараженных компьютеров.

- Проведение хакерских атак. Ботнеты могут также использоваться для осуществления атак на компьютерные системы, вызывающих отказ в обслуживании. В ходе такой атаки компьютеры, входящие в ботнет, начинают одновременно обращаться к атакуемой системе, что ведет к превышению ее допустимой нагрузки. Целью такой атаки может быть как вывод из строя атакуемой системы, так и последующее проникновение в нее.

Во всех случаях речь идет о генерировании большого объема исходящего трафика с компьютера пользователя, что ведет как минимум к заметному снижению производительности интернет-канала, иными словами скорости работы пользователя в интернете, а нередко и к увеличению ежемесячных счетов от интернет-провайдера. И, естественно, как говорилось выше, наиболее подвержены этому риску пользователи нелицензионного ПО, чья экономия на покупке лицензий может в итоге обходиться им довольно дорого.

Использование персонального компьютера жертвы в качестве шлюза для рассылки нелегального контента

Ущерб: возможное уголовное преследование, потеря репутации

Владельцы ботнета могут использовать его не только для рассылки спама или распространения нелицензионного ПО, но и для рассылки другого нелегального контента, само нахождение которого на компьютере пользователя может иметь очень неприятные последствия, в том числе и правовые.

Речь идет, в первую очередь, о порнографии. Это могут быть фильмы, фотографии, все, что угодно. Помимо того, что, как и любой другой контент, несанкционированно рассылаемый с зараженного компьютера, он увеличивает объем исходящего трафика, его наличие на компьютере может иметь неприятные последствия для репутации жертвы, а иногда стать причиной уголовного преследования. В отличие от пиратского ПО, которое хранится на зараженном компьютере в виде набора непонятных для неспециалиста файлов, фото и видео файлы может открыть и посмотреть даже ребенок. Кому хочется, чтобы ваш ребенок случайно наткнулся на "веселые картинки" на родительском компьютере? Или таможенник, попросив вас включить компьютер, увидел, чем вы "увлекаетесь". При этом необходимо помнить, что во многих странах хранение некоторых или даже всех видов порнографии является уголовно наказуемым.

Нелегальный контент может попадать на компьютер жертвы разными путями. Он может быть скопирован вместе с нелицензионным ПО с компакт-диска или с сайта, через который распространяются пиратские программные продукты, или может быть скачан из интернета с помощью вредоносного кода, который либо изначально содержался в пиратской версии ПО, либо попал туда через уязвимости из интернета.

Кража чужих идентификационных данных в социальных сетях или других персонализированных системах с целью совершения незаконных операций от имени жертв кражи

Ущерб: потеря репутации

Постоянно появляющиеся в СМИ сообщения о новых способах мошенничества играют важную роль в повышении осведомленности пользователей. Преступникам становится все труднее находить своих жертв, рассылая обезличенные сообщения и надеясь на наивность их получателей. Другое дело, если пользователь получает сообщение, адресованное лично ему: даже у опытного пользователя не сразу возникнут подозрения в обмане, а если сообщение еще и отправлено от имени хорошо знакомого ему человека, то шансы быть обманутым возрастают многократно.

В этой ситуации для вирусописателей начинает представлять интерес не только информация финансового характера, хранящаяся на компьютере их жертв, но и любые логины и пароли к их почтовым ящикам и учетным записям в социальных сетях, т.е. то, что может быть использовано для создания персонализированных сообщений.

Казалось бы, что в этом такого? Ведь пользователь, у которого украли его идентификационные данные, как правило, не несет финансовых потерь. Это не совсем так. Зачастую вместе с доступом к учетным записям злоумышленники получают доступ и к списку всех контактов пользователя и уже пытаются их обмануть от его имени. И тут уже возникает большой вопрос, что опаснее, прямой финансовый ущерб или потеря репутации среди хорошо знакомых тебе людей? И стоила ли экономия полутора тысяч рублей на покупке лицензионной версии ОС потери репутации?

Похищение конфиденциальных данных с последующей их публикацией на общедоступных вебсайтах

Ущерб: потеря репутации, финансовые потери

Получив доступ к персональным идентификационным данным пользователям, преступники могут использовать их не только для того, чтобы войти в доверие к знакомым своей жертвы, но и для ее шантажа. Наиболее очевидный способ – это размещение на публичных сайтах персональной информации жертвы (личных фотографий, писем и т.д.) с требованием платы за ее удаление. При

этом не надо думать, что такой угрозы следует опасаться только известным людям, а публикация личной информации рядового пользователя пройдет незамеченной. Имея доступ к списку контактов жертвы, злоумышленники могут обеспечить доступ к публикуемой информации всем тем, чьим мнением жертва особенно дорожит.

Недавно была обнаружена новая разновидность мошенничества, связанного с вымогательством. Например, троян Kenzero внедрялся на компьютеры посетителей популярного файлообменника Winni, после чего размещал на общедоступном сайте истории их Web-серфинга и предлагал своим жертвам заплатить определенную сумму за удаления этой информации из открытого доступа. Понятно, что даже в случае удаления компрометирующей информации из открытого доступа после получения денег от жертвы, т.е. причинения финансового ущерба, никто не может гарантировать сохранение репутации пользователя, так как даже за небольшое время информация могла попасть третьим лицам и могла быть скопирована.

Похищение конфиденциальных документов, связанных с работой жертвы, которые зачастую хранятся на домашнем ПК

Ущерб: риск потерять работу

Опросы, проводимые IDC среди руководителей ИТ-отделов компаний, свидетельствуют о том, что одной из основных их проблем, связанных с защитой корпоративной информации, является человеческий фактор. Действительно, при наличии достаточных средств можно создать практически "непробиваемую" систему защиты от вирусов, хакерских атак и других внешних угроз, но на порядок сложнее контролировать поведение сотрудников компании. Причем случаи умышленной кражи информации у работодателя – это не такое уж частое явление. Основная доля утечек – это небрежное обращение с информацией.

Статистика свидетельствует, что около половины пользователей домашних ПК хранят на них те или иные данные, относящиеся к работе. Кто-то брал работу на дом и потом не удалил ненужные файлы, кто-то намеренно скопировал информацию "на всякий случай". Факт остается фактом: помимо личных данных пользователь подвергает риску данные, относящиеся к его работе и нередко носящие конфиденциальный характер.

Излишне говорить, к каким негативным последствиям может привести их утечка. Для компании это может означать финансовые потери или потерю репутации, для ее сотрудника – как минимум риск потерять работу, а возможно и правовые последствия, если выяснится, что он не имел прав доступа к этой информации.

Как и в случае с другими рисками, риск потерять данные с домашнего компьютера выше у пользователей нелицензионного ПО.

ВЫВОДЫ

Ущерб для пользователей домашних ПК от использования нелицензионного ПО можно разделить на три основных категории:

Финансовые потери

Наиболее часто встречающийся вид ущерба и наиболее легко поддающийся оценке. Финансовые потери также часто являются следствием и двух других видов ущерба, потери репутации и уголовного преследования.

Величина ущерба может быть сопоставима, а зачастую значительно превосходит стоимость ПО, установленного на компьютере пользователя, если бы оно приобреталось легально.

Ущерб репутации

Все более часто встречающийся вид ущерба как следствие роста ценности персональной информации. Может включать в себя ущерб деловой репутации или компрометацию жертвы среди родных и знакомых. Также может иметь финансовые последствия.

Величина ущерба, хотя во многих случаях и не выражается в деньгах, но для большинства пользователей несопоставима с суммой, которую можно было потратить на лицензионное ПО с тем, чтобы с большей вероятностью избежать неприятных последствий.

Правовые последствия

Скорее теоретически возможная, чем реальная осуществимая угроза для абсолютного большинства пользователей домашних ПК. И тем не менее совсем сбрасывать ее со счетов не стоит, так как один такой инцидент может в тысячу раз превзойти по своей тяжести и финансовый ущерб, и потерю репутации.

МЕТОДОЛОГИЯ

Данный документ был подготовлен на основе существующих данных IDC. Более подробно о проблеме компьютерного пиратства и угрозах, связанных с использованием нелицензионного ПО, можно прочитать в следующих открытых документах IDC:

- Seventh Annual BSA/IDC Global Software 09 Piracy Study
- The Risks of Obtaining and Using Pirated Software
- Понимание рисков и затрат компании, связанных с использованием нелицензионного ПО