Социально опасные сайты

Каждый интернет-пользователь может попасться в ловушки, которые киберпреступники расставили в разных местах Сети.

Интернет приближает к нам сервисы и серверы, расположенные в разных странах и на разных континентах: все, что душе угодно, оказывается «на расстоянии клика». Но на таком же расстоянии – то есть совсем рядом! – находятся и созданные киберпреступниками ресурсы, которые с легкостью заразят ваш компьютер вирусом, украдут персональные данные, превратят ваш компьютер в «зомби», который без вашего ведома будет рассылать спам или участвовать в атаках на сайты… Где может таиться опасность и как обычному пользователю ее обойти?

Чего опасаться в Интернете?

Вредоносные программы. Они могут скрываться в скачиваемых файлах, приходить к вам по почте и даже «гнездиться» непосредственно в коде электронного документа, открытого вами в браузере. Очень часто случается, что попадание на ПК одного-единственного «вредителя» незаметно для вас открывает доступ к системе множеству других программ – они могут не только частично или полностью уничтожать данные, но также воровать и пересылать своим хозяевам конфиденциальную информацию.

Пиратский контент. Программное обеспечение, фильмы и музыка очень популярны во всех сегментах Интернета, в том числе и в русскоязычном. При этом операции с нелегальным контентом – даже загрузка, а тем более распространение – противозаконны. Отсутствие в России эффективнной юридической практики преследования пользователей, нелегально скачивающих или выкладывающих в Интернет и локальные сети контент, защищенный авторским правом, не означает, что однажды и отечественные правоохранительные органы, взяв пример со своих европейских и американских коллег, не решат заняться массовой борьбой с пиратством «на пользовательском уровне». Впрочем, возможность оказаться вне закона – не единственная опасность, поджидающая пользователей, охочих до халявы.

Фальшивые антивирусы. Программа может называться антивирусом, выглядеть и работать, как антивирус, но при этом делать кое-что еще. Она станет выводить предупреждения о шпионском «софте» или вирусах, которых на самом деле нет на вашем ПК, а за лечение от этой мифической болезни требовать покупки полной версии или специализированных «лекарств».

Вредоносные программы

Сайты, распространяющие трояны и вирусы.

Такие сайты появляются в Сети часто. Чтобы заманить на них пользователей, киберпреступники идут на различные ухищрения.

Например, при появлении броского новостного повода – резком высказывании публичной персоны, выходе нового фильма, клипа или другом событии, освещаемом в различных СМИ,

в блогах и т.д., – киберпреступники публикуют на популярных и посещаемых сайтах явную или скрытую рекламу, которая приводит ничего не подозревающих пользователей на сайты с вредоносным контентом.

При посещении такого сайта «зловредное» программное обеспечение может оказаться на компьютере пользователя разными способами. Например, посетителю могут предложить скачать разрекламированный клип или просмотреть его прямо в окне браузера. Но вот незадача: для просмотра необходимо установить специализированный плеер или плагин для браузера. Те, кто скачал и установил рекомендуемое киберпреступниками ПО, возможно, получат доступ к желаемому контенту, но «в дополнение» к нему на компьютер совершенно точно будет установлено вредоносное программное обеспечение.

Так как работа по «продвижению» подставных сайтов требует значительных трудозатрат, она должна приносить соответствующий доход: сложные вредоносные программы должны обеспечивать захват максимального количества компьютеров для проведения незаконных действий. Чаще всего вирусы распространяются через бесчисленные порносайты – исключительно потому, что подобные ресурсы весьма популярны во всем мире, но могут рекламировать любые услуги (от социальных сетей до такси).

Многие трояны, которые очень распространены на подставных сайтах, самостоятельно устанавливаются на компьютере при открытии страницы в браузере пользователя. Если вы вовремя не обнаружите «вредителя», хакеры смогут загрузить на ваш жесткий диск и другие вредоносные программы, узнать ваши персональные данные или использовать компьютер для рассылки спама незаметно для хозяина. В этом смысле троян полностью оправдывает свое название: незаметно попав в систему, он открывает доступ в нее другим – часто гораздо более опасным программам.

Но опасность может исходить не только от сомнительных сайтов. Хакеры используют популярные ресурсы и внедряют в них вредоносные коды. Например, этой весной оказался инфицирован сайт популярного певца Димы Билана: при обращении к главной странице ресурса пользователь автоматически скачивал скрипт, который в свою очередь обращался к некоему китайскому сайту, откуда на ПК жертвы попадала программа, обеспечивающая злоумышленникам доступ к личной информации пользователя, а также контроль над его компьютером в целом. Даже видеопортал YouTube уже использовался для распространения вирусов – троян там был замаскирован под видеофайл.

Есть и другой коварный способ заражения компьютеров тысяч пользователей по всему миру: преступники создают копии известных интернет-сайтов, таких как YouTube или MySpace, внешне почти не отличающихся от оригинала, и размещают на них вредоносные программы. Даже написание адреса сайта может быть очень схожим с оригинальным. На подобные «заменители» сайтов пользователей заманивают на обычных форумах или в чатах описанными выше способами. Но чаще опасность подстерегает тех, кто посещает ресурсы, посвященные созданию вирусов, распространению пиратского контента или, например, все те же порносайты.

Кому и зачем нужны вирусы и трояны?

Времена меняются: хакеры теперь редко создают вирусы ради развлечения или славы – гораздо чаще умелые и нечистые на руку программисты используют Интернет в качестве среды для получения выгоды.

По всему миру появились криминальные группы, которые выявляют все новые слабые места в системах защиты компьютеров. Поскольку пользователи стали подходить к вопросу установки приложений более разборчиво и осознанно, да и развитие антивирусных средств не стоит на месте, то и для проникновения в компьютеры понадобились новые хитроумные способы. Захват ПК проводится с целью их дальнейшего несанкционированного использования и контроля над ними:

1. для похищения конфиденциальной информации – паролей, номеров счетов и банковских карт, получения контроля над оплаченными аккаунтами в различных онлайн-системах (например, в сервисах IP-телефонии);

2. для осуществления удаленного управления тысячами компьютеров по всему свету; это может понадобиться для самых различных целей: чаще всего, получив контроль за компьютером-жертвой, злоумышленники превращают его в спам-агент (компьютер – без ведома законного владельца! – начинает рассылать спам от его имени по его контакт-листу или по списку адресов, полученному вирусом от его создателей; кстати, такие письма, кроме непосредственно рекламного текста, могут содержать и очередные копии вирусов, которые заражают все новые и новые машины);

3. разветвленная сеть, состоящая из многих тысяч машин по всему миру, может использоваться также для осуществления DDOS-атак.

Самые опасные «замаскированные» сайты с троянами и вирусами

Адрес	Содержание и угрозы	Адрес	Содержание и угрозы
www.fevertube.com	сайт содержит видеофайлы с изображениями обнаженных знаменитостей. В необходимом для просмотра роликов видеокодеке находится вирус	www.astalavista.box.sk	популярный форум хакеров, где размещено много ссылок на опасные программы
www.girls-forever.com	привлекает фотографиями порнографического содержания, сканирует браузер в поисках слабых мест в системе защиты	www.stepbystepbg.org	обещанные способы изучения иностранного языка отсутствуют. Вместо этого присутствуют трояны
www.kassperskylabs.cn	не путать с сайтом Kaspersky.com! Поддельный ресурс при обращении к нему сканирует систему в поисках слабых мест и устанавливает вредоносные программы	www.thetextdesk.com	на этом сайте предлагается ПО для мобильных телефонов, которое содержит интегрированные вредоносные программы
www.magicpornotube.net	секс-видеопортал. Здесь тоже можно подхватить троян	www.hqticket.com	здесь предлагается бесплатно скачать музыку, фильмы и игры, но для скачивания необходимо установить программу, содержащую вирус
www.adultan.com	привлекает видеороликами порнографического содержания. Программа для скачивания этих роликов содержит троян	www.web-money.cn/arm	служба онлайн-платежей, которая автоматически попытается установить вам программу с трояном
www.nudeteens.in/3	заманивает с помощью фотографий обнаженной натуры и внедряет в систему троян	www.pokerfinds.com	сайт для игры в покер, который ищет слабые места в системе безопасности и использует их для установки вредоносного кода

Кто стоит за рассылкой спама?

Спам заказывают для привлечения клиентов. Рассылка спама сегодня стоит сравнительно недорого – 4000–7000 руб. за несколько миллионов сообщений (стоимость услуги изменяется в зависимости от широты охвата: к примеру, рассылка спама абонентам только в Москве и Московской области будет стоить дешевле).

Спамеры – только исполнители. В настоящее время против спамеров все чаще возбуждаются судебные процессы, но заказчики спама пока остаются безнаказанными.

Спамер российского происхождения Леонид Куваев был приговорен судом США к многомиллионному штрафу за свою деятельность. Куваев занимался рассылкой спама с рекламой своих услуг (спам-рассылки весьма часто рекламируют спам как услугу), лекарств и интернет-казино, а также ресурсов с жестким порно (в том числе и детским). Для своей деятельности Куваев активно использовал бот-сети – захватывая управление многими сотнями компьютеров, он заставлял системы ничего не подозревающих владельцев рассылать рекламные письма. Действия это, безусловно, противозаконные. Но вряд ли по данному делу понесли наказание заказывавшие спам-рассылки владельцы интернет-казино или производители лекарственных средств.

Генераторы серийных номеров, «краки», «взломщики» и хакерское ПО

Так просто и заманчиво: быстро скачать trial-версию дорогой программы с сайта разработчика и, используя crack с нелегального источника, снять ограничения на использование данной программы, превратив ее в полнофункциональную. Но подобные действия не только противозаконны, но и опасны: зачастую вместе со взломанным ПО на компьютер устанавливаются вредоносные программы!

В Интернете – как в русскоязычной его зоне, так и на мировых ресурсах – вы можете найти:

серийные номера для лицензионного ПО (с их помощью можно установить копии программ или преобразовать тестовые версии программ в полные; номера либо размещаются непосредственно на нелегальном сайте, либо копируются на компьютер в текстовом формате);

crack-элементы – один или несколько файлов, с помощью которых trial-копия превращается в полнофункциональную; для этого, например, деактивируется проверка серийного номера, а файл запуска программы меняется на поддельный (при последующем обновлении программы могут возникнуть проблемы, для решения которых придется использовать новый crack);

генераторы ключей (эти программы способны создавать последовательности символов, воспринимаемые защитными системами программ в качестве реальных ключей для регистрации ПО).

Самые опасные сайты с «краками» и инструментами хакеров

Адрес	Содержание и угрозы	Адрес	Содержание и угрозы
www.easycracks.net	поисковик для «краков»; имеется «ежедневное обновление»; ссылки → 05 (стр. 28) содержат трояны	www.crackportal.com	более 100 тыс. «краков» для загрузки одновременно с установкой вредоносного ПО
cracks.thebugs.ws	хранилище «краков»; файлы содержат трояны	www.serialsbox.com	угроза установки трояна при скачивании данных
www.icracks.net	при скачивании какого-либо файла с этого сайта есть риск получить троян	www.keygen.us	генератор серийных номеров и «краки» для скачивания; все ссылки заражены
www.anycracks.com	на этом сайте за ссылками на «краки» также спрятаны трояны	www.seriall.com	при скачивании «крака» с этого сайта вы получаете троян ISmall и другие!
www.keygen.name	огромный выбор «краков», генераторов серийных номеров и ключей, использование которых грозит проблемами с вирусами и троянами	www.hackpalace.com	«сайт безопасности» с руководствами для хакеров, «краками», программами слежения и многим другим
www.serialz.to	ресурс с 80 тыс. серийных номеров для загрузки; при использовании происходит установка шпионских программ и программ для рассылки спама	www.hackingstore.de www.hacker-spider.at.nr	отсюда якобы можно скачать программы для хакеров, на самом же деле с сайта автоматически устанавливается вредоносное ПО

Откуда берутся «краки», серийные номера и генераторы ключей?

Crack для программного пакета создается хакерами – высококвалифицированными программистами, умеющими использовать недокументированные методы. Иногда хакеров, специализирующихся на создании решений для взлома, называют «кракерами» (от англ.

Craker). В большинстве слу чаев «кракеры» создают инструменты для взлома защиты программ для самоудовлетворения и для развития собственных программистских способностей, а также с тем, чтобы снискать уважение у других пользователей, соревнующихся в том, кто быстрее всех взломает систему защиты современной программы. Заметим, что «кракерами» называют не только создателей инструментов для взлома защиты программ, но и взломщиков сайтов, которые могут преследовать и коммерческие цели.

Чаще всего киберпреступники действуют организованными группами. Целью одних участников группы является заблаговременный поиск оригинального продукта (иногда его воруют раньше, чем релиз поступит на завод по тиражированию оптических дисков). Другие отвечают за взлом защиты программы. Но «достоянием общественности» результаты работы этих двух специалистов обычно делают другие.

Кто стоит за crack-сайтами?

Поисковая машина www.cracks.am находит 951 нелегальную crack-програм-му для различных версий Adobe Photoshop; неясным остается вопрос, сколь-ко из этих crack-файлов содержат в себе вирусы и трояны

Обычно «кракеры» не занимаются распространением собственной продукции – данная деятельность требует особой квалификации и лежит за пределами области интересов хороших программистов. Специализированные группы киберпреступников создают crack-ресурсы для получения стабильной выгоды. Разумеется, эти же группы занимаются «продвижением» своих сайтов например, добиваются того, чтобы именно их ресурсы появлялись на первых позициях в «поисковиках» по запросам типа «serial number <название программы>».

Откуда получают выгоду создатели crack-ресурсов? В предлагаемые широкой публике «за копейки» инструменты для взлома вставляются «зловредные» элементы. А «навар», питающий всю crack-индустрию, получается от использования возможностей, открываемых многочисленными троянами, шпионами и клавиатурными перехватчиками, которые внедряются в компьютеры пользователей, польстившихся на возможность на халяву превратить trail-версии в полнофункциональные.

Хотя основной доход crack-ресурсы дают в результате краж персональной информации – от номеров и паролей кредитных карт до данных об индивидуальных предпочтениях пользователя. Эти сайты приносят своим создателям деньги и вполне легальными традиционными методами (например, баннерной рекламой).

Примером такого ресурса может служить сайт www.serialz.to, представляющий собой огромное собрание (почти 80 тыс.) серийных номеров для загрузки. Причем для активных пользователей такие сервисы предоставляют возможность рассылки писем с обновлениями и пополнениями баз серийных номеров. Вирус пользователи этого сервиса могут получить не только в результате установки crack-утилиты, но и, например, в рассылке с данного нелегального ресурса.

Кто такие хакеры?

Технические специалисты высокой квалификации, способные использовать недокументированные возможности цифрового оборудования и программного обеспечения. Слово «хакер» не является синонимом слова «киберпреступник», а «хакерство» само по себе не есть преступление.

На хакера не учат нигде. Большинство хакеров сочетает «стандартную» техническую подготовку с активным самообразованием. Например, языки программирования, принципы работы «железа», коммуникационных элементов, операционных систем и прикладных программ удобнее изучать в рамках стандартных учебных курсов. А вот недокументированные возможности программ и оборудования, особенности работы вирусов, «болевые точки» защитных структур, операционных систем и т.д. можно в тонкостях изучить только самостоятельно. Для последнего необходимо знание английского языка – мировое хакерское сообщество не признает локальных языков, а переводить на русский материалы хакерских конференций и ресурсов для вас никто не будет.

Знания и инструменты хакера сами по себе не опасны (равно как и любые другие инструменты). Они могут оказаться крайне полезными (например, если вы забыли пароль от архива или учетной записи), а могут стать орудиями совершения преступлений. Даже наборы вирусов и трояны, которые представлены на хакерских сайтах, могут быть опасными, если «экспонаты» модифицировать и выпустить в открытый Интернет, а могут быть совершенно безобидными, если используются для изучения особенностей программирования.

Самые опасные «замаскированные» сайты с «краками» и инструментами хакеров

Адрес	Содержание и угрозы
www.biohazard.xz.cz	собрание вирусов из Чехии
www.hackpalace.com/virii/indexe.shtml	обширное собрание вирусов
www.phreak.org/html/virii.shtml	вирусы и генераторы вирусов; многие вредоносные программы запускаются при скачивании
vx.netlux.org	большое собрание комплектов для создания вирусов
www.rigacci.org/comp/virus	небольшое, но очень опасное собрание вирусов
www.worst-viruses.2ya.com	вирусы и комплекты для создания вирусов
vx.org.ua/delphi	собрание исходных кодов вирусов на языке программирования Delphi
members.fortunecity.com/acid_knight	беспорядочное собрание вредоносного ПО

Адрес	Содержание и угрозы
www.pugnax.co.uk/code	исходные коды для некоторых вирусов в качестве «учебного материала»
www.textfiles.com/virus	различные руководства по созданию вирусов
membres.lycos.fr/gatesbillou	генераторы вирусов для скачивания
www.freewebs.com/green-hell	вирусы для скачивания со спрятанным трояном; тот, кто скачивает файл, получает программу-шпион
vxchaos.2hell.com	обширное собрание вирусов, троянов и прочих программ сомнительного содержания
www.geocities.com/randy027dsz36	генератор вирусов для скачивания; файлы содержат программы для установки другого вредоносного кода
web.tiscalinet.it/dec_spiderman/home.	вирусы и их описания (текст на итальянском языке)
www.nvkz.kuzbass.net/as	обширное собрание вирусов с описаниями на русском языке

Что можно найти на сайтах для создателей вирусов?

Желающим попробовать себя в деле написания вирусов доступны сотни специализированных программ – все их можно скачать со специальных ресурсов в Сети. Но стоит помнить об опасности! Создать вирус может даже начинающий программист (для этого доступно много элементов, собрать которые в действующую систему так же просто, как объединить детали детского конструктора), а вред может быть нанесен значительный.

Но в «вирусостроительных» комплектах также могут быть спрятаны вредоносные элементы! Особенно опасен в этом плане ресурс www.freewebs.com/green-hell. Здесь чуть ли не в каждом файле, предназначенном для скачивания, содержится вредоносная программа, которая открывает путь для других вредителей.

Кто стоит за сайтами с вирусами?

В большинстве случаев – хулиганы, считающие себя «крутыми хакерами». Но попадаются и идеалисты, которые хотят указать производителям ПО на слабые места в системе безопасности их «софта». Некоторые называют себя «экстремалами», которым просто не хватает адреналина. Немало и хакеров, движимых исключительно «неправовыми» побуждениями, стремящихся заработать как можно больше, обманывая простых пользователей и компании, производящие ПО. Но в любом случае работа с вирусами стимулирует изучение технологий.

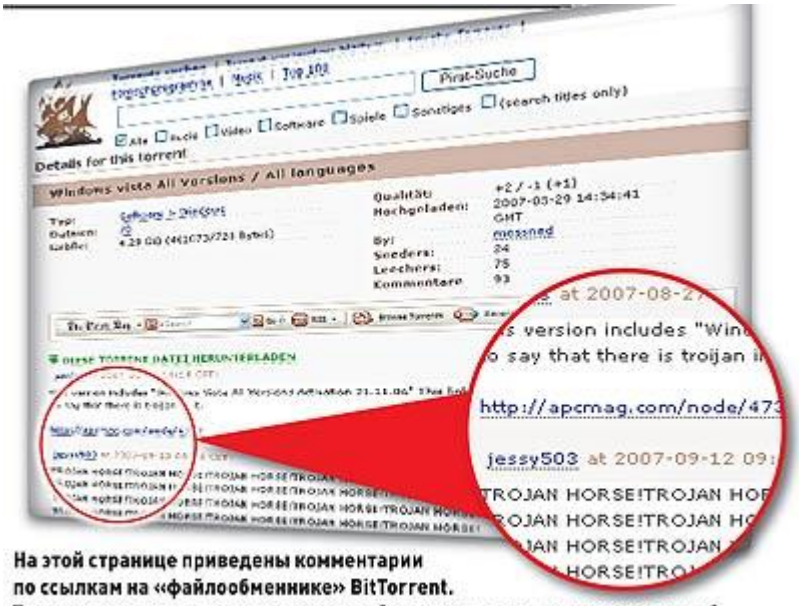
Кто стоит за «файлообменниками»?

Файлообменные сервисы (как сети, так и сайты) сами по себе вполне легальны, поэтому их владельцы ничем не отличаются, например, от предоставляющих сервисы хостинга, электронной почты, «виртуальных дисков» и т.д. Заметим, что такие сервисы предлагают даже крупные порталы, в том числе и российские, например «Яндекс» (служба «Народ.Диск») и Mail.ru (сервис «Файлы@Mail.ru»).

Только администрациям файлообменных сервисов приходится всячески ограждать себя от обвинений в пиратстве. Например, администрация многочисленных платных и бесплатных музыкальных ресурсов, предлагающих пользователям покупать MP3-файлы по относительно невысокой (по сравнению с крупными зарубежными сервисами типа iTunes Music Store) цене, пытается оградить себя от преследований за распространение пиратской продукции, утверждая, что все файлы выложены на сервисах исключительно с целью ознакомления и после прослушивания должны быть удалены. Текст «Если вам понравилась та или иная песня, вы должны купить компакт-диск, а скачанный MP3-файл «стереть» или похожий вы можете найти практически на каждом ресурсе.

В конечном счете, заработать могут даже создатели бесплатных ресурсов с пиратским продуктом: «файлообменники» пестрят рекламой.

Какие опасности поджидают пользователей пиратского контента?



На этой странице приведены комментарии по ссылкам на «файлообменнике» BitTorrent. Также приводятся предупреждения об опасности: два пользователя сообщают, что распространяемая пиратская копия Microsoft Windows Vista заражена трояном

Вредоносные программы. Недобросовестные люди пытаются распространять вирусы и трояны и через «файлообменники». Особую опасность представляют собой программы для взлома защитных систем пакетов и программ – «краки», генераторы ключей и даже архивы, содержащие текстовые файлы с серийными номерами, так как все они могут содержать вредоносные коды. Впрочем, на популярных торрент-трекерах и файлообменных ресурсах проводится проверка файлов на наличие инфицированных компонентов, и опасные ссылки удаляются.

Преследование по закону. В правоохранительных органах всех стран (за исключением государств, в которых Интернет запрещен в принципе) существуют специальные отделы по борьбе с киберпиратством. Их сотрудники ведут простую игру: они предлагают нелегальные музыкальные файлы и фиксируют IP-адреса, куда они скачивалась. Затем они налагают на пользователей взыскания – в основном штрафы. Подобная практика применительна к пользователям, которые не извлекают из незаконного копирования прямой выгоды, и пока не сильно распространена, особенно в России, но все же существует.

Пиратский контент за деньги

Полный пакет Microsoft Office 2007 всего лишь за 50 евро вместо обычных 500? Того, кому это не покажется странным, профессиональные пираты уже поймали на крючок. И тот, кто «клюет» на подобные рекламные сообщения и спам, приобретает нелегальное программное обеспечение.

Что обычно рекламируется в магазинах нелегального «софта»?

Одним из лучше всего оформленных нелегальных магазинов является Euro Software. У него качественный интерфейс, большой ассортимент, причем программы стоят до смешного дешево. Продаются здесь исключительно пиратские копии программного обеспечения

Дорогое программное обеспечение по «бросовым» ценам. Предлагая популярные программные продукты – прежде всего производства Microsoft, Adobe и Corel, – владельцы подобных магазинов зарабатывают огромные деньги: затраты на контент-то у них практически нулевые. Обычно ими предлагается однажды купленная программа, «лицензионную чистоту» которой обеспечивают уже знакомые нам генераторы серийных номеров или crack-утилиты.

Если человек совершил покупку в таком магазине, оплатив товар с помощью кредитной карты, он может скачать данные прямо на жесткий диск. Часто клиент получает копии CD или DVD («имиджи», или образы дисков), которые перед использованием необходимо записать на «болванку».

Благодаря профессиональному оформлению, наличию товарной корзины, службы поддержки и других механизмов, присущих нормальным интернет-магазинам, такие ресурсы могут произвести впечатление серьезных и заслуживающих доверие. Многие зарубежные сайты могут даже привлечь российского пользователя русскоязычным интерфейсом – по крайней мере часть их страниц будет переведена на понятный язык. В качестве основания для столь значительного снижения цен многие магазины ссылаются на отсутствие упаковки или руководства пользователя. Часто они обозначают свой товар как OEM-Software, то есть программы, которые, как правило, могут продаваться только вместе с компьютером конкретной марки.

Дешевая пиратская музыка

Популярные зарубежные музыкальные интернет-магазины почти не имеют клиентов из России – им у нас противостоит множество локальных ресурсов, предлагающих музыку значительно дешевле или бесплатно. При этом нарушение авторских прав не волнует ни пользователей, ни создателей подобных ресурсов. Впрочем, не стоит считать, что российские музыкальные интернет-магазины совершенно безопасны – их клиентуру также могут ожидать неприятные сюрпризы.

Если вы оплачиваете музыку с помощью карты, будьте осторожны: нелегальные магазины крайне ненадежны – ваши данные могут быть похищены, что приведет к исчезновению денег со счетов.

Произведенная оплата еще не означает, что вы получите тот файл, который заказывали; также никто не гарантирует, что битрейт композиции не окажется ниже, чем нужно, и что в файле не будет ошибок.

Если при регистрации на сервисе вы вводите адрес своего электронного почтового ящика, будьте готовы к тому, что скоро в него с большой вероятностью польются потоки спама.

Как работает система обмена?.

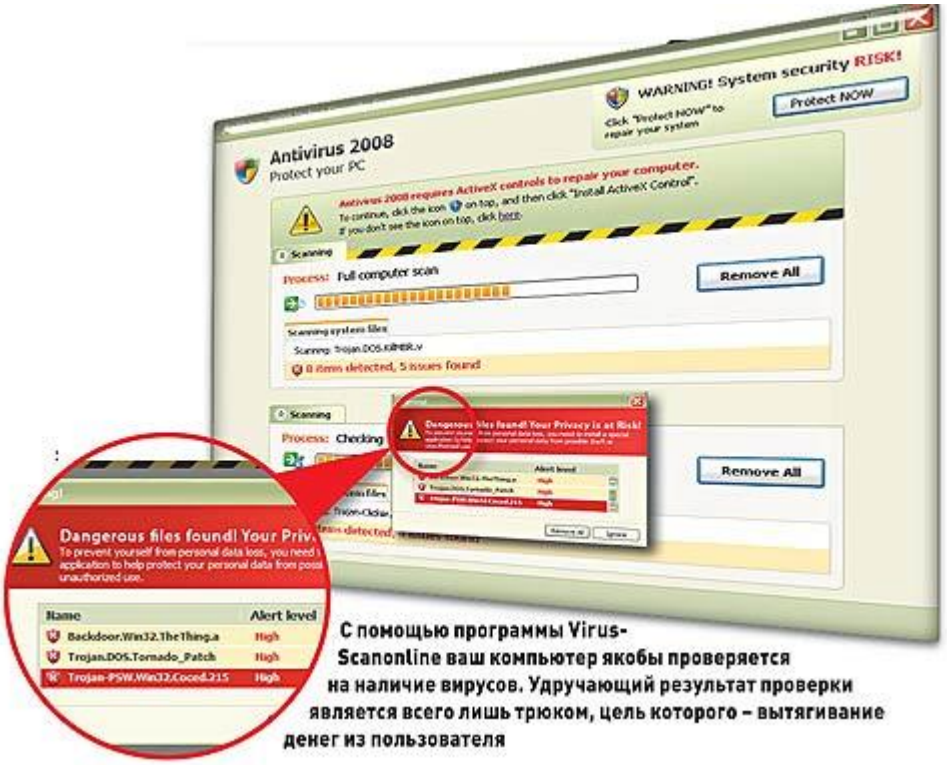
Пользователи обмениваются ссылками на пиратские копии через соответствующие интернет-сайты, форумы и даже при личной переписке. Обычно передача фильмов и музыки происходит через файлообменные сети или хранилища данных (такие, как BitTorrent или «файлообменник» Rapidshare). Здесь можно найти и бесплатно скачать как новые, так и уже известные фильмы в TB-, DVD- или даже HD-качестве, музыку различных исполнителей и многое другое – вплоть до сугубо профессиональных программных пакетов.

Для скачивания из сети BitTorrent требуется установка на компьютер программы-клиента (например, µTorrent). Пользователь, посредством данной программы скачивающий музыку или фильмы, автоматически становится источником этих файлов для пользователей, подключенных к торрент-трекеру. Так создается всемирная сеть, состоящая из различных источников, – центрального компьютера с файлами для обмена не существует.

Данные, размещенные на Rapidshare и других тому подобных «файлообменниках», можно скачать одним щелчком мыши («прямое скачивание») без установки дополнительного программного обеспечения (понадобится разве что программа-архиватор для распаковки архивов с файлами).

Обмен такими данными – не такой уж и невинный поступок: предложение и использование нелегальных копий в большинстве стран мира преследуется по закону. Использование файлообменных сервисов является вполне законным, пока вы скачиваете с них и размещаете на них легальные данные, например созданные вами фотографии и видео, бесплатно распространяемые программы и т.д. Но как только вы скачиваете/размещаете контент с нарушением авторских прав, ваши действия становятся противозаконными – со всеми вытекающими отсюда последствиями.

Опасные антивирусы



С помощью программы Virus-Scanonline ваш компьютер якобы проверяется на наличие вирусов. Удручающий результат проверки является всего лишь трюком, цель которого – вытягивание денег из пользователя

«Альтернативные» антивирусы, рекламируемые в Сети, подчас могут стать источниками массы проблем для пользователя. Такие программы имеют названия типа Win-Antivirus, Malwarealarm или Spystriker – множество подобных утилит предлагается для бесплатного скачивания на ресурсах, занимающихся распространением программного обеспечения, и даже на фирменных сайтах производителей ПО. Но то, что выглядит как пакет программ для защиты от вирусов и «шпионов», на самом деле им не является, так как эти и другие «программы для обеспечения безопасности» лишь делают вид, что защищают компьютер. В действительности ни одна из них не обеспечивает необходимую защиту. Напротив, многие из таких программ сами приносят на диски ПК вирусы.

Как работают подобные программы?

Схема всегда одинакова: на убедительно оформленном сайте для бесплатного скачивания предлагается антивирус или утилита для защиты от программ-шпионов. После ее установки может происходить следующее:

1. бесплатным оказывается лишь поиск; вирусы удаляются, только если вы приобретаете «полную версию программы»;

2. для того чтобы заставить клиента платить, эти программы-вымогатели выводят сообщения о несуществующих вирусах;

3. настоящими программами-«вредителями» даже купленные «полные версии программ по защите компьютера» совсем не занимаются, или все же ловят их, но делают это крайне плохо;

4. даже безобидные файлы (например, cookies) определяются в качестве вредителей для того, чтобы пользователь купил «антивирус»;

5. многие программы устанавливают на ваш ПК реальные вирусы, которые затем, конечно же, «обнаруживаются» во время очередной проверки;

некоторые программы забрасывают клиента рекламой и похищают приватную информацию;

6. многие из таких «антивирусов» крайне сложно удалить.

Кстати, даже если ничего из описанного выше при использовании сомнительного антивируса не произошло, это не означает, что ваш компьютер защищен.

Заметим, что существуют бесплатные антивирусы, которые честно выполняют свою работу.

Как определить, что я обладатель лжеантивируса?

К сожалению, определить такую программу очень сложно. В данный момент существует более 100 подобных программ. Сайты создателей самых распространенных лжеантивирусов вы найдете в списке внизу. Например, к их числу относится программа Winantivirus, классический пример лжеантивируса, который присутствует на рынке уже несколько лет и постоянно обновляется.

Берегите ваши деньги!

Сетевая торговля постепенно развивается и в нашей стране, но повсюду находятся мошенники, желающие поживиться за счет незадачливого пользователя. Если вы решили приобрести товар или услугу в Сети, будьте осторожны, ведь вам придется вводить данные своей банковской карты, номер счета в электронных платежных системах и соответствующие пароли. Самой безобидной из проблем, связанной с регистрацией в ненадежном интернет-магазине (не говоря уже о явно мошенническом ресурсе), будет возрастание потока спама, который обрушится на e-mail-адрес, указанный при создании аккаунта. Гораздо хуже, если с вашего счета пропадут деньги, а товар при этом окажется совсем не таким, какой описывался на сайте. Более того, может случиться, что покупка так никогда и не будет доставлена…

Чтобы избежать этого, следуйте простым рекомендациям:

1. приобретайте товары только в проверенных и популярных интернет-магазинах;

не верьте продавцам, предлагающим товар по цене значительно ниже средней (согласитесь, новый стабильно работающий iPhone от Apple вряд ли может стоить 3000 руб.);

2. внимательно присмотритесь к оформлению сайта, выясните, указаны ли на нем адрес и телефон продавца и являются ли они подлинными; если интерфейс ресурса сделан топорно и содержит ошибки, воздержитесь от онлайн-оплаты товара в таком магазине;

3. заведите специальную банковскую карту для покупок в Интернете и не используйте ее в других случаях – на связанный с нею счет можно каждый раз класть небольшую сумму денег, достаточную только для оплаты товаров;

4. подготовьтесь к покупке, внимательно изучив характеристики товара (например, на сайте производителя); обязательно уточните, что вы получаете товар с теми же характеристиками и в той же комплектации, как и у версий, предлагаемых, например, в офлайновых магазинах;

5. с помощью «Яндекса» или Google поищите в Интернете упоминания о магазине и отзывы о его работе; если с ним были связаны какие-то неприятные ситуации, пользователи не преминут об этом рассказать.

Другие средства защиты от опасных сайтов

Встроенная защита браузеров

Современные браузеры имеют различные встроенные средства защиты от вредоносных сайтов. Например, Firefox 3.0 просто отказывается переходить на опасные ресуры – вместо содержимого ненадежной страницы вы увидите соотвествующее предупреждение. В этом случае вы можете либо вернуться на предыдущую страницу, кликнув по кнопке либо перейти на стартовую страницу браузера. Если, несмотря на все предупреждения, вы все-таки решили перейти к опасному сайту, кликните по ссылке.

Список опасных сайтов создается на основе сообщений пользователей и компаний, отслеживающих степень безопасности контента.

Опасные и пиратские сайты и поисковые ресурсы

Крупные поисковики также преудпреждают о ненадежных ресурсах, встреча с которыми может грозить пользователю неприятностями. Рядом с названием сайта в результатх поиска могут появляться специальные обозначения, которые предупредят пользователя о ненадежном или опасном содержимом ресурса. Такие вредоностные и пиратские сайты могут даже исключаться из результатов поиска.