
detect...

Удаление программ spyware

СМЕРШ для компьютера

Программы

В Интернете слишком много желающих познакомиться с содержимым вашего компьютера. Пути и методы такого проникновения могут быть разными, но цель одна — шпионаж. Мы не будем сейчас касаться вопросов хакерских атак и методов защиты от них. Речь пойдет о программах-шпионах, которые мы часто получаем в качестве довеска к полезным и распространенным утилитам.

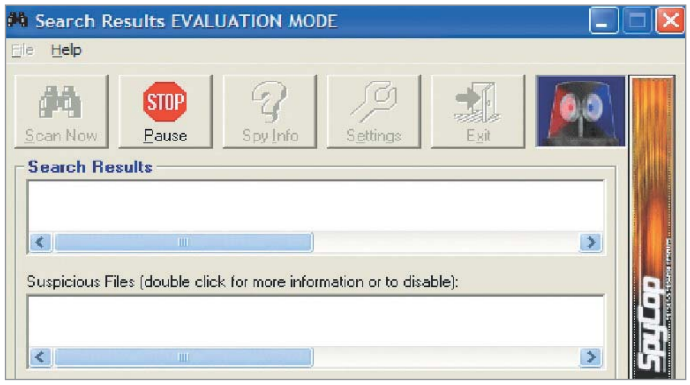
Например, имеется целый ряд весьма полезных утилит, которые широко применяются большинством пользователей (как частных, так и корпоративных), не ведающих о двойной жизни их любимого софта. Дело в том, что эти программы отличаются нездоровым интересом к содержимому компьютера, на котором они установлены. Этим грешат, например, некоторые версии таких популярных программ, как CuteFTP, GetRight, Go!Zilla, Net Sonic и многие другие. Они очень часто содержат шпионские модули (spyware). Наиболее известны такие spyware, как Aureate, Cydoor, DoubleClick, EverAd, OnFlow и Web3000. Чаще всего шпионские модули попадают на ваш компьютер через программы типа adware, поэтому их еще называют spyware рекламного типа. Количество программ со шпионской начинкой на момент написания статьи составляло, по нашим оценкам, около 250.

Конечно, рекламный тип шпионских программ относительно безопасен, но тем не менее неприятно, что эти программы в процессе работы потихоньку собирают конфи- »

» денциальную информацию и передают ее либо на сайт разработчика, либо еще куда-то. Желающие могут в этом наглядно убедиться, используя специальные средства защиты. Но об этом пойдет речь немного позже.

Однако существуют и другие виды spyware. Наиболее опасным типом spyware являются так называемые программы для тотальной слежки за вашим компьютером (например, Y3K , Spektor, AgentSpy и т. п.). Они пробираются на ваш компьютер самыми различными путями и очень умело маскируются, так чтобы быть абсолютно незаметными для пользователя. Действуют они, естественно, также не афишируя своего присутствия.

Их цель — запись абсолютно всего, что происходит на вашем компьютере: создание «мгновенных снимков» экрана, фиксирование последовательности нажатия клавиш на клавиатуре, перехватывание паролей для доступа в Интернет или номеров кредитных карточек и т. д. и т. п. Кроме того, некоторые программы этого класса могут записывать происходящее на вашем компьютере на видео.



▲ Не слишком удобный интерфейс программы и отсутствие локализации — основные недостатки SpyCop

Существуют различные способы защиты от шпионского софта. Понятно, что самый простой способ — вообще не подключаться к Интернету. Но это крайняя мера. Можно также установить на компьютере программу-firewall и спать спокойно. Однако такой подход не позволяет детектировать существование самих шпионских программ в вашей системе. Проблематично также, что он защитит вас от вредоносной работы уже проникших в вашу систему и хорошо замаскировавшихся шпионских модулей.

Именно для того чтобы обнаружить непрошенных гостей на вашем компьютере на ранней стадии их развития и, естественно, оградить себя от их работы, предназначены специальные антишпионские программы. О них-то и пойдет речь.

SpyBlocker 4.75 Beta

На наш взгляд, это довольно интересная и полезная программа. Принцип ее работы от- »

System Cleaner

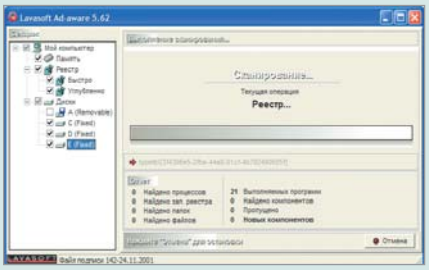
Лучший продукт CHIP >> 05/2002

Lavasoft Ad-Aware 5.62

Враг не пройдет

Признание не бывает незаслуженным: Ad-Aware в наибольшей степени удовлетворяет всем условиям тестирования.

Оценка	▶	4,7
Разработчик	▶	Lavasoft Team USA
Адрес загрузки	▶	www.lavasoft.de
Размер дистрибутива, Кбайт	▶	883
Условия распространения	▶	freeware



▲ Ad-Aware имеет приятный интерфейс и проста в управлении

ПЛЮСЫ/МИНУСЫ

+ Обширная база данных программы
+ Удобный интерфейс
+ Возможность русификации

Самая знаменитая антишпионская программа. Создана шведской фирмой Lavasoft. Сайт и национальная принадлежность этой программы, вообще-то, «тайна великая есть», ибо в течение последних трех лет авторский сайт плавно перетек из Швеции через Германию в США.

Программа может обнаружить около 230 шпионских программ на основе собственной базы данных. Поиск производится в разных областях системы: в реестре, в памяти, в папках, в файлах. Немного подкачала функция восстановления состояния системы, которая работает не всегда надежно и может вызывать небольшие проблемы с реестром. В частности, некоторые записи могут не восстановиться. Но это не портит общего хорошего впечатления от программы.

Что касается эвристических способностей, то программа действительно способна искать «шпионов», отсутствующих в ее базе данных. Она анализирует работу оперативной памяти и отыскивает те программы (процессы), к которым система не должна была достаточно долго обращаться, учитывая характер текущей деятельности. Если такие процессы не запускались, но проявляют, тем не менее, избыточную активность, Ad-Aware предупреждает пользователя. Таким образом, удается обнаружить паразитические программы (трояны, вирусы, шпионские модули и т. п.).

Lavasoft Ad-Aware позволяет создавать «языковые модули» для интерфейса. Файл для русификации программы можно с легкостью найти в Интернете.

личается от методик обнаружения шпионских программ, которые используют все прочие утилиты, представленные в нашем обзоре. SpyBlocker перехватывает и блокирует подозрительные запросы, направляемые вашей системой к различным IP-адресам, еще до того, как эти запросы дойдут до адресатов.

Такой алгоритм ее работы позволяет заметно повысить вероятность обнаружения шпионов. На основании того же метода эта программа находит действующие троянские программы, активно работающих интернет-червей и прочие вирусные отпрыски.

Очевидно, что SpyBlocker успешно обнаружил нашего тестового шпиона Alexa. Только произошло это не сразу, а лишь после того, как тот начал подключаться к удаленному серверу.

Интерфейс данной программы в целом интуитивно понятен, но не имеет локализации, то есть не русифицируется.

К серьезному недостатку программы можно отнести ее настойчивое желание отредактировать файл hosts.sam в папке Windows для Windows 9x или lmhosts.sam в папке %SystemRoot%\system32\drivers\etc\ для Windows XP или 2000 при первом запуске после установки, что в некоторых случаях вызывает конфликт с системой. Также надо быть осторожным, если у вас установлены программа типа WatzNew или аналогичные утилиты для скачивания информации из Интернета в режиме реального времени, поскольку вы можете добавить себе изрядных неприятностей. Это связано с блокировкой обращения к удаленному серверу.

Данная программа обладает эвристической функцией, то есть она отлично обнаруживает неизвестные еще шпионские модули. Эта возможность и является основным достоинством программы. К сожалению, в ней не предусмотрена функция восстановления состояния системы до перехвата запроса шпиона к удаленному серверу и блокировки оного.

Программа распространяется абсолютно бесплатно без каких-либо ограничений, что, несомненно, понравится пользователю. В целом, можно сказать, что программа удобна и надежна, хотя и не лишена недостатков.

▲ SpyBlocker — достаточно надежный борец со шпионами

SpyCop 3.5 Trial

По утверждению авторов программы, она умеет вылавливать настоящих шпионов на вашем PC. Она сканирует исполняемые файлы на предмет наличия в них шпионских модулей. Trial-версия программы, которая была в нашем распоряжении, проверяет, к сожалению, только выбранные ею 200 файлов в системе. Понятно, что это слишком мало для то- »

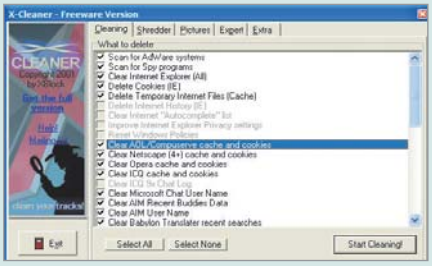
ОПТИМАЛЬНЫЙ ВЫБОР CHIP >> 05/2002

XCleaner 2.0.49 Lite

Антишпионский набор высокого класса

Наряду с уверенным распознаванием программ spyware XCleaner предлагает несколько дополнительных полезных инструментов.

Оценка	4,3
Разработчик	XBlock
Адрес загрузки	www.xblock.com
Размер дистрибутива, Кбайт	278
Условия распространения	freeware (версия Lite), box — $90



▲ Программа умеет бороться не только с рекламными шпионскими модулями

ПЛЮСЫ/МИНУСЫ

+ Полезные дополнительные функции
+ Корректная работа с новыми версиями Windows

Великолепная профессиональная программа для защиты как индивидуальных, так и корпоративных компьютеров. Это относится, естественно, к наиболее полным коробочным версиям антишпионского пакета. Однако имеется и демо-версия (вариант Lite), которую можно бесплатно скачать для ознакомления.

Вместе с тем даже такой урезанный вариант может быть полезен, ибо он не только знакомит вас с этой программой, но и неплохо работает.

Кроме обычных «рекламных» spyware-систем, XCleaner ищет также и программы типа Spector, Y3K, AgentSpy, GhostSpy и другие, действующие незаметно для пользователя системы тотального шпионажа. Надо особо отметить, что XCleaner имеет много полезных дополнительных функций, защищающих личную безопасность. Например, встроенная функция Schredder позволяет необратимо удалять файлы с диска.

Интерфейс программы интуитивно понятный и не вызывает нареканий. Но, к сожалению, он не имеет возможности русификации.

Программа отлично показала себя на всех системах семейства Windows, начиная с Windows 95 и кончая Windows XP.

К сожалению, возможности поиска шпионских программ, отсутствующих в базе данных, у XCleaner нет. Она также не позволяет восстанавливать состояние системы «до лечения».

Однако мы можем порекомендовать эту программу каждому пользователю, поскольку она проста в освоении и использовании и стабильна.

	Lavasoft Ad-Aware 5.62	XCleaner 2.0.49 Lite	SpyBlocker 4.75 Beta	SpyCop 3.5 Trial
Разработчик	Lavasoft Team USA	XBlock	SpyBlocker Software	SpyCop Software
Сайт разработчика	www.lavasoft.de	www.xblock.com	personal.bellsouth.net	www.spycop.com
Условия распространения	freeware	freeware (версия Lite)	freeware	shareware, $ 49,95
Размер дистрибутива	883 Кбайт	278 Кбайт	1,9 Мбайт	1,2 Мбайт
Общая оценка	4,7	4,3	3,5	2,9
Функциональность	10	10	9	6
Интерфейс	10	10	8	7
Локализация	8,6	4	4	4
Совместимость с другим ПО	10	10	9,4	10
Восстановление состояния системы	8,4	4	4	4
Эвристический анализ	9,4	4	8	4

го, чтобы провести полную проверку ее возможностей.

Со шпионскими программами рекламного типа бороться она не умеет. Это мы проверяли неоднократно, и заставить ее проделать такую работу не удалось.

Интерфейс SpyCop не очень удобен и в чем-то кажется примитивным. Локализации не поддается. В программе не предусмотрено восстановление системы после удаления паразитов. Поскольку программа обращается исключительно к внутренней базе данных и не анализирует работу активных исполняемых файлов, она не имеет возможности и вылавливать незнакомые подозрительные программы.

Учитывая наши скудные возможности для анализа данного ПО, не приходится удивляться и низкой оценке, которую мы ей выставили. Не исключено, что коробочная версия имеет лучшие функциональные возможности.

SpyChecker 1.1

Принцип работы этой программы прост до неприличия. Она сверяет свою (надо заметить, весьма обширную — около 240 записей) базу данных шпионских программ и, если обнаруживает на вашем любимом компьютере нечто подозрительное, имеющее отношение к противоправной деятельности, предупреждает вас об этом. Понятно, что помогает такая защита далеко не всегда.

Но, как известно, кто предупрежден, тот и вооружен. Так что решайте сами. Интересен сайт базы данных в Интернете, к которой эта милая программка обращается при поиске: http://spychecker.com/cgi-bin/spybase.pl? [Название]. Вы можете ввести сами название программы, которую вы бы хотели проверить на принадлежность к славной шпионской когорте. Далее получаете ответ: есть таковая в базе или нет. К этому, собственно, и сводится вся работа SpyChecker.

Рис. 3. С помощью SpyChecker вы можете проверить любую программу на принадлежность к шпионам

Мы можем порекомендовать эту программу тем пользователям, которые не хотят загружать из Интернета (или с какого-нибудь диска) программы, которые могут начать шпионить за своими хозяевами.

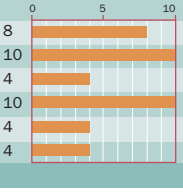
XP-AntiSpy 3.41

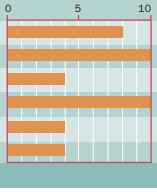
Эта программа заслуживает отдельного упоминания благодаря своей уникальности. Она предназначена для использования в Windows XP. И это просто замечательно. Значит, пока не слишком много пользователей пострадают от ее воздействия, учитывая относительно небольшой процент распространения новой операционной системы Microsoft.

При запуске это «гениальное произведение» передовой программистской мысли показывает вам список настроек, предлагая пометить те опции, которые должны, по ее мнению, спасти ваш компьютер от шпионов и любых несанкционированных вмешательств извне.

Однако большинство опций почему-то уже помечено заранее авторами программы, которые, естественно, лучше знают, что вам нужно. Возможность изменить программные настройки у вас отсутствует. В итоге ваш выбор реально сводится к мелочам. Если вы, не дай бог, кликнули по кнопке «Старт», то обречены. Умная программа перекроет все мыслимые каналы передачи и получения информации, отключив вам на всякий случай Windows Media Player, Windows Update, некоторые

SpyChecker 1.1	XP-AntiSpy 3.41
SpyChecker	TR-Software
http://spychecker.com	www.xp-antispy.de
freeware	freeware
285 Кбайт	76 Кбайт
3,3	3,3
8	8
10	10
4	4
10	10
4	4
4	4





Как мы тестировали

Экзамен для контрразведчиков

- Функциональность. Претенденты должны, прежде всего, обнаруживать программы, осуществляющие некую скрытую от пользователя (чаще всего шпионскую) деятельность, а также лечить (удалять) найденных паразитов. Очень хорошо, если имеется возможность восстановления системы к первоначальному состоянию.
- Эргономичность. Утилита должна иметь удобный интерфейс и возможность локализации.
- Совместимость. Программы не должны конфликтовать с новыми версиями Windows (Windows Millenium Edition, Windows XP).
- Эвристический анализ. Желательно, чтобы программа могла обнаруживать в системе не только известные, но и новые программные продукты шпионского характера.

Качественную проверку детективных способностей мы осуществляли на примере известной шпионской программы Alexa.

функции Internet Explorer и т. д. и т. п. Короче, имеем «железный занавес» и firewall в одном флаконе.

И все бы ничего (хотя, конечно, проще вообще не подключаться к Интернету, да и дело с концом), но все установки по умолчанию эта программа с немецким педантизмом и аккуратностью доводит до логического конца. Она попросту удаляет соответствующие записи из реестра или отключает соответствующие системные службы без возможности их восстановления (!). Это, без сомнения, гарантирует вам отсутствие шпионов в вашей системе. И если вы не воспользовались функцией «отката», которую вам предоставляет Windows XP, то я вам не завидую. Чтобы восстановить нормальную работоспособную систему, вам придется либо восстановить реестр, либо переустановить Windows. Кстати, с некоторыми шпионскими модулями эта программа борется неплохо, например качественно отключает шпиона Alexa. Насчет эвристических функций сказать нечего, поскольку их нет. О восстановлении системы мы говорили только плохие слова.

Так что я не рекомендую использовать XP-AntiSpy. На всякий случай...

Николай Амеличев

Использование шпионских программ

Кто любит знать о нас все?

Я вынес этот вопрос в заголовок не для красного словца. Ведь все чаще выясняется, что информацию о пользователях хотят получить не полубезумные хакеры-одиночки для удовлетворения своих амбиций, а серьезные фирмы и государственные организации. Да и в самом деле — велика ли выгода одинокому полуночнику от того, что он узнал, насколько часто вы заходите на Napster и какие музыкальные файлы скачиваете?

Между тем, Windows Media Player 8, намертво вплавленный в состав Windows XP, собирает информацию обо всех файлах, которые проигрывались в нем. Более того, при закачивании файлов, проигрываемых с ее помощью, программа передает на сайт (а это сайт, принадлежащий Microsoft) идентификационный номер пользователя. Согласитесь, что подобная информация может оказаться полезной многим компаниям, например звукозаписывающим или продюсерским. И все бы хорошо, только почему-то Microsoft решила предупреждать пользователей о таком своеобразном поведении программы только после того, как в адрес компании был направлен запрос от Associated Press.

Подобным повышенным интересом к пользователям компьютеров отличаются не только частные фирмы, но и государственные учреждения. Так, среди покупателей программы Investigator значится Федеральное бюро расследований. Говорят, что ФБР использовало эту программу для поимки русских хакеров в Сиэтле. А позволяет Investigator ни много ни мало как отслеживать и записывать все действия, совершаемые пользователем, вплоть до передачи хозяину программы всего, введенного с клавиатуры. Последняя версия программы позволяет делать скриншоты пользовательского экрана, снимки web-камер, отслеживать общение в чатах.

Вообще, программа Investigator является классическим примером того, как можно извратить изначально хорошую мысль. Первоначально программа задумывалась как инструмент для поиска и исправления ошибок в других приложениях. Но популярность она снискала именно как программа-шпион. Именно в этом направлении автор и стал в дальнейшем ее развивать.

На момент написания этой статьи число проданных копий перевалило за 200 тысяч. Возникает закономерный вопрос о том, кто же эти копии использует и какую информацию о чужих компьютерах собирает?