Обзор вирусных событий 2009 года

18 декабря 2009 года

Компания "Доктор Веб" представляет обзор основных вирусных событий 2009 года. По восточному календарю завершающийся год считается годом быка. Для киберпреступников «красной тряпкой» стали деньги пользователей – легкая добыча в условиях, когда человек доверчиво кликает по ссылкам, присланным якобы от друзей, и скачивает программы, «необходимые» для решения тех или иных задач. Создание разрушительных вредоносных программ при этом осталось в прошлом. Требования о переводе денег злоумышленникам выводились как в окнах различных интернет-браузеров, так и на рабочем столе или поверх всех окон в системе. В качестве транспорта для распространения вирусов использовались как классические каналы – электронная почта, системы мгновенного обмена сообщениями, так и новые – социальные сети и блоги. Рассмотрим наиболее заметные типы вредоносных программ, которые составляли основную часть вредоносного трафика 2009 года, а также намечающиеся тенденции будущих лет.

Руткиты

Больше всего загадок разработчикам антивирусных технологий Dr.Web в 2009 году задали авторы новых руткитов. Эти вредоносные программы скрывают своё присутствие в системе, а также позволяют работать в скрытом от глаз пользователя и большинства антивирусов режиме другим вредоносным программам, которые они загружают с вредоносных интернет-сайтов. Нередки случаи, когда компоненты руткита уже добавлены в вирусную базу какого-либо антивируса, но он, тем не менее, не замечает присутствия вредоносного объекта в системе.

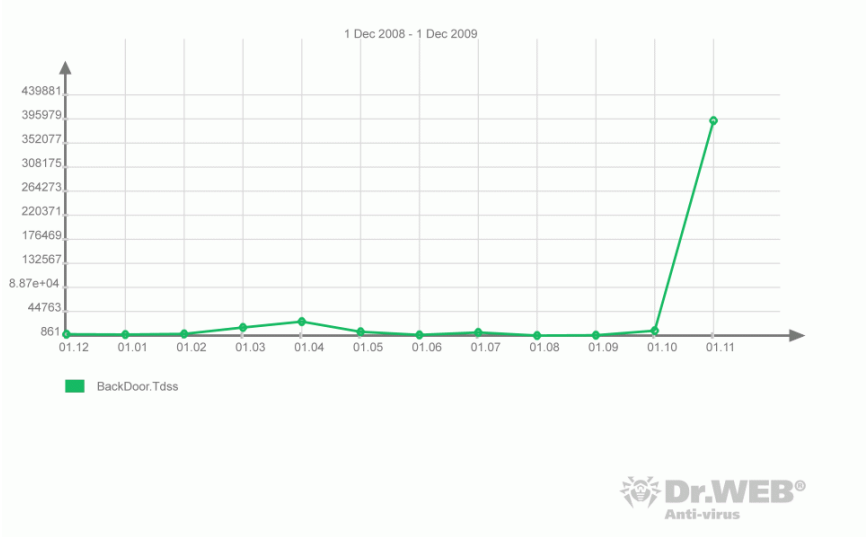
Наиболее заметными вредоносными программами данного класса стало семейство **BackDoor.Tdss** (название приводится по классификации Dr.Web). За 2009 год компания "Доктор Веб" оперативно выпустила несколько горячих дополнений сканера с графическим интерфейсом, включающего в себя обновлённый антируткит-модуль Dr.Web Shield для противодействия новым руткит-технологиям.

В марте текущего года мы сообщали о том, что очередная модификация **BackDoor.Tdss** препятствует работе файловых мониторов, входящих в состав некоторых антивирусов, а также обходит антируткиты. В то время распространённость **BackDoor.Tdss** была относительно невысокой.

В ноябре 2009 года новые модификации **BackDoor.Tdss** распространились значительно шире. Сервер статистики компании "Доктор Веб" в прошедшем

месяце зафиксировал около 400 000 определений данной вредоносной программы на компьютерах пользователей. До этого момента данная цифра редко поднималась выше 1 000 определений в месяц.

Интересно, что новые модификации **BackDoor.Tdss** злоумышленники стали оснащать инструментами сокрытия в системе. К примеру, специально создаваемый зашифрованный виртуальный диск и механизм обхода некоторых типов поведенческих анализаторов. Несмотря на это специалисты "Доктор Веб" в короткие сроки решили данную задачу, обеспечив продукты компании возможностями корректного лечения **BackDoor.Tdss**.



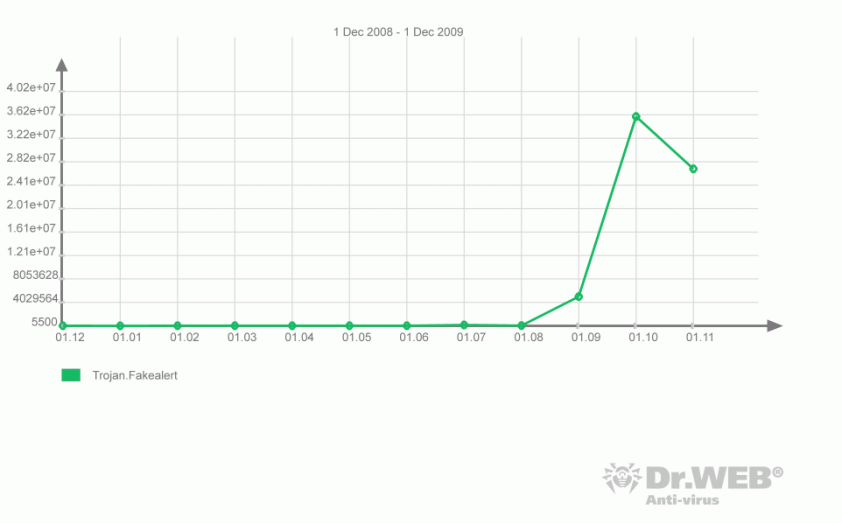
Лжеантивирусы

В последние месяцы уходящего года существенно увеличилась активность распространения лжеантивирусов, которые по классификации Dr.Web называются **Trojan.Fakealert**. Эти программы при запуске внешне похожи на настоящие антивирусные программы, но не являются таковыми. Цель создателей лжеантивирусов - завлечь пользователя на специально подготовленный вредоносный сайт, на котором он должен приобрести якобы полную версию продукта.

Как правило, лжеантивирусы распространяются в виде приложений к спам-письмам или через специально подготовленные вредоносные сайты. При этом чаще всего таким образом передаётся загрузчик лжеантивируса, который при запуске загружает с сервера злоумышленников компоненты, составляющие основной функционал. Упор во вредоносном ПО этого типа делается на визуальную часть – программа отображает системные окна Windows, которые сообщают о том, что данный антивирус якобы интегрирован в систему. Основное окно программы показывает процесс сканирования компьютера и имитирует обнаружение вирусов.

После того, как пользователь заплатит деньги за якобы полную версию такого антивируса, его беды отнюдь не заканчиваются - он остаётся "на крючке", и в систему могут быть загружены какие-либо другие вредоносные объекты.

С сентября 2009 года наблюдается всплеск активности данных угроз - в октябре и ноябре было зафиксировано по несколько десятков миллионов определений программ данного типа. До сентября общее количество обнаруживаемых в месяц лжеантивирусов на компьютерах пользователей было аж на 4 порядка меньше.



Блокировщики Windows

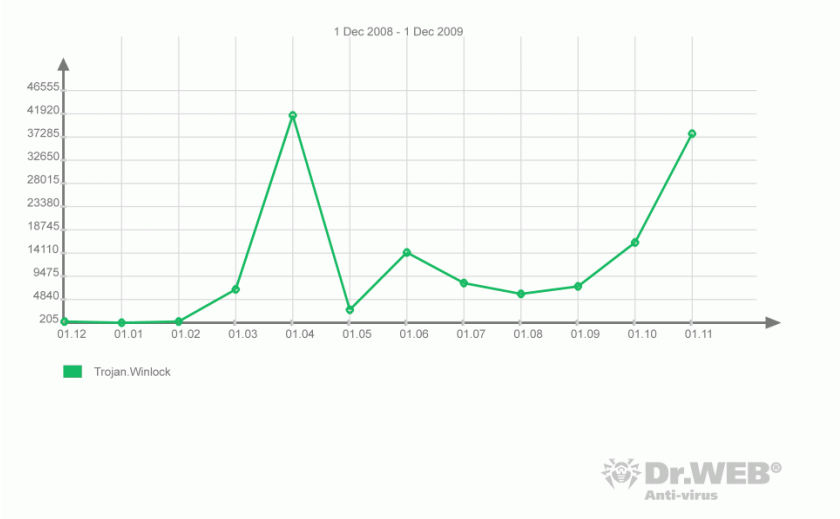
Много бед в 2009 году принесли пользователям и блокировщики Windows – вредоносные программы, которые по классификации Dr.Web называются **Trojan.Winlock**. Эти вредоносные программы при старте Windows выводят поверх всех окон сообщение о том, что доступ в систему заблокирован, и для того, чтобы данное окно исчезло, необходимо отправить платное СМС-сообщение.

В качестве причины блокировки программа могла информировать о том, что на компьютере установлена якобы нелицензионная операционная система или другое программное обеспечение (реже используются другие «поводы»). Известны случаи распространения конструкторов данных вредоносных программ за определённую сумму – приобрести их мог любой желающий.

Несколько лет назад вредоносные программы семейства **Trojan.Winlock** были гораздо безобиднее: в отличие от современных экземпляров они автоматически удалялись с компьютера через несколько часов после установки, если пользователь не совершал никаких действий; не запускались в Безопасном режиме Windows; система действительно разблокировалась в случае ввода правильной строки, а стоимость СМС-сообщений была невысокой.

Последние модификации **Trojan.Winlock** стали более агрессивными. СМС-сообщения для разблокировки существенно подорожали. Некоторые модификации могут и не содержать в себе правильного кода для разблокировки, и, соответственно, пользователь после отправки денег злоумышленникам остается ни с чем. Данные программы не удаляются автоматически из системы по прошествии некоторого времени. **Trojan.Winlock** научился препятствовать запуску множества программ, способных упростить исследование блокировщика на заражённой системе или просто завершающих работу системы при попытке запуска такого ПО.

В случае заражения системы очередной модификацией **Trojan.Winlock** не следует передавать деньги злоумышленникам. Вместо этого необходимо обратиться в техподдержку используемого антивируса или на форум компании "Доктор Веб".

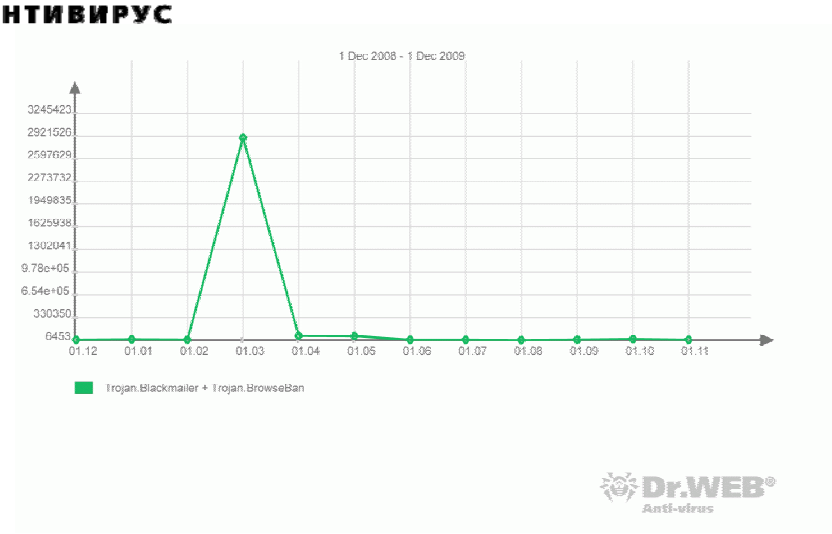


Браузерные баннеры

Ещё одной модификацией троянцев-вымогателей является семейство вредоносных программ, устанавливаемых в качестве дополнения к используемому интернет-браузеру. В результате установки появляется окно, которое может занимать до половины полезной площади окна браузера. Для удаления этого окна требуется отправить СМС-сообщение.

По классификации Dr.Web основная часть таких вредоносных программ определяется как одна из модификаций **Trojan.Blackmailer** или **Trojan.BrowseBan**. Если **Trojan.Blackmailer** устанавливается обычно только в браузер Internet Explorer, то **Trojan.BrowseBan** может устанавливаться в несколько различных популярных браузеров - Internet Explorer, Mozilla Firefox и Opera. Для этого на вредоносных сайтах, с которых распространяется данная вредоносная программа, злоумышленники создают скрипт, который позволяет определять используемый браузер и после этого загружать предназначенную для него модификацию вредоносной программы.

В марте 2009 года был замечен всплеск активности распространения вредоносных программ данного типа. Тогда было зафиксировано около 3 млн. определений **Trojan.Blackmailer** на компьютерах пользователей. В среднем же в течение года количество определений вредоносных браузерных баннеров держалось на уровне 5 000 – 10 000 в месяц.

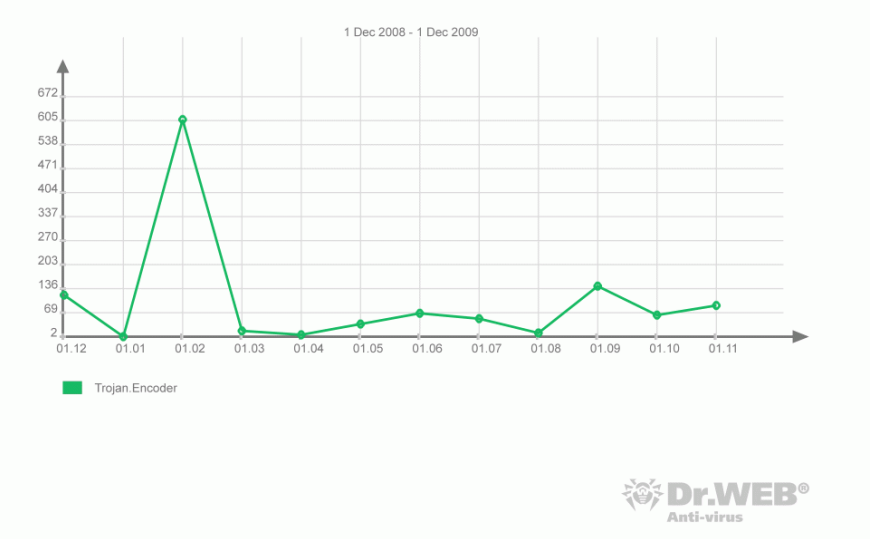


Шифровальщики документов

Очередной проблемой, с которой столкнулись многие пользователи в 2009 году, стали шифровальщики документов – вредоносные программы, которые определяются антивирусом Dr.Web как различные модификации **Trojan.Encoder**. Данная вредоносная программа, проникая в систему, шифрует с помощью определённого алгоритма документы пользователей, не затрагивая файлы, относящиеся к операционной системе. После этого на рабочий стол выводится уведомление о том, что данные пользователя зашифрованы, а для восстановления необходимо перечислить злоумышленникам определённую сумму денег.

Компания "Доктор Веб" столкнулась с фактами использования своей корпоративной атрибутики в материалах одного из авторов **Trojan.Encoder**. Также были зафиксированы случаи распространения спам-сообщений от имени сотрудников компании "Доктор Веб", а некоторые модификации **Trojan.Encoder** использовали дополнительное расширение drweb для зашифрованных файлов. Такое поведение автора **Trojan.Encoder**, видимо, вызвано тем, что специалисты компании "Доктор Веб" успешно оказывают помощь пострадавшим пользователям. Конечно, наша компания не имеет отношения к подобным инцидентам.

Несмотря на относительно малую распространённость вредоносных программ данного типа, при попадании в систему они наносят весьма ощутимый урон – ведь документы часто имеют высокую ценность для пользователей. Пострадавшие от **Trojan.Encoder** всегда могут обратиться в вирусную лабораторию компании "Доктор Веб" – в подавляющем большинстве случаев специалисты помогут в восстановлении зашифрованных документов, причём бесплатно.

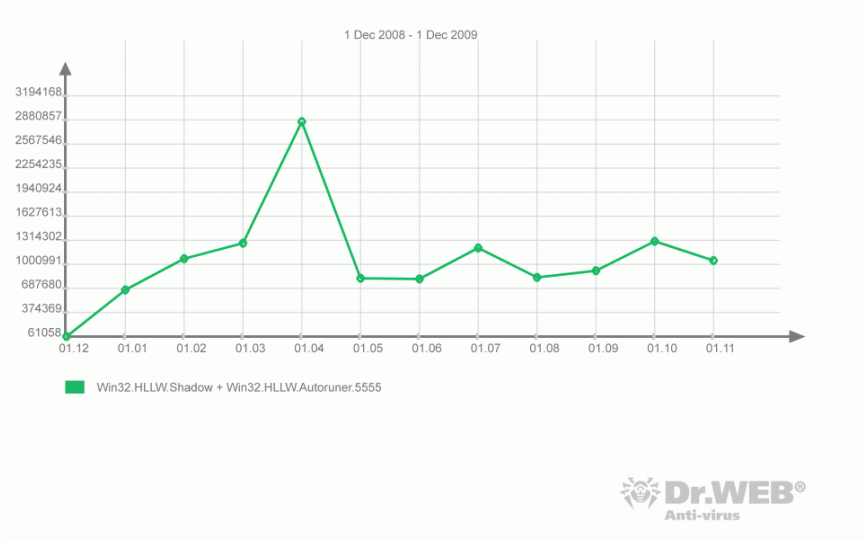


Сетевые черви

Сетевые черви в 2009 году заставили многих администраторов локальных сетей предприятий вспомнить об элементарных правилах информационной безопасности. Наиболее ярким представителем этих вредоносных программ стал сетевой червь **Win32.HLLW.Shadow.based**.

Во-первых, данный червь использует для своего распространения съёмные носители и сетевые диски, напоминая о том, что в современных условиях необходимо отключать автозапуск программ с таких дисков. Во-вторых, данная программа может использовать стандартный для Windows-сетей протокол SMB. При этом она по словарю перебирает наиболее часто встречающиеся пароли, напоминая администраторам сетей о том, что подобные пароли должны быть достаточно сложными – ведь от этого зависит функционирование всей сети. Наконец, **Win32.HLLW.Shadow.based** использует несколько известных уязвимостей Windows-систем. При этом на момент начала активного распространения **Win32.HLLW.Shadow.based** эти уязвимости уже были закрыты производителем. Этот факт говорит о том, что автоматическая установка обновлений на используемую операционную систему никогда не будет лишней потерей интернет-трафика.

Как видно из графика, активное распространение Win32.HLLW.Shadow.based продолжается и сейчас. Данный сетевой червь продолжает своё своеобразное, но весьма эффективное обучение сетевых администраторов.

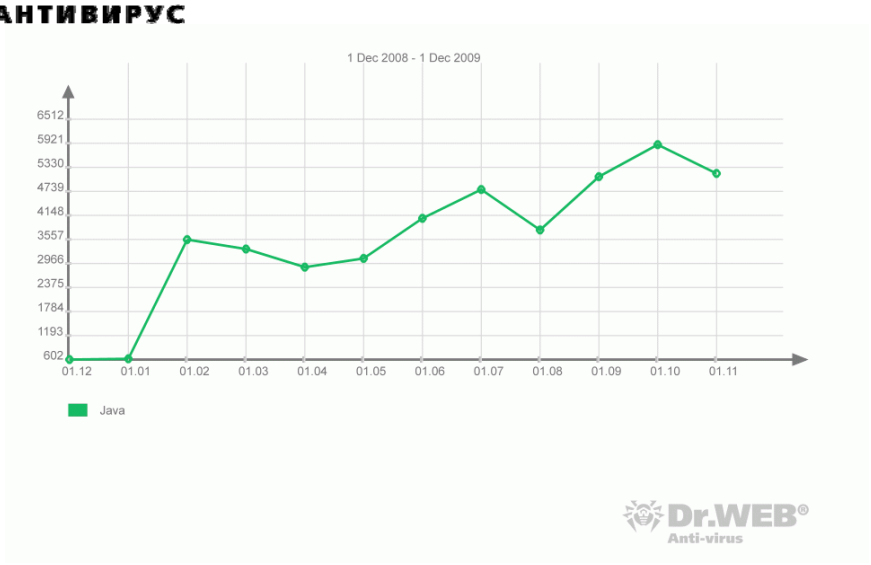


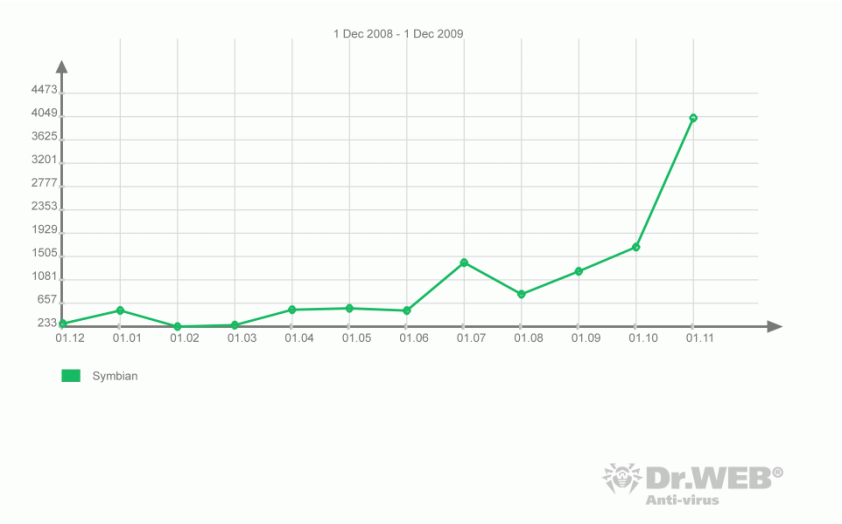
Многообразие программных сред

Как мы упоминали, некоторые вредоносные объекты сегодня уже способны определять используемую операционную систему, браузер, версии другого популярного ПО для того, чтобы более эффективным образом поразить систему. Но для того, чтобы данная схема начала работать, злоумышленникам нужно научиться создавать вредоносные программы, которые смогут работать на большинстве популярных операционных систем. Как обстоят дела на этом фронте?

Если мы обратимся к статистике распространения вредоносных программ по различным платформам за 2009 год, то сможем сделать следующие выводы. Интерес к альтернативным платформам постоянно растёт. Судя по статистике, для таких платформ как Mac OS, Linux, Windows CE тенденция не так очевидна, хотя в новостях часто можно услышать про вредоносные программы под эти системы. А вот к таким мобильным платформам как программная среда Java (которую поддерживают множество мобильных устройств) и Symbian интерес увеличивается с каждым месяцем. Даже несмотря на то, что доля определений вредоносных программ в общем вредоносном трафике по-прежнему весьма мала.

Разработчики компании "Доктор Веб" постоянно следят за развитием ситуации. В частности, в настоящее время в бета-тестировании находится антивирус Dr.Web для Symbian OS, который в скором времени будет доступен всем пользователям смартфонов, работающих под управлением этой ОС.





Прогнозируемые тенденции 2010 года

В 2010 году можно ожидать продолжение тенденции к одномоментному охвату злоумышленниками пользователей как можно большего числа операционных систем и браузеров. Можно предположить, что увеличится количество вредоносных сайтов, на которых будут работать скрипты, способные определять используемую программную среду и в зависимости от этого производить загрузку соответствующей вредоносной программы. Рынок операционных систем постепенно расслаивается – появляются новые ОС, новые мобильные устройства, всё больше пользователей интересуются свободным или альтернативным программным обеспечением, и вирусописатели будут реагировать на эти тенденции, чтобы не упустить свою выгоду.

Следует ожидать, что в последующие годы злоумышленники будут больше времени уделять обходу не только классических сигнатурных и эвристических технологий, но и противодействию различным поведенческим анализаторам, примеры чему мы видим уже сегодня.

Наверняка будет продолжаться разработка новых руткит-технологий, и борьба с ними будет такой же острой, как и в последние годы. Вероятно, уже в 2010 году будут осуществлены первые попытки создать руткит для 64-битной платформы Windows. Многие эксперты утверждают, что это лишь вопрос времени. Весьма вероятно более активное использование полиморфных технологий, которые могут с лёгкостью препятствовать работе так называемых облачных антивирусов. Если распространение вредоносных программ, уникальных в каждом своем экземпляре, будет составлять значительную часть всего вредоносного трафика, это может сделать использование подобных антивирусных технологий крайне неэффективным.

Количеством будут брать и создатели вредоносных сайтов. Уже сегодня антифишинговые технологии, используемые в любом современном браузере и призванные уберечь пользователей от посещения вредоносных сайтов, частенько не справляются с поставленной задачей. Злоумышленники быстро создают слишком много копий одного и того же сайта, и антифишинговые системы просто не успевают сработать на каждый из них.

В заключение приведём несколько рекомендаций, которые помогут существенно снизить риск заражения системы. Для уменьшения вероятности заражения компания "Доктор Веб" рекомендует пользователям организовывать информационную защиту своих компьютеров сразу на нескольких уровнях.

Во-первых, необходимо настроить автоматическое обновление операционной системы и другого ПО, снизив тем самым вероятность использования вредоносными программами известных уязвимостей этого ПО. Во-вторых, необходимо настроить автоматическое обновление антивируса для того, чтобы существенно снизить вероятность заражения системы новыми угрозами. В-третьих, необходимо настроить параметры учётной записи пользователя, под которой осуществляется работа в Интернете, таким образом, чтобы ограничить её возможности по управлению основными настройками системы. Также рекомендуется отключить автоматический запуск программ с внешних дисков.

Для корпоративных пользователей кроме рекомендации использовать в условиях предприятия корпоративные антивирусные продукты мы советуем также принять политику информационной безопасности, а также посвящать хотя бы минимальное рабочее время сотрудников обучению в области элементарных правил ИБ. В частности, можно воспользоваться циклом учебных курсов «Доктор Веб», посвящённых информационной безопасности предприятий с использованием антивирусных продуктов Dr.Web.

Топ-20 вредоносных программ, обнаруженных в 2009 году в почтовом трафике

01.12.2008 00:00 - 01.12.2009 00:00		
1	Win32.HLLM.Netsky.35328	45817344 (16.28%)
2	Trojan.DownLoad.47256	25287535 (8.99%)
3	Win32.HLLM.Beagle	22187775 (7.88%)

4	Trojan.DownLoad.36339	15808084 (5.62%)
5	Trojan.Fakealert.5115	15588235 (5.54%)
6	Trojan.DownLoad.37236	12785630 (4.54%)
7	Win32.HLLM.MyDoom.33808	12283970 (4.37%)
8	Trojan.Fakealert.5238	10516195 (3.74%)
9	Trojan.Packed.683	6970575 (2.48%)
10	Trojan.MulDrop.40896	6932828 (2.46%)
11	Trojan.PWS.Panda.122	6591442 (2.34%)
12	Win32.HLLM.MyDoom.based	6563953 (2.33%)
13	Trojan.DownLoad.50246	5684473 (2.02%)
14	Win32.HLLM.MyDoom.44	4988808 (1.77%)
15	Trojan.Botnetlog.9	4958443 (1.76%)
16	Trojan.Packed.2915	4722719 (1.68%)
17	Trojan.MulDrop.19648	4612563 (1.64%)
18	Win32.HLLM.Netsky.based	4578015 (1.63%)
19	Trojan.Fakealert.5825	4529188 (1.61%)
20	Trojan.Fakealert.5356	4051498 (1.44%)

Всего проверено: 768,599,094,754

Инфицировано: 281,404,910 (0.04%)

Топ-20 вредоносных программ, обнаруженных в 2009 году на компьютерах пользователей

01.12.2008 00:00 - 01.12.2009 00:00		
1	Trojan.DownLoad.47256	15123101 (6.72%)
2	Win32.HLLW.Gavir.ini	13451665 (5.97%)
3	Win32.HLLW.Shadow.based	8168356 (3.63%)
4	Win32.HLLM.Beagle	7552860 (3.35%)
5	Trojan.Fakealert.5115	7111405 (3.16%)
6	Trojan.DownLoad.36339	6896609 (3.06%)
7	Win32.HLLM.Generic.440	6139494 (2.73%)
8	Trojan.Fakealert.5238	5705545 (2.53%)
9	DDoS.Kardraw	5234473 (2.32%)

10	Win32.HLLM.Netsky.35328	4756893 (2.11%)
11	JS.Nimda	4476017 (1.99%)
12	Win32.Virut.14	4199541 (1.87%)
13	Trojan.MulDrop.16727	3682581 (1.64%)
14	Trojan.Botnetlog.9	3350630 (1.49%)
15	Win32.Virut.5	3268197 (1.45%)
16	Win32.HLLW.Autoruner.5555	3234720 (1.44%)
17	W97M.Thus	3202955 (1.42%)
18	Win32.Alman	3025843 (1.34%)
19	Win32.Sector.17	2966478 (1.32%)
20	Win32.HLLM.MyDoom.49	2907279 (1.29%)

Всего проверено: 2,289,643,009,454

Инфицировано: 225,141,202 (0.01%)

-конец-

За дополнительной информацией обращайтесь:
Кирилл Леонов
k.leonov@drweb.com
+7 (495) 789-4587 доб. 651

О компании «Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности. Компания предлагает эффективные антивирусные и антиспам-решения как для крупных компаний и государственных организаций, так и для частных пользователей. Антивирусные продукты Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности. Сертификаты и награды, а также обширная география пользователей Dr.Web свидетельствуют о степени исключительного доверия к продуктам компании.

www.drweb.com