ВирусБлокАда

# Анализ вирусной активности за 2011 год

Александр Изотов,
вирусный аналитик
ООО «ВирусБлокАда»

**Справка ТБ**

*Александр Изотов, выпускник Белорусского государственного университета (факультет Радиофизики и компьютерных технологий), вирусный аналитик компании «ВирусБлокАда» с 2010 года.*

Антивирусная лаборатория компании «ВирусБлокАда» проанализировала вирусную активность за 2011 год на основе обращений в службу технической поддержки компании.

На основе полученной информации можно выделить следующие тенденции 2011 года:

1) использование социальной инженерии;
2) отклик на мировые события;
3) использование уязвимостей;
4) появление специализированных угроз;
5) развитие технологий сокрытия.

Наиболее популярной тенденцией является использование социальной инженерии, которая базируется на незнании основ информационной безопасности. Это явление широко распространено в Интернете для получения конфиденциальной информации или информации, которая представляет большую ценность. Для злоумышленника становится гораздо проще хитростью выудить информацию из системы, чем взломать ее. В связи с этим в 2011 году появилось большое количество вредоносных программ, которые реализуют принципы социальной инженерии.

• В очередной раз заставил обратить на себя внимание **Trojan.Winlock**, блокирующий работу ОС Windows. Следует заметить, что семейство Trojan.Winlock существует еще с 2007 года. Лето 2011 года ознаменовалось появлением «национального» экземпляра Trojan.Winlock, ориентированного на белорусских пользователей Windows и требующего у них перечислить злоумышленникам некоторую сумму в белорусских рублях на электронный кошелек WebMoney. Главные причины широкого распространения этой угрозы — невнимательность либо некомпетентность пользователей, оказывающихся жертвами вымогателей.

• Наблюдалась и активность **ArchSMS** (фальшивого самораспаковывающегося архива). Как правило, вредоносная программа загружается пользователем из сети Интернет под видом самораспаковывающегося архива (исполняемого файла), содержащего требуемый пользователю файл. Пользователь, запустив исполняемый файл, наблюдает на мониторе процесс, похожий на распаковку. Но в определенный момент «распаковка» останавливается, появляется сообщение о том, что для окончания распаковки архива необходимо отправить с мобильного телефона платное SMS-сообщение. При этом размер самого файла близок к «оригиналу» запрашиваемой информации.

• С середины 2011 года наблюдалось значительное уменьшение количества фальшивых антивирусов (**FakeAV**), программ, которые находят на компьютере пользователя множество несуществующих вирусов и для «чистки» машины предлагают активировать себя через SMS на определенный номер. Количество фальшивых антивирусов постепенно начало переходить в качество. Отдельные вирусописатели организуют кибергруппы и пишут уже меньшее количество фальшивых антивирусов, но пытаются сделать их более совершенными — более подобными на настоящие, чтобы пользователь, который незнаком с особенностями работы реальных антивирусов, попадался на данные уловки.

Следующей значимой тенденцией является отклик на мировые события. Спамеры традиционно используют интерес пользователей к событиям, имеющим широкий общественный резонанс, в своих корыстных целях. И последние месяцы 2011 года также не стали исключением. Так, после смерти 5 октября основателя компании Apple Стива Джобса мошенники распространяли информацию о бесплатных устройствах iPad «в память о Стиве Джобсе». Пройдя по ссылке, предложенной злоумышленниками, пользователей перенаправлялись на вредоносные сайты.

Использование уязвимостей является одной из самых динамичных тенденций. Новым направлением стало активное использование злоумышленниками уязвимостей платформы Java, являющейся самым слабым элементом в защите операционных систем, на которых она установлена. В этом году хакеры, как и в предыдущие годы, активно использовали уязвимости в веб-приложениях, в IIS, MS SQL, а также системах обработки файлов и сервисах сообщений операционной системы.

Еще одной тенденцией являются специализированные угрозы, цель которых — проведение шпионажа. В конце 2011 года отмечено много ярких примеров данного направления.

• В октябре появились сообщения о повышенной активности червя **Duqu**, который имеет сходство с компьютерным червем **Stuxnet** (впервые обнаруженным компанией «ВирусБлокАда» летом прошлого года). Главная задача Duqu — сбор конфиденциальных данных об имеющемся на предприятии оборудовании и системах, используемых для управления производственным циклом. Это может быть любая информация, которая пригодится при организации нападения: снимки с экрана, журналы нажатых клавиш, список запущенных процессов, данные учетных записей пользователей, названия открытых окон, сетевая информация, сведения о домене, имена дисков, файлов и пр.

• Также в октябре была обнаружена программа **Bundestrojaner**, которая по своей природе аналогична вирусу, следит за Интернет-браузером и такими программами, как Skype, электронная почта и чаты. Немецкие госслужбы использовали эту шпионскую программу около 100 раз, заявил представитель фракции ХДС-ХСС в парламенте Германии Ганс-Петер Уль в интервью Neue Osnabruecker Zeitung. Программа может делать снимки с экрана, которые в немецких судах рассматриваются в качестве доказательств. Помимо прослушки телефонных разговоров и слежки за пе-

*Продолжение см. стр. 57*

*Начало см. стр. 56*

рeпиской, на зараженном компьютере можно дистанционно включить микрофон или веб-камеру. Таким образом, полиция способна прослушать и увидеть, что происходит в помещении, где стоит ПК. Данные события представляют собой примеры промышленного и правительственного шпионажа.

За 2011 год соотношение вредоносного ПО выглядит следующим образом:

Наибольший объем (44%) занимает Trojan. BackDoor/Downloader/Dropper, Trojan.Injector и т.д. Они имеют различные технологии внедрения и существования в ОС. Следующей крупной группой, составляющих 38 %, являются FraudTool (мошеннические программы). Это те виды вредоносных программ, к которым относятся фальшивые антивирусы, трояны, блокирующие работу систем (FakeAV, ArchSMS, Winlock , Ransom Encoder, Trojan.Cidox). Крупной группой, занимающей 9 % от общего количества вредоносных программ, является **Adware**. Adware — это программное обеспечение, содержащее рекламу или же предназначенное для показа рекламных сообщений. В большинстве случаев Adware скрытно инсталлируется в систему с какой-нибудь бесплатной или условно бесплатной программой, после чего удалить его, как правило, не представляется возможным, так как Adware-модуль маскируется в системе, используя технологии, близкие к вредоносному ПО. Базовое назначение Adware — это неявный метод оплаты использования бесплатного программного обеспечения, рекламодатели платят за показ их рекламы рекламному агентству, рекламное агентство — разработчикам Adware-программ. Доля сетевых червей составляет около 5 %. В 2011 г. мошеннические программы, трояны и Adware имели положительную динамику. Соответственно, из-за их роста объем всех остальных вредоносных программ в этот период сокращался.

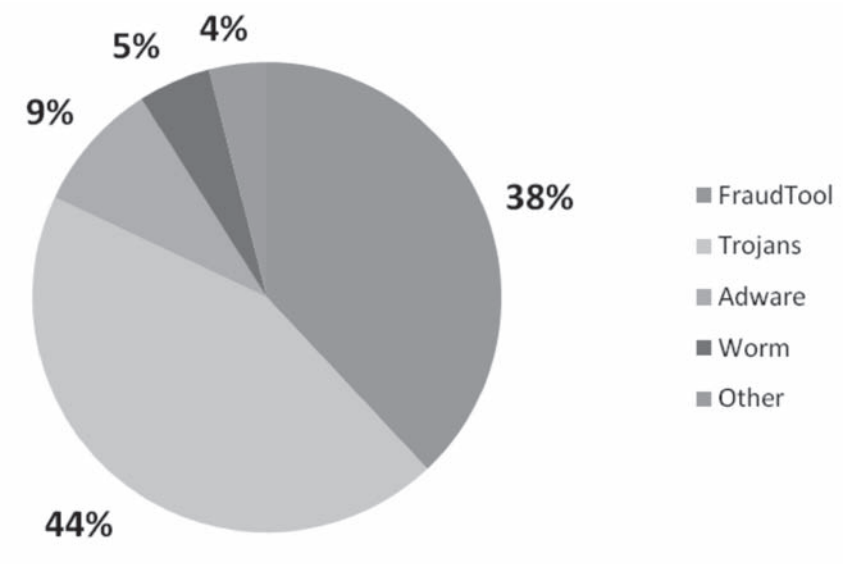


**Рисунок 1. Распределение вредоносных программ по типам**

Таким образом, на основе анализа вирусной активности в 2011 году можно сделать некоторые выводы. Динамика роста вредоносных программ остается постоянной, можно наблюдать устойчивость тенденций еще с 2010 г. Вирусы и трояны усложняются, увеличивается масштаб их распространения, а также скорость, с которой они поражают компьютеры пользователей. В 2011 году, как и прогнозировалось, увеличилось число угроз, работающих на 64-битных платформах. Люди, как и прежде, остаются самым уязвимым звеном в обеспечении информационной безопасности. ■

**Белорусская антивирусная компания «ВирусБлокАда»**
**220088, г.Минск, ул. Смоленская, 15 - 803б**
**Тел.: (+375 17) 294-84-29 (коммерческий отдел),**
**290-59-29 (технический отдел)**
**E-mail: info@anti-virus.by**
**Сайт: www.anti-virus.by**