Обзор вирусных программ. Современные тенденции.

Топорков С.Д.

414 группа

Продолжают увеличиваться темпы роста численности вредоносных программ, тысячи новых вариантов которых обнаруживаются каждый день. Этот процесс постепенно начинает сопровождаться и ростом их технологической сложности, а также смещением вектора атаки в сторону тех областей информационной безопасности, которые пока не защищены в той же мере, что и традиционные – как технологии Web 2.0, так и мобильные устройства. Наверное, именно в первом квартале 2008 года и произошла символическая, но окончательная, смерть «старой школы» вирусописательства. Никто уже не создает вредоносные программы для самовыражения, самоутверждения или исследований – гораздо более выгодно генерировать сотни примитивных троянских программ на продажу.

Буткит

Именно буткиты - руткиты с функцией загрузки из бут-секторов любых устройств - стали главной проблемой антивирусной индустрии в начале 2008 года.

Принцип их действия достаточно прост, используются алгоритмы запуска операционной системы при включении или перезагрузке компьютера - программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление. Если в загрузочном секторе находится вирус, управление получает он.

Заражение дискет производится единственным известным способом — вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами — вирус записывается либо вместо кода MBR *(Главная загрузочная запись (англ. master boot record, MBR) — это первый физический сектор на жёстком диске или другом устройстве хранения информации.)*, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR винчестера. При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный).

В самом начале 2007 двое индийских программистов Nitin и Vipin Kumar представили Vbootkit – руткит с функцией загрузки из бут-секторов любых устройств, способный работать в Windows Vista. Исходный код разработки не был опубликован, но был доставлен в некоторые антивирусные компании.

Общий принцип работы Vbootkit выглядит примерно так:

BIOS --> Vbootkit code(from CD,PXE etc.) --> MBR --> NT Boot sector --> Windows Boot manager --> Windows Loader --> Vista Kernel.

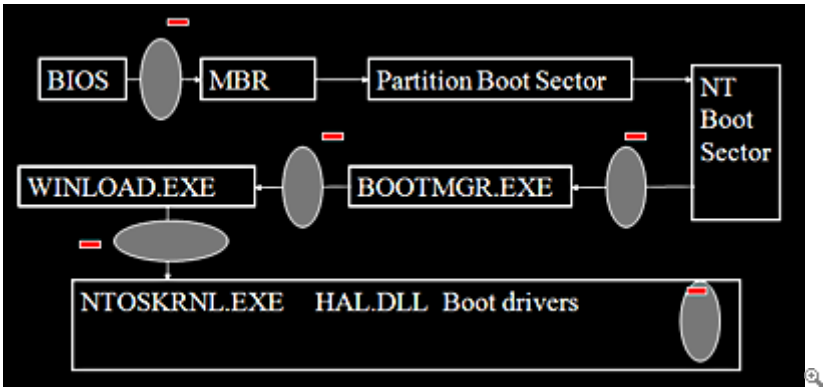

Схема загрузки системы, пораженной буткитом. Серые области показывают места, где буткит перехватывает управление на себя

В следующей версии буткита авторы обещали реализовать и заражение BIOS.

Собственно, произошло то, что должно было произойти – старая технология заражения бут-секторов пересеклась с модой на руткиты. Несмотря на то, что практически все современные антивирусные программы имеют функцию сканирования загрузочных секторов дисков, проблема обнаружения перехваченных и подмененных системных функций остается весьма актуальной и по сей день и не решена окончательно даже в рамках работы троянца и антивируса в одной ОС, не говоря уже о бэкдоре, стартующем до операционной системы.

Выглядело это все, как гремучая смесь, которая в любой момент может взорваться. Она взорвалась в ноябре 2007 года. Хотя узнали об этом чуть позже - в конце декабря, когда несколько тысяч пользователей (точных

данных о числе зараженных нет) могли стать объектами атаки со стороны первой вредоносной реализации идеи загрузочного руткита.

Загрузочный руткит

В период с 19 по 28 декабря в Интернете появилось несколько веб-сайтов, которые производили при помощи техники drive-by-download (заражение с помощью размещенных на веб-сайтах эксплойтов) загрузку вредоносной программы. Детальный анализ этой программы выявил, что мы столкнулись с кодом, способным поражать MBR и сектора жесткого диска. Вредоносный код после попадания на компьютер изменяет MBR, записывает руткит-части в сектора диска, извлекает из себя и устанавливает бэкдор в Windows после чего самоудаляется.

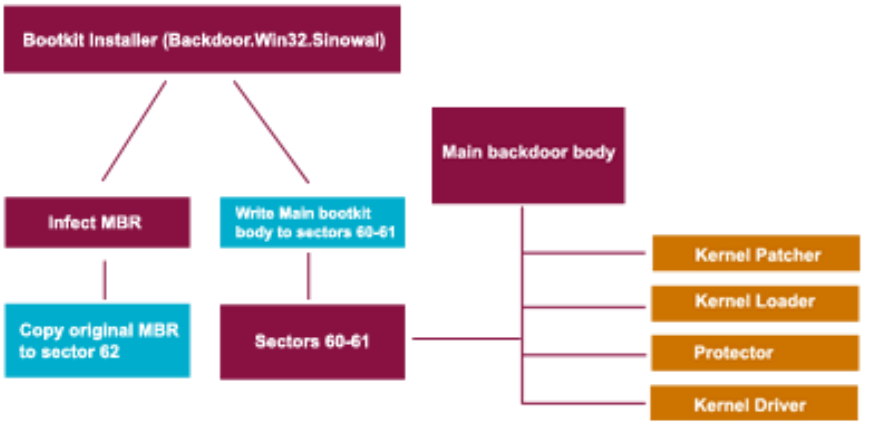

Схема работы инсталлятора буткита

При заражении в MBR размещаются инструкции, передающие управление основной части руткита, помещенной в нескольких секторах жесткого диска и не имеющей представления в виде файлов в системе. Эта часть затем контролирует уже загруженную операционную систему Windows и при чтении путем перехвата и подмены системных функций скрывает зараженный MBR и «загрязненные» сектора, подставляя вместо них чистые.

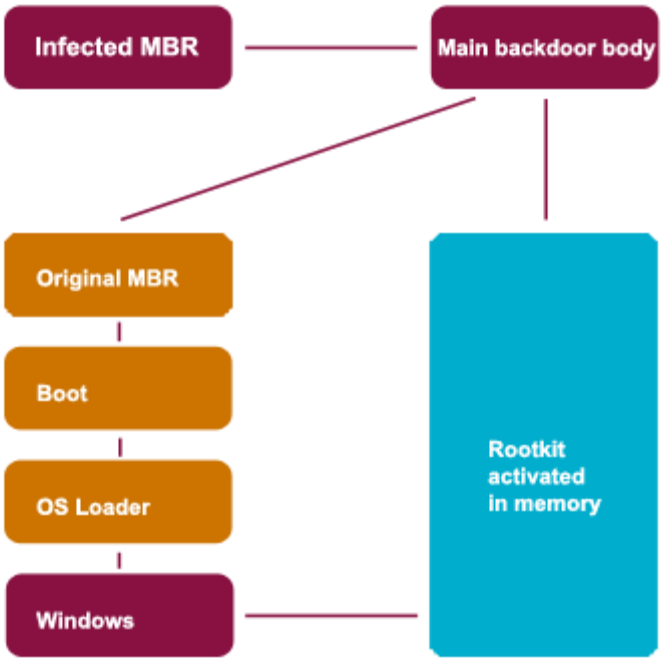

Схема работы зараженной операционной системы

Помимо сокрытия своего присутствия в системе, вредоносный код устанавливает в Windows бэкдор, который занимается также кражей информации - в том числе аккаунтов доступа к ряду банковских систем.

Вредоносная программа, несущая функционал буткита и бэкдора, была классифицирована Лабораторией Касперского как Backdoor.Win32.Sinowal, поскольку многие функции в бэкдоре, а также использованная методика «замусоривания» кода были идентичны тем, которые мы давно знаем по шпионской программе Trojan-PSW.Win32.Sinowal.

Несмотря на все ухищрения и новшества, реализованные в бутките, он мог защитить только самого себя, оставляя файл бэкдора полностью доступным для детектирования и удаления. Тем не менее, буткит выглядит как некая самодостаточная платформа, которая может быть легко добавлена к любой существующей вредоносной программе для ее защиты и сокрытия. Это означает, что не исключено скорое появление буткита на продажу, в результате чего технология станет доступной тысячам script-kiddies, и - учитывая текущие темпы роста числа вредоносных программ – может оказаться одной из наиболее распространенных угроз.

Проблемы защиты от буткитов

Что же конкретно представляет сложность в борьбе с буткитами?

Основных проблем несколько:

1. Вредоносный код получает управление еще до старта ОС, а значит и антивирусной программы
2. Перехват функций сложно обнаружить, находясь внутри зараженной ОС.
3. Восстановление перехваченных функций может приводить к сбою всей ОС.
4. Лечение MBR возможно только при обнаружении оригинального MBR.

Понятно, что самым эффективным способом защиты является недопущение заражения системы изначально – ведь буткит из воздуха не берется, и сначала ему необходимо как-то попасть на компьютер. Некоторые антивирусные программы способны предотвратить заражение, даже новыми, еще неизвестными вариантами вредоносов. Однако, вероятность пробивания такой защиты все равно существует, и так или иначе мы приходим к необходимости излечения уже зараженного компьютера.

Здесь возможны два варианта – либо антивирус уже стоит в системе (и тогда для него актуальны все четыре пункта, приведенных выше), либо антивируса в системе не было, и его необходимо установить. Во втором случае мы сталкиваемся с еще одной проблемой, которая вытекает из пункта 1, а именно: вредоносный код может блокировать попытки установки антивируса в систему.

Вирусописатели проанализировали, каким образом антивирусные компании решают перечисленные выше проблемы, и в феврале 2008 года выпустили новую, усиленную версию буткита. В результате реализованные на тот момент методы противодействия буткитам вновь оказались бесполезными. Одновременно с этим, началась и новая стадия распространения буткита. Ссылки на сайты с эксплоитами, устанавливающими буткит, были обнаружены на нескольких взломанных европейских сайтах. Пока еще не зафиксировано других - кроме Sinowal - вредоносных программ, оснащенных буткитом.

Ключевой вопрос – кто первый получает управление? Если первым оказывается вирус, антивирус априори будет бесполезен.

Итак, вирусы добрались (снова) до главной загрузочной записи. 10 лет назад мы решили эту проблему при помощи загрузочных дискет с антивирусом. Похоже, что наступает время возвращения старых технологий не только для зловредов, но и для антивирусных программ.

Шторм продолжается

В середине января 2008 года исполнился год с появления в Сети первых экземпляров того, что впоследствии получило названия Zhelatin, Nuwar и Storm Worm. До этого история еще не знала примеров столь динамично и разнообразно развивающихся вредоносных программ.

Zhelatin оказался достойным продолжателем идей и концепций, ранее реализованных в червях Bagle и Warezov. У первого Zhelatin позаимствовал модульность структуры, у второго - частоту появления новых вариантов, отказ от рассылки основного функционала по электронной почте, использование сотен зараженных сайтов для распространения и распространение через Skype и IM. К этому были добавлены социоинженерные трюки, руткит-технологии, методы обратной атаки на антивирусные компании и децентрализованный ботнет. И менее чем за год Storm Worm стал главной проблемой информационной безопасности - в первую очередь, из-за своего почти мифического ботнета.

Точные размеры «штормового» ботнета так и остались загадкой. В 2007 году нам приходилось слышать самые разнообразные оценки числа зараженных машин, причем в одно и тоже время. Так, например, в сентябре одни эксперты считали, что в ботнет входит два миллиона машин, другие полагали, что число зараженных машин составляет от 250 000 до миллиона, третьи оценивали размеры ботнета в 150 000 машин. Были и такие, кто говорил о 50(!) миллионах инфицированных компьютеров. Собственно, причины таких расхождений очевидны – из-за децентрализации ботнета невозможно установить точное число зомби-машин. Можно оперировать только косвенными показателями, которые весьма спорны.

Так или иначе, но «штормовой» ботнет существовал. И при этом бездействовал. Никакой «классической» активности ботнета зафиксировано не было: он не был замечен ни в организации спам-рассылок, ни в проведении DDoS-атак (что, впрочем, не исключает возможности его коммерческого использования киберкриминалом другими способами). Складывалось впечатление, что никаких задач, кроме распространения Storm Worm (рассылка новых писем со ссылками на зараженные сайты и размещение на зараженных компьютерах модулей для загрузки на компьютеры новых жертв), ботнет не решает. И было совершенно непонятно, с какой целью он создается. Ботнет ради самого ботнета? Но так не бывает - слишком значительные ресурсы требуются на его создание и поддержание.

Примерно с октября 2007 года активность рассылок Zhelatin стала несколько снижаться. Эксперты, ранее говорившие о миллионах зараженных машин, стали ограничивать размеры «штормового» ботнета до 150-200 тысяч компьютеров. Появились предположения, что ботнет готов к продаже по частям. Появились и первые зафиксированные случаи рассылки спама с компьютеров, пораженных Storm Worm. Однако нельзя однозначно утверждать, что спам рассылался именно через его ботнет, а не при помощи каких-то других вредоносных программ, которые также могли иметься на зараженных компьютерах.

Ответ на вопрос, что происходит со «Штормовым» червем, дали конец 2007 года и первые месяцы 2008.

На Рождество он вернулся. Ботнет начал рассылку миллионов писем с заголовками вроде "Find Some Christmas Tail," "Warm Up this Christmas" и "Mrs. Clause Is Out Tonight!", заманивая пользователей на сайт merrychristmasdude.com, где были установлены эксплоиты, использующие технику drive-by-download для загрузки на компьютеры жертв Storm Worm. На самом деле сайт merrychristmasdude.com не был каким-то одним сайтом, который можно было бы оперативно закрыть и остановить инфекцию. Zhelatin в полной мере использовал методику fast-flux смены DNS-адреса, постоянно меняя реальное расположение сайта между более чем 1000 подготовленными компьютерами.

Подобные атаки с небольшими вариациями повторялись в течение еще нескольких дней, вплоть до 15 января, когда случилось нечто странное. То ли это было шуткой авторов, то ли они действительно ошиблись, но ботнет стал рассылать письма с «валентиками», хотя до дня Святого Валентина оставался еще месяц!

Your download should begin shortly. If your download does not start in 10-20 seconds, you can click here to launch the download and then press Run. Enjoy!

«Валентинка», разосланная со штормового ботнета в январе

Письма с заголовками «Sent with Love», «Our Love is Strong», «Your Love Has Opened» и так далее, вновь заводили пользователей на очередной fast-flux сайт.

Январские рассылки оказались наиболее массовыми и заметными не только в первом квартале 2008 года, но и превзошли показатели второй половины 2007 года. Несколькими мощными ударами авторы Zhelatin, несомненно, вернули размеры своего ботнета к прежнему состоянию, а то и превзошли его. Компьютеры, пораженные им, стали встречаться в некоторых DoS-атаках, а компания MessageLabs стала

считать «штормовой» ботнет ответственным почти за 20% всего рассылаемого в настоящее время в Сети спама.

TrojanGet

Инциденты информационной безопасности, в которых легальное ПО и софтверные компании становятся распространителем инфекции, довольно редки, но все же случаются. В историях прошлых лет рассказывается то о зараженных дистрибутивах, то об инфицированных файлах документов, рассылаемых клиентам-партнерам.

Каждый такой инцидент наносит сильный удар по репутации ПО или компании, затрагивает пользователей, соблюдающих базовые правила компьютерной безопасности, и доставляет проблемы антивирусным компаниям, которые воспринимают легальный софт и источники его получения как изначально доверенные. Первый квартал 2008 года вписал еще одну главу в хронику подобных событий.

В начале марта эксперты столкнулись с обращениями пользователей по поводу наличия у них троянских программ в каталоге популярного клиента-загрузчика FlashGet. Анализ ситуации показал, что проблема существует у пользователей этой программы по всему миру. Основными симптомами является появление в системе файлов с именами inapp4.exe, inapp5.exe, inapp6.exe, детектируемых Антивирусом Касперского как Trojan-Dropper.Win32.Agent.exo, Dropper.Win32.Agent.ezo и Trojan-Dowloader.Win32.Agent.kht.

Ситуация выглядела очень странной, т.к. никаких других троянских программ, через которые они могли попасть в систему, не обнаруживалось. У некоторых из пострадавших пользователей были установлены все патчи для операционных систем и браузеров. Каким же образом вредоносные программы проникали на компьютеры? Внимание сразу привлекло месторасположение троянцев — каталог самого FlashGet. Проверка выявила, что кроме троянцев свежую дату создания и модификации имеет файл FGUpdate3.ini (курсивом выделены отличия от оригинального файла):

```
[Add]
fgres1.ini=1.0.0.1035
FlashGet_LOGO.gif=1.0.0.1020
inapp4.exe=1.0.0.1031
[AddEx]
[fgres1.ini]
url=http://dl.flashget.com/flashget/fgres1.cab
flag=16
path=%product%
[FlashGet_LOGO.gif]
url=http://dl.flashget.com/flashget/FlashGet_LOGO.cab
flag=16
path=%product%
[inapp4.exe]
url=http://dl.flashget.com/flashget/appA.cab
flag=2
path=%product%
```

Ссылка на файл inapp4.exe, являющийся троянцем, вела на настоящий сайт FlashGet. Именно оттуда он загружался в виде appA.cab.

Никакой информации об инциденте на сайте FlashGet обнаружено не было, зато изучение форума пользователей программы выявило множество сообщений о случаях заражения и полное молчание со стороны разработчиков.

Судя по информации, найденной в Сети, первые случаи заражения были зафиксированы еще 29 февраля. Последний известный нам на тот момент — 9 марта. 10 дней легальная программа выступала в роли троянца-загрузчика, осуществляя установку и запуск в системах пользователей троянских программ, размещенных на сайте компании-производителя! Спустя менее чем две недели, 22 марта, сайт Flashget и сама программа очередной раз стали распространять вредоносный код. Способов, при помощи которых FlashGet может быть превращен в троянца-загрузчика, два.

Первый способ самый очевидный - взлом сайта компании-производителя. Именно в результате такого взлома злоумышленникам удалось подменить стандартный файл конфигурации на файл, указывающий на троянскую программу, размещенную там же. Почему хакеры не использовали другой сайт, мы не знаем — возможно, для лучшей маскировки (ссылка на сайт FlashGet в конфиг-файле может не вызвать подозрений).

Можно ли использовать этот трюк для загрузки любых других файлов с любых других сайтов? Ответ — да. Достаточно добавить в файл FGUpdate3.ini собственную ссылку на что угодно, и это «что угодно» будет автоматически загружено и запущено на вашем компьютере при каждом запуске FlashGet. Даже если вы не нажимаете кнопку «Обновить», FlashGet самостоятельно использует информацию из ini-файла!

«Уязвимость» существует во всех версиях FlashGet 1.9.xx. Это означает, что хотя на данный момент проблема с взломом сайта FlashGet может быть решена, уязвимость в системе пользовательской безопасности остается. Любая троянская программа может изменить локальный ini-файл FlashGet, заставив его ыполнять функции троянца-загрузчика. И этот способ является вторым из двух упомянутых выше.

Социальные черви

По некоторым прогнозам, в 2008 году пользователи социальных сетей станут основной мишенью фишинга. Учетные данные абонентов таких сервисов, как Facebook, MySpaces, Livejournal, Blogger и аналогичных им, будут пользоваться повышенным спросом у злоумышленников. Это станет опасной альтернативой методике размещения вредоносных программ на взломанных сайтах. В 2008 году множество троянских программ будут распространяться именно через аккаунты пользователей социальных сетей, через их блоги и профили. Февраль 2008 года показал справедливость подобных ожиданий. В очередной раз объектом атаки стала популярная социальная сеть Orkut, принадлежащая Google.

Orkut пользуется громадной популярностью в ряде стран мира – в первую очередь, в Бразилии и Индии. Согласно информации сервиса Alexa.com, в настоящий момент более 67% обращений к Orkut происходит из Бразилии, на долю Индии приходится более 15%. В Бразилии очень популярен онлайн-банкинг. В Бразилии очень популярен Orkut. В Бразилии очень много вирусописателей. Эти три фактора могли привести только к одному – к появлению червя, распространяющегося через Orkut и крадущего аккаунты доступа к банковским системам.

Список вредоносных программ в Orkut, пожалуй, самый обширный среди всех социальных сетей. В 2006 и 2007 годах там уже случались вирусные эпидемии, в 2005-2007 годах Orkut становился объектом хакерских атак, и в нем было обнаружено множество уязвимостей. Последним громким инцидентом стало появление скрипт-червя в декабре 2007 года, в результате чего было заражено около 700 000 пользователей.

Спустя два месяца, в феврале 2008 года произошла новая эпидемия. На этот раз хакеры не стали мучаться с поиском и использованием XSS-уязвимостей в Orkut. Схема работы нового червя была довольно простой:

1. Пользователь получает сообщение от одного из своих контактов, содержащее порно-картинку, реализованную в виде флеш-ролика.
2. При нажатии на нее происходит переадресация на вредоносный сайт.
3. Пользователю предлагается установить проигрывать флеш-роликов, на самом деле являющийся троянской программой.
4. После загрузки и запуска троянец загружает из Сети на пораженный компьютер еще ряд своих компонентов.
5. Аккаунт пользователя используется для создания новых сообщений, аналогичных описанному в пункте 1.
6. Вредоносный модуль отслеживает обращения пользователя к сайту Orkut.
7. Прочие модули занимаются перехватом вводимой с клавиатуры информации при обращении пользователя ко многим бразильским банковским сайтам.

Точное число пострадавших в ходе этой атаки установить невозможно, однако Symantec сообщает о минимуме в 13 000 пользователей.

Данный инцидент очередной раз показывает, насколько уязвимы могут быть пользователи социальных сетей. Основными факторами, обеспечивающими одновременный интерес пользователей и хакеров к сервисам Web 2.0, являются:

- Миграция пользовательских данных с персонального компьютера в Сеть
- Использование одного аккаунта для нескольких разных сервисов
- Детальная информация о пользователе
- Информация о его связях, контактах и знакомых

- Место для публикации чего угодно
- Доверительные отношения между контактами

Проблема достаточно серьезна уже сейчас и имеет все шансы стать главной проблемой информационной безопасности.

Мобильные новости

Новостей из мира мобильной вирусологии в первом квартале 2008 года было довольно много. Налицо продолжающийся прогресс технологий и все большее число участников этого процесса – как среди вирусописателей, так и среди антивирусных компаний.

Вредоносные новинки примерно поровну распределились между четырьмя основными мишенями мобильных угроз – ОС Symbian, Windows Mobile, J2ME и iPhone.

Symbian

Что касается Symbian, то здесь мы получили очередного червя из нового самостоятельного семейства. До сих пор нам были известны только два основоположника жанра – распространяющийся через Bluetooth червь Cabir и распространяющийся через MMS червь ComWar, а также различные их модификации.

В конце декабря в антивирусные базы попал, казалось бы, очередной клон ComWar. Однако его появление в январе в мобильном трафике одного из крупных мобильных операторов заставило более детально взглянуть на новый образец.

Анализ, проведенный финской компанией F-Secure, показал, что на самом деле это совершенно новое семейство, не имеющее общих корней с созданным три года назад в России ComWar. Принцип действия червя, классифицированного как Worm.SymbOS.Beselo.a (чуть позже был обнаружен еще один вариант – Beselo.b), очень схож с ComWar и является классическим для червей такого типа. Распространение происходит через рассылку инфицированных SIS-файлов по MMS и через Bluetooth. После запуска на атакуемом устройстве червь начинает рассылать себя по адресной книге смартфона, а также на все доступные устройства в радиусе действия Bluetooth.

Собственно новостью является именно сам факт появления нового активного семейства мобильных червей (а значит и активного вирусописателя) и наличие этого червя в «дикой природе». Не исключено, что новые модификации Beselo могут привести к серьезным локальным эпидемиям, как это случилось весной прошлого года в Валенсии, когда 115000 пользователей смартфонов оказались жертвами испанской модификации червя ComWar.

Windows Mobile

Обнаружение в конце февраля троянца InfoJack.a интересно по ряду причин.

InfoJack.a:

1. атакует Windows Mobile;
2. обнаружен в «дикой природе»;
3. распространяется в Китае;
4. занимается кражей информации.

Эта троянская программа для Windows Mobile попала в «дикую природу» и вызвала множественные заражения пользователей. Распространение происходило с одного из китайских сайтов, размещающего различный софт (легальный). Троянец был добавлен в состав дистрибутивов мобильных продуктов, таких как клиент для Google Maps и игры. Владелец сайта, с которого происходило распространение троянца, заявил, что он не преследовал никаких криминальных целей, а производил сбор информации о своих посетителях только с целью улучшения сервиса и анализа рынка мобильных приложений.

Попав в систему, троянец пытается отключить защиту от установки приложений, не содержащих цифровой подписи производителя. После того как зараженный смартфон подключается к Интернету, InfoJack начинает отсылать на собственный сайт приватную информацию с телефона - серийный номер телефона, информацию об операционной системе, установленных приложениях. Одновременно он может загружать на

телефон дополнительные файлы и запускать их (без уведомления пользователя, поскольку защита от запуска «неподписанных» приложений отключена).

Китай стал первой страной, пострадавшей от Windows Mobile троянца. Возможно, автор InfoJack действительно не преследовал криминальных целей, но начало положено, и его пример может оказаться заразительным для тысяч китайских хакеров, сейчас создающих вирусы для персональных компьютеров.

J2ME

В первом квартале 2008 года троянцы для J2ME (работающие практически на любом современном мобильном телефоне, а не только на смартфонах) появлялись с пугающей периодичностью. В январе был обнаружен Smarm.b, в феврале - Smarm.c и Swapi.a, в марте - SMSFree.d.

Все они были обнаружены в России и используют один и тот же способ зарабатывания денег на пользователях – отправку SMS на платные premium-номера. (Исследование инцидента с SMS-троянцем Viver, показало, что всего за три дня автор троянца мог заработать около 500 долларов США.) Несмотря на все инциденты, российские мобильные контент-провайдеры продолжают сохранять высокий уровень анонимности для всех регистраторов premium-номеров, что приводит к безнаказанности вирусописателей – появление новых вариантов вредоносных программ и отсутствие информации об аресте кого-либо из их авторов очень хорошо это подтверждают.

Кроме перечисленных выше троянцев для J2ME, рассылкой платных SMS занимаются еще два зловреда, реализованных на языке Python и предназначенных для смартфонов - Flocker.d и Flocker.e, обнаруженные в январе 2008.

Способ распространения таких угроз полностью аналогичен описанному выше способу распространения InfoJack – через популярные сайты, на которых размещается мобильный софт. Троянцы либо выдаются за полезные утилиты, либо включаются в состав таких продуктов.

iPhone

Закончим наш обзор мобильных угроз информацией о долгожданном событии – выходе в марте SDK для iPhone. Считалось, что выход SDK приведет к появлению множества вредоносных программ для iPhone. Однако возможности открытого Apple SDK очень ограничены.

Apple пошла по пути Symbian - модель создания и распространения программ для iPhone базируется на идее «подписанных» приложений. Основное ограничение сформулировано в соглашении об использовании iPhone SDK: «В создаваемом приложении не может запускаться загружаемый код, если только он не интерпретируется опубликованным Apple API и встроенными интерпретаторами. Приложение не может устанавливать или запускать другой запускаемый код, в том числе использовать архитектуру с дополнениями (plug-in), вызывать сторонние программные интерфейсы и другие подобные подсистемы».

Подобные ограничения осложняют жизнь не только вирусописателям, они ставят под фактический запрет существование таких приложений как Firefox, Opera, многих игр, IM-клиентов и массы другого полезного софта, который мог бы пользоваться популярностью на iPhone и расширить возможности использования устройства. За первые четыре дня распространения SDK он был загружен более 100 000 раз. Казалось, что такое количество потенциальных разработчиков приложений должно привести к росту новых приложений, созданных при помощи SDK. Однако этого не происходит. Формально обещание открыть SDK Apple выполнено, но пока не понятно, как на практике этот шаг сможет повлиять на разработку даже легального софта для телефона – слишком серьезные ограничения, слишком много функций в SDK не раскрыто. Вторым важным ограничением является возможность распространения созданных приложений только через электронный магазин самой Apple. И здесь воздвигнуты множественные барьеры, от ограниченного числа допущенных «продавцов»-создателей до ограничений по территориальному признаку (только из США). В подобных условиях очевидно, что мы по-прежнему остаемся в ситуации невозможности выпустить антивирусный продукт для iPhone. И проблема эта - не техническая.

Все это происходит на фоне продолжающихся взломов iPhone. Оценки числа «разлоченных» телефонов варьируются уже от 25 до 50 процентов от всех проданных – и все эти устройства потенциально подвержены риску заражения любой вредоносной программой для IPhone, поскольку пользователи загружают на них файлы из десятков различных неофициальных репозиториев. Этот процесс никак не контролируется, эти пользователи лишены официальной технической поддержки, и мы тоже не можем предоставить им антивирусную защиту.

В обозримом будущем число таких пользователей сравняется с числом пользователей смартфонов на базе Symbian в 2004 году, когда появился Cabir.

Заключение

Итоги первого квартала 2008 года показывают, что период технологического затишья на вирусном фронте подходит к концу.

Явно наметилось изменение тенденции – об этом свидетельствует прежде всего появление первой вредоносной реализации буткита. Кроме того, все чаще и чаще используются различные методы заражения файлов, в том числе с использованием сложных полиморфных технологий. Стоит отметить и начало прямого заимствования вирусописателями некоторых антивирусных технологий.

В настоящее время происходит переосмысление старых технологий и реализация их на новом уровне. В борьбе «вирус-антивирус» намечается переход с программного уровня на уровень аппаратный.