TOP самых опасных вирусов за всю историю

Безмалый В.Ф.

Microsoft Security Trusted Advisor

MVP Consumer Security

История компьютерных вирусов начинается в 1983 году, когда американский ученый Фред Коэн (Fred Cohen) в своей диссертационной работе, посвященной исследованию самовоспроизводящихся компьютерных программ впервые ввел термин компьютерный вирус. Известна даже точная дата - 3 ноября 1983 года, когда на еженедельном семинаре по компьютерной безопасности в Университете Южной Калифорнии (США) был предложен проект по созданию самораспространяющейся программы, которую тут же окрестили вирусом. Для ее отладки потребовалось 8 часов компьютерного времени на машине VAX 11/750 под управлением операционной системы Unix и ровно через неделю, 10 ноября состоялась первая демонстрация. Фредом Коэном по результатам этих исследований была опубликована работа "Computer Viruses: theory and experiments" с подробным описанием проблемы.

Основы теории самораспространяющихся программ были заложены еще в 40-х годах XX века в трудах американского ученого Джона фон Неймана (John von Neumann), который также известен как автор базовых принципов работы современного компьютера. В этих работах описывались теоретические основы самовоспроизводящихся математических автоматов.

В связи с этим хотелось бы рассказать о наиболее опасных образцах вредоносного ПО за всю долгую историю.

Прежде чем говорить о наиболее опасных образцах, давайте решим, что мы будем иметь ввиду под наиболее опасными?

С точки зрения пользователя – это вирус, который нанес ему максимальный ущерб. А с точки зрения офицера информационной безопасности – это тот вирус, который вы все еще не можете обнаружить.

Именно этим критерием мы и будем руководствоваться в дальнейшем.

Итак, наиболее опасное вредоносное ПО, на мой взгляд, это то, которое открывает новые возможности для заражения.

Creeper

Первый сетевой вирус Creeper появился в начале 70-х в военной компьютерной сети Arpanet, прототипе Интернет. Программа была в состоянии самостоятельно выйти в сеть через модем и сохранить свою копию на удаленной машине. На зараженных системах вирус обнаруживал себя сообщением: "I'M THE CREEPER : CATCH ME IF YOU CAN". В целом вирус был безобидным, но раздражал персонал.

Для удаления назойливого, но в целом безобидного вируса неизвестным была создана программа Reaper. По сути это также был вирус, выполнявший некоторые функции, свойственные антивирусу: он распространялся по вычислительной сети и в случае обнаружения тела вируса Creeper уничтожал его.

Появление Creeper не только положило начало современному вредоносному ПО, но и дало этап развитию вирусов, на протяжении которого вирусописательство было уделом немногих талантливых программистов не преследовавших при этом никаких материальных целей.

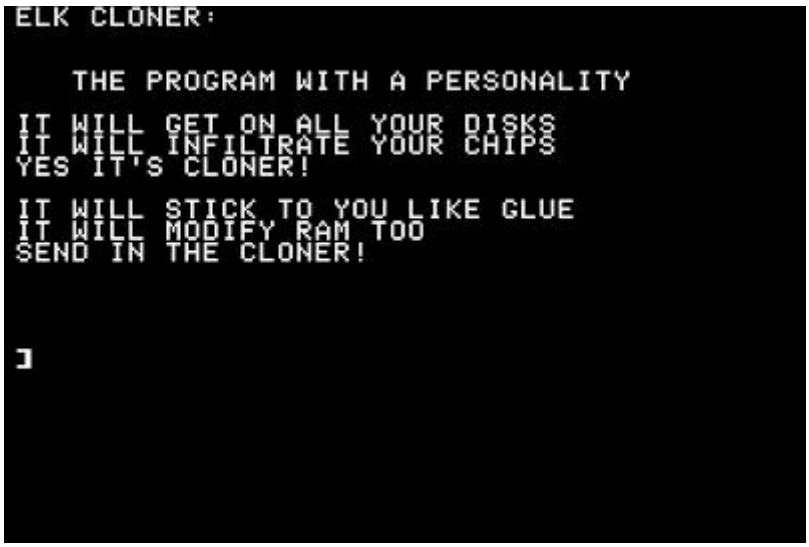


Рисунок 1 Creeper

Brain

Brain (1986 год) — первый вирус для IBM-совместимых компьютеров, вызвавший глобальную эпидемию. Он был написан двумя братьями-программистами Баситом Фарук и Амжадом Алви (Basit Farooq Alvi и Amjad Alvi) из Пакистана. Отличительной чертой его была функция подмены в момент обращения к нему зараженного сектора незараженным оригиналом. **Это дает право назвать Brain первым известным стелс-вирусом.** В течение нескольких месяцев программа вышла за пределы Пакистана и к лету 1987 года эпидемия достигла глобальных масштабов. Фактически это была первая, и, увы, далеко не последняя эпидемия вирусов для IBM PC. В данном случае масштабы эпидемии, безусловно, были не сопоставимы с теперешними заражениями, но ведь эпоха Интернет была еще впереди.

Рисунок 2 Вирус Brain

Virdem

Немецкий программист Ральф Бюргер (Ralf Burger) в 1986г. открыл возможность создания программой своих копий путем добавления своего кода к выполняемым DOS-файлам формата

COM. Опытный образец программы, получившей название Virdem, был продемонстрирован на форуме компьютерного андеграунда - Chaos Computer Club (декабрь 1986 года, Гамбург, ФРГ). Это послужило толчком к написанию сотен тысяч компьютерных вирусов, частично или полностью использовавших описанные автором идеи. Фактически данный вирус положил начало массовым заражениям.

Jerusalem

Самая известная модификация вирусного семейства резидентных файловых вирусов **Suriv** (1987 год) — творения неизвестного программиста из Израиля, **Jerusalem**, стала причиной глобальной вирусной эпидемии, первой настоящей пандемией, вызванной MS-DOS-вирусом. Таким образом, именно с данного вируса начались первые компьютерные пандемии (от греч. pandemía — весь народ), эпидемии, характеризующаяся распространением на территорию многих стран мира).

Именно благодаря этому вирусу сочетание «Пятница, 13» до сих пор заставляет чаще биться сердца системных администраторов. Именно в пятницу, 13 мая 1987 года данный вирус начал уничтожать зараженные файлы при попытке их запуска. Проявил себя в Европе, США и на Ближнем Востоке. Так же этот вирус носил названия «Jerusalem», «Friday the 13th 1813», «Hebrew University», «Israeli» и «Suriv-3».

Рисунок 3 Jerusalem

Jerusalem обладал несколькими вредоносными функциями. Наиболее известной стала та, которая удаляла с компьютера все запускаемые в пятницу, 13-го числа, программы. Поскольку совпадение пятницы с 13-м числом месяца случается не так уж часто, то большинство времени Jerusalem распространялся незаметно, без какого-либо вмешательства в действия пользователей. Вместе с тем, через 30 минут после загрузки в память вирус замедлял скорость работы компьютеров XT в пять раз и демонстрировал маленький черный прямоугольник в текстовом режиме экрана.

Червь Морриса

Червь Морриса (ноябрь 1988) – первый сетевой червь, вызвавший эпидемию. Написан 23-летним студентом Корнельского университета (США) Робертом Моррисом, использовавшим ошибки в системе безопасности операционной системы Unix для платформ VAX и Sun Microsystems. С целью незаметного проникновения в вычислительные системы, связанные с сетью Arpanet, использовался подбор паролей (из списка, содержащего 481 вариант). Общая стоимость ущерба

оценивается в 96 миллионов долларов. Ущерб был бы гораздо больше, если бы червь изначально создавался с разрушительными целями.

Рисунок 4 Роберт Моррис

Данное вредоносное ПО показало, что ОС Unix также уязвима для подбора паролей, как и другие ОС.

Chameleon

Chameleon (начало 1990 года) — первый полиморфный вирус. Его автор, Марк Уошбурн (Mark Washburn) за основу для написания программы взял сведения о вирусе Vienna из книги Ральфа Бюргера "Computer Viruses. The Disease of High Technologies" и добавил к ним усовершенствованные принципы самошифрации вируса Cascade - свойство изменять внешний вид как тела вируса, так и самого расшифровщика.

Данная технология была быстро взята на вооружение и в сочетании со стелс-технологии (Stealth) и бронированием (Armored) позволила новым вирусам успешно противостоять существующим антивирусным пакетам.

С появлением данной технологии бороться с вирусами стало значительно сложнее.

Concept

Concept (август 1995) — первый макровирус, поражавший документы Microsoft Word. Именно в 1995 году стало понятно, что заражаться могут не только исполнимые файлы, а и файлы документов.

Особой зловредностью данный экземпляр не отличался, его эпидемия проходила очень вяло (в течение нескольких лет) и поразил он не так уж и много компьютеров (Лаборатория Касперского зарегистрировала всего 800 жалоб от клиентов на этот вирус). По сравнению с сегодняшним днем, масштабы Concept выглядят весьма скромными. Но для 1995-1997 гг. результат был очень

впечатляющим. Как и маленький ручеек, дающий силу бурной реке, макровирусы предопределили стремительный выход вирусов на мировую арену.

Среди пользователей бытует мнение, что макровирус – это такая безобидная подпрограмма, способная лишь на мелкие пакости вроде замены букв и знаков препинания. На самом деле макровирус может очень многое: отформатировать винчестер или украсть что-то ценное для него не проблема.

Win95.CIH

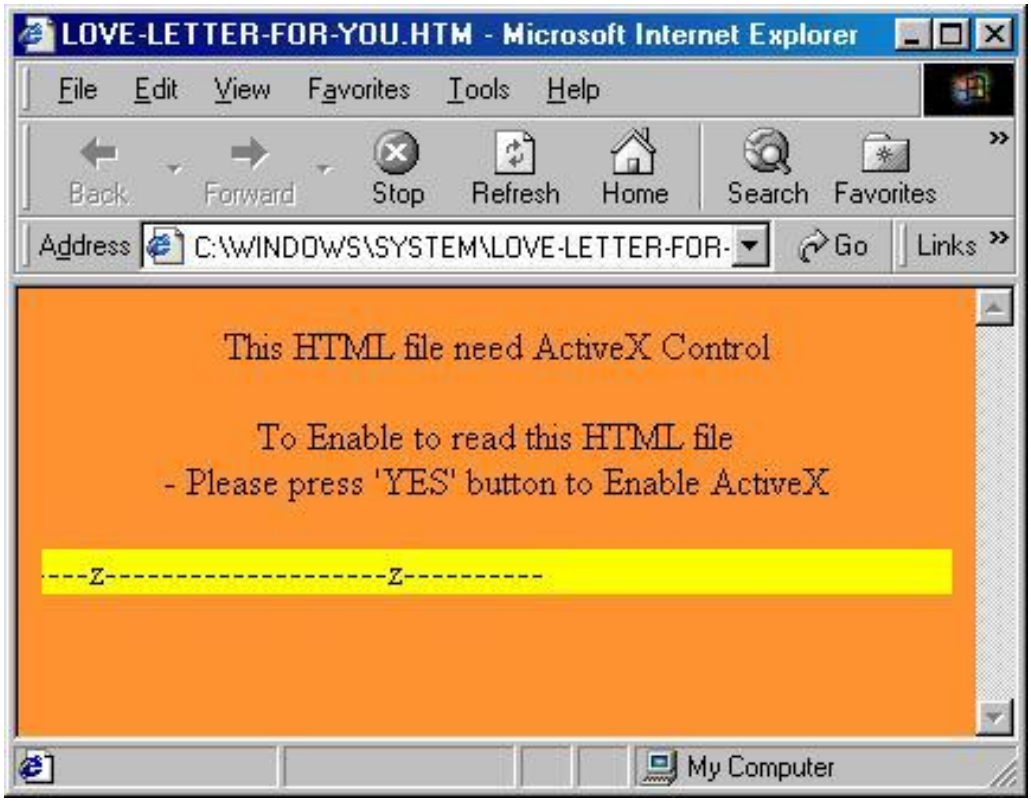
В июне 1998 года был обнаружен вирус тайваньского происхождения Win95.CIH, содержащий логическую бомбу на уничтожение всей информации на жестких дисках и порчу содержимого BIOS на некоторых материнских платах. Дата срабатывания программы (26 апреля) совпадала с датой аварии на Чернобыльской атомной электростанции, вследствие чего вирус получил второе имя — Чернобыль (Chernobyl). Именно данный вирус показал уязвимость систем перезаписи BIOS. Таким образом, вдруг оказалось, что вредоносное ПО может вывести из строя не только информацию, а и компьютерное «железо».

Вирус Win95.CIH - уникальный в свое время вирус. И не только потому, что он является первым из "вирусов, действительно портящих железо". Он не изменяет SYSTEM.INI, он не пишет .VXD-файлов в WINDOWS\SYSTEM, он только заражает PE-файлы... и (иногда) стирает FLASH BIOS и жесткие диски... Это первый "по-настоящему резидентный" Win95/98 вирус

Активизируется 26 апреля (дата катастрофы на Чернобыльской АЭС и дата рождения автора вируса)

LoveLetter

LoveLetter — скрипт-вирус, 5 мая 2000 года побивший рекорд вируса Melissa по скорости распространения. Всего в течение нескольких часов были поражены миллионы компьютеров - **LoveLetter** попал в Книгу Рекордов Гиннеса.



Ситуация развивалась стремительно. Количество обращений (и количество пострадавших) увеличивалось в геометрической прогрессии.

Данный вирус распространялся с сообщениями электронной почты и по каналам IRC. Письмо с вирусом легко выделить. Тема письма - "ILOVEYOU", что сразу же бросается в глаза. В самом письме содержится текст "kindly check the attached LOVELETTER coming from me" и присоединенный файл с именем "LOVE-LETTER-FOR-YOU.TXT.vbs". Вирус срабатывал только в том случае, если пользователь открывал этот присоединенный файл.

Вирус рассылал себя по всем адресам, которые находил в адресной книге почтовой программы MS Outlook инфицированного компьютера, а также записывал свои копии в файлы на жестком диске (необратимо затирая тем самым их оригинальное содержание). Жертвами вируса в частности являлись картинки в формате JPEG, программы Java Script и Visual Basic Script и целый ряд других файлов. Также вирус "прятал" видео- и музыкальные файлы в формате MP2 и MP3.

Кроме этого, вирус совершал несколько действий по инсталляции себя в систему и по установке некоторых дополнительных вирусных модулей, которые сам перекачивал из Internet.

Все это говорит о том, что вирус VBS.LoveLetter - очень опасен! Кроме прямой порчи данных и нарушения целостности защиты операционной системы, вирус рассылал большое количество сообщений - своих копий. В ряде случаев вирус парализовал работу целых офисов.

Ramen

Ramen (январь 2001) — вирус, за считанные дни поразивший большое количество крупных корпоративных систем на базе операционной системы Linux.

Опасный Интернет-червь, атаковавший сервера под управлением операционных систем Red Hat Linux 6.2 и Red Hat Linux 7.0. Первые сообщения о появлении данного червя были получены из стран Восточной Европы, что позволяет подозревать его восточноевпропейское происхождение. Для своего размножения червь использует некоторые слабые места в приложениях этих операционных систем.

Червь представлял собой архив с именем ramen.tgz, содержащий в себе 26 различных исполняемых файлов и shell-скриптов. Каждый исполняемый файл содержится в архиве в двух экземплярах: скомпилированный для запуска в Red Hat 6.2 и в Red Hat 7.0. Также в архиве содержится исполняемый файл с именем wu62, который при работе червя не используется.

При внешней безвредности червь чрезвычайно опасен, так как нарушает нормальное функционирование сервера: работа http-сервера будет нарушена уничтожением содержимого всех index.html файлов, анонимный ftp-доступ к серверу будет запрещен, сервисы rpc и lpd будут удалены, ограничения доступа через hosts.deny будут сняты.

Червь использует в своем коде многие слегка модифицированные эксплоиты, доступные ранее на хакерских сайтах, а также на сайтах, посвященных сетевой безопасности.

Следует отметить, что червь использует при атаках «дыры", самая «свежая" из которых известна с конца сентября 2000 года. Однако тот факт, что при инсталляции системы на нее устанавливаются уязвимые сервисы, а многие пользователи и администраторы не производят должный мониторинг предупреждений о «слабых местах" системы и вовремя не производят их устранение, делает червь более чем жизнеспособным.

Именно с его появлением был разрушен миф о том, что вирусов под Linux не бывает.

CodeRed

CodeRed (12 июля 2001 года) — представитель нового типа вредоносных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов. В процессе работы такие программы существуют исключительно в системной памяти, а при передаче на другие компьютеры - в виде специальных пакетов данных.

Самое подробное и оперативное описание и анализ червя были сделаны программистами группы eEye Digital Security. Они также дали вирусу название — намёк на вид напитка Mountain Dew и фразу-предупреждение в вирусе «Hacked By Chinese!» («Взломано китайцами!») — намёк на коммунистический Китай, хотя в действительности вирус скорее всего был написан этническими китайцами на Филиппинах. Этой фразой червь заменял содержимое веб-сайтов на заражённом сервере.

Червь использовал уязвимость в утилите индексирования, которая поставлялась с веб-сервером Microsoft IIS. Эта уязвимость была описана вендором — Microsoft — на их сайте MS01-033 (англ.); кроме того, за месяц до эпидемии была опубликована соответствующая заплатка.

Эксперты eEye утверждают, что червь начал распространение из Макати-Сити на Филиппинах.

Фактически данный вирус положил начало целой серии вирусов (и, увы, это продолжается до сих пор). Отличительной чертой этой серии явилось то что вирусы появляются через некоторое время после того, как появляются соответствующие обновления от производителей ПО.

По оценкам CERT (Carnegie Mellon Computer Response Center — Центр обработки компьютерных запросов Карнеги Меллона) число компьютеров, зараженных червем Code Red, достигает примерно 350000. Созданный им трафик в Интернете, по мере того как зараженные компьютеры искали новые жертвы, наложил существенный отпечаток на общую скорость Интернета.

Проявления, изначально заложенные в Code Red, заключались в использовании всех зараженных им компьютеров для организации DOS-атаки против web-сайта Whitehouse.gov (web-сайта Белого дома).

Таком образом было положено начало использованию халатного отношения системных администраторов к установке обновлений ПО.

Cabir

Cabir (июнь 2004) — первый сетевой червь, распространяющийся через протокол Bluetooth и заражающий мобильные телефоны, работающие под управлением OS Symbian. Таким образом, с появлением этого червя стало понятно, что отныне заражаемы не только ПК, но и смартфоны. Сегодня же угрозы для смартфонов уже исчисляются миллионами. А начиналось все в далеком 2004 году.

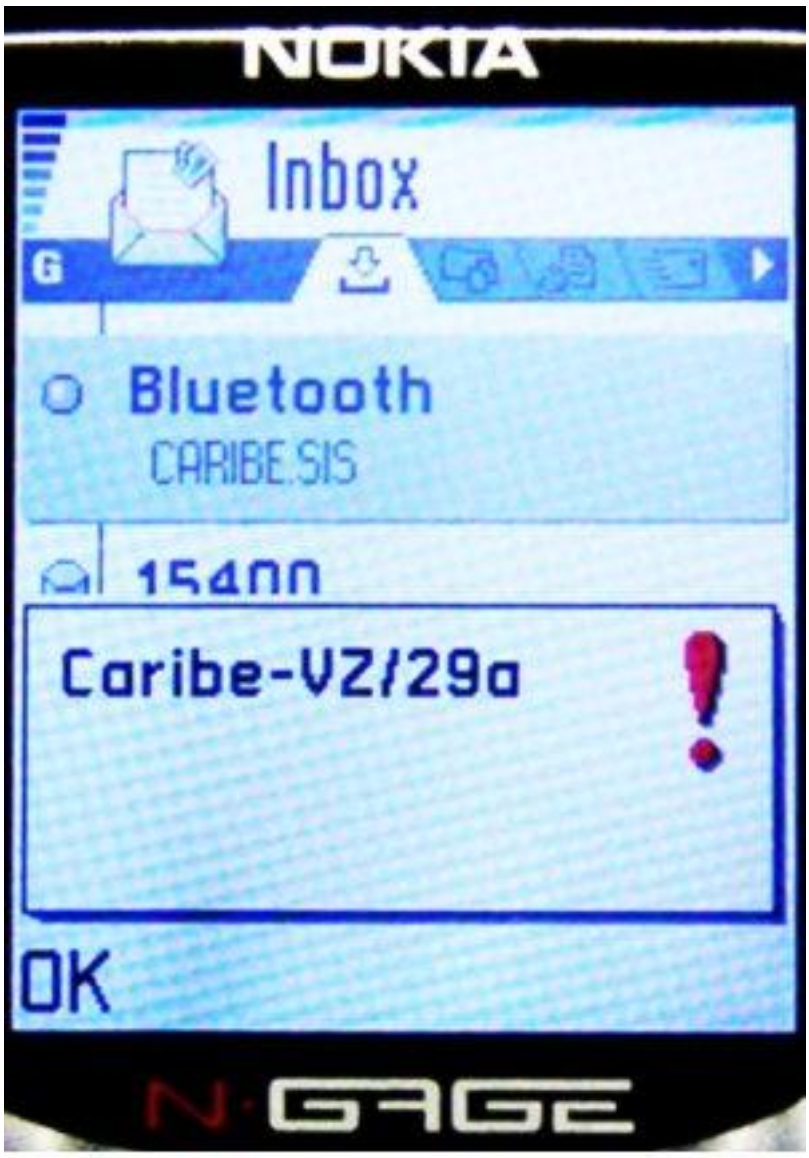


Рисунок 5 Cabir

На рис.1 приведена статистика увеличения численности мобильных зловредов в 2013 году поквартально.

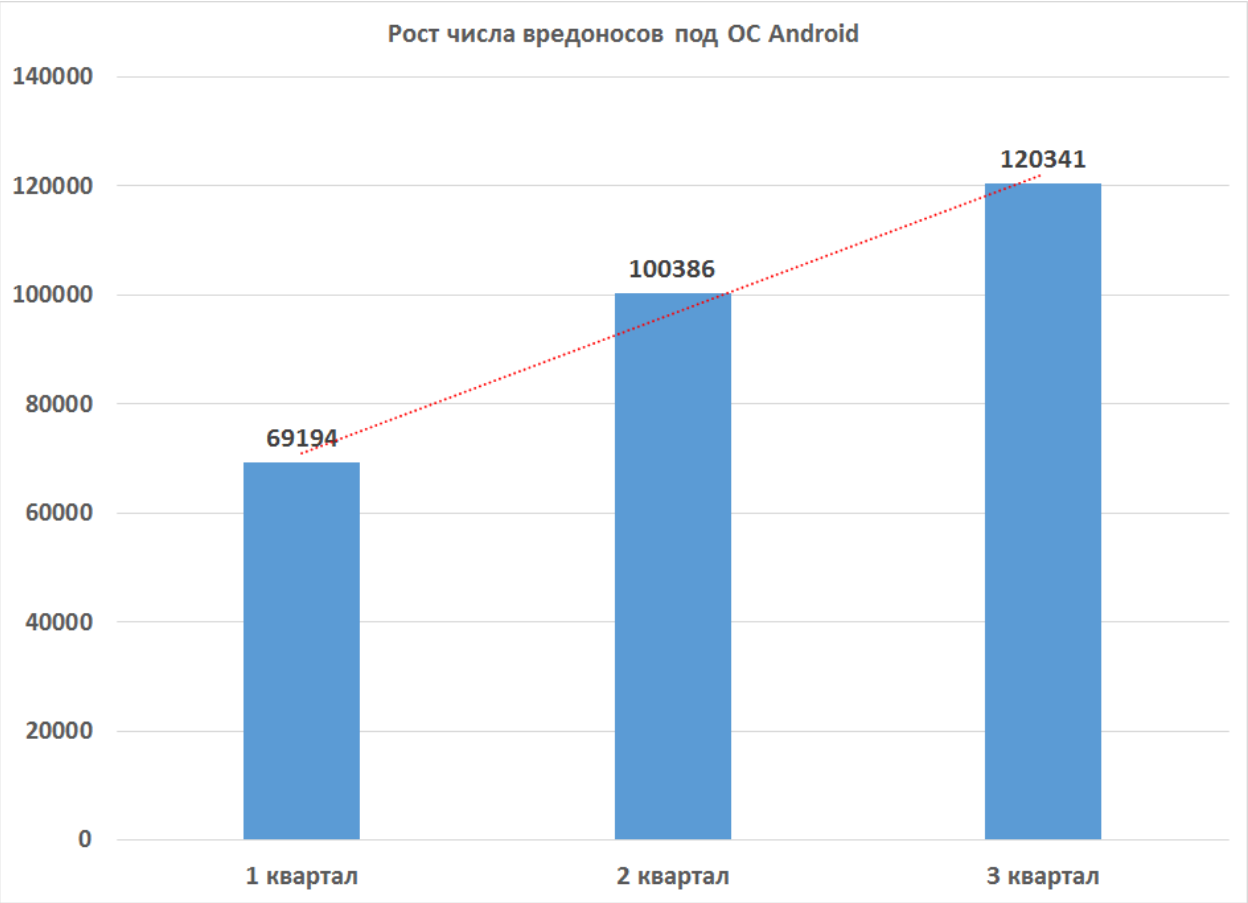


Рисунок 6 По данным Лаборатории Касперского

А начиналось все в 2004 году с первого вируса Cabir…

Kido

Главной эпидемией 2009 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.

Вместе с тем, создатели Kido не проявляли большой активности до марта 2009года, хотя по разным оценкам, к этому времени он уже смог заразить до 5 000 000 компьютеров во всем мире. И в ночь с 8 на 9 апреля 2009 года зараженным ПК была дана команда на обновление с использованием соединения P2P. Помимо обновления Kido на зараженные ПК происходила загрузка двух дополнительных программ: почтовый червь семейства Email-Worm.Win32.Iksmas, занимающийся рассылкой спама, вторая программа — лжеантивирус семейства FraudTool.Win32.SpywareProtect2009, требующий деньги за удаление якобы найденных программ.

Для борьбы с этой 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.

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

Появление кибероружия в 2012 году

Wiper

«Мистический» троянец в конце апреля 2012 года сильно встревожил Иран: появившись неизвестно откуда, он уничтожил множество баз данных в десятках организаций. Одним из тех, кто больше всего пострадал от него, стал крупнейший в Иране нефтяной терминал, работа которого была остановлена на несколько дней из-за того, что были уничтожены данные о нефтяных контрактах.

Создатели Wiper сделали все возможное, чтобы уничтожить абсолютно все данные, которые можно было бы использовать для анализа инцидентов. Поэтому ни в одном из случаев, которые мы проанализировали, после активации Wiper от вредоносной программы не осталось почти никаких следов.

Нет никакого сомнения в том, что существовала вредоносная программа, известная как Wiper, которая атаковала компьютерные системы в Иране (и, возможно, в других частях света) до конца апреля 2012 года.

Вредоносная программа была написана так профессионально, что, будучи активирована, она не оставляла после себя никаких данных. Поэтому, несмотря на то, что были обнаружены следы заражения, сама вредоносная программа остается неизвестной: ничего не известно ни о каких других инцидентах с перезаписью содержимого диска, произошедших по той же схеме, что при заражении Wiper; не зарегистрировано также обнаружения этого вредоносного ПО компонентами проактивной защиты, входящими в состав защитных решений.

Все это в целом приводит к мысли что данное решение скорее является продуктом деятельности технических лабораторий ведения компьютерных войн одной из развитых стран, чем просто плодом разработки злоумышленников.

Flame

Flame представляет собой весьма хитрый набор инструментов для проведения атак, значительно превосходящий по сложности Duqu. Это троянская программа — бэкдор, имеющая также черты, свойственные червям и позволяющие ей распространяться по локальной сети и через съемные носители при получении соответствующего приказа от ее хозяина.

После заражения системы Flame приступает к выполнению сложного набора операций, в том числе к анализу сетевого трафика, созданию снимков экрана, аудиозаписи разговоров, перехвату клавиатурных нажатий и т.д. Все эти данные доступны операторам через командные серверы Flame.

Червь Flame, созданный для кибершпионажа, попал в поле зрения экспертов «Лаборатории Касперского» при проведении исследования по запросу Международного союза электросвязи (МСЭ), обратившегося за содействием в поиске неизвестной вредоносной программы, которая удаляла конфиденциальные данные с компьютеров, расположенных в странах Ближнего Востока. Хотя Flame имеет иной функционал, чем печально известные образцы кибероружия Duqu и Stuxnet, все эти вредоносные программы имеют много общего: географию атак, узкую целевую направленность в сочетании с использованием специфических уязвимостей в ПО. Это ставит Flame в один ряд с «кибернетическим супероружием», развертываемым на Ближнем Востоке

неизвестными злоумышленниками. Без сомнения, Flame является одной из самых сложных киберугроз за всю историю их существования. Программа имеет большой размер и невероятно сложную структуру. Она заставляет переосмыслить такие понятия, как «кибервойна» и «кибершпионаж».

Червь Flame — это огромный пакет, состоящий из программных модулей, общий размер которых при полном развертывании составляет почти 20 МБ. Вследствие этого анализ данной вредоносной программы представляет огромную сложность. Причина столь большого размера Flame в том, что в него входит множество разных библиотек, в том числе для сжатия кода (zlib, libbz2, ppmd) и манипуляции базами данных (sqlite3), а также виртуальная машина Lua.

Gauss

Gauss — это сложный комплекс инструментов для осуществления кибершпионажа, реализованный той же группой, что создала вредоносную платформу Flame. Комплекс имеет модульную структуру и поддерживает удаленное развертывание нового функционала, который реализуется в виде дополнительных модулей.

Gauss – это «банковский» троянец, созданный государством, имеющий вредоносный функционал неизвестного назначения». В дополнение к краже разнообразных данных с зараженных Windows-компьютеров он содержит неизвестный пока вредоносный функционал, код которого зашифрован и который активируется только в системах с определенной конфигурацией.

Известные на сегодняшний день модули выполняют следующие функции:

- перехват cookie-файлов и паролей в браузере;
- сбор и отправка злоумышленникам данных о конфигурации системы;
- заражение USB-носителей модулем, предназначенным для кражи данных;
- создание списков содержимого системных накопителей и папок;
- кража данных, необходимых для доступа к учетным записям различных банковских систем, действующих на Ближнем Востоке;
- перехват данных по учетным записям в социальных сетях, почтовым сервисам и системам мгновенного обмена сообщениями.

Заключение

Хотелось бы чтобы читатели понимали, что никто и никогда не сможет создать полный список всех наиболее опасных образцов вредоносного ПО. Потому что самым опасным вирусом будет тот, который вы так и не сумели обнаружить!