Классификация вирусов

Введение

- Существует класс программ, которые были изначально написаны с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов и т. п., или же приобрели такие свойства вследствие каких-либо причин. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными.
- ***Вредоносная программа*** – *это программа, наносящая какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети.*

- Поскольку мало пользователей в здравом уме добровольно поставят себе на компьютер заведомо вредоносную программу, их авторы вынуждены использовать различные обманные методы или специальные технологии для несанкционированного проникновения в систему. Следовательно, классифицировать вредоносные программы удобно по способу проникновения, размножения и типу вредоносной нагрузки.
- Все вредоносные программы в соответствии со способами распространения и вредоносной нагрузкой можно разделить на четыре основные типа – компьютерные вирусы, черви, трояны и другие программы.

Вирусы

- ***Компьютерный вирус*** *– это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.*
- Условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий:
  1. Проникновение на чужой компьютер
  2. Активация
  3. Поиск объектов для заражения
  4. Подготовка копий
  5. Внедрение копий

- Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения – фактически, все каналы, по которым можно скопировать файл. Однако в отличие от червей, вирусы не используют сетевые ресурсы – заражение вирусом возможно только если пользователь сам каким-либо образом его активировал. Например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.
- После проникновения следует активация вируса. Это может происходить несколькими путями и соответствии с выбранным методом вирусы делятся на такие виды:
- **Загрузочные вирусы** заражают загрузочные сектора жестких дисков и мобильных носителей.
- **Файловые вирусы** – файлы.

Файловые вирусы

- **Классические файловые вирусы** – они различными способами внедряются в исполняемые файлы (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы
- **Макровирус** , которые написаны на внутреннем языке так называемых макросах какого-либо приложения. Подавляющее большинство макровирусов используют макросы текстового редактора Microsoft Word
- **Скрипт-вирусы**, написанные в виде скриптов для определенной командной оболочки – например bat-файлы для DOS или VBS и JS – скрипты для Windows Scripting Host

- Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочки, для которой каждый конкретный вирус был написан. Это означает, что вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например Unix. Точно также макровирус для Microsoft Word 2003 скорее всего не будет работать в приложении Microsoft Excel 97.

Черви

- **Червь** *(сетевой червь) – это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.*
- Жизненный цикл червей состоит из таких стадий:
  1. Проникновение в систему
  2. Активация заражения
  3. Поиск объектов для
  4. Подготовка копий
  5. Распространение копий

Типы червей

- **Сетевые черви** используют для распространения локальные сети и Интернет.
- **Почтовые** – распространяются с помощью почтовых программ.
- **P2P-черви** – при помощи пиринговых файлообменных сетей.
- **IM-черви** используют системы мгновенного обмена.
- **IRC-черви** распространяются по каналам IRC.

- После проникновения на компьютер, червь должен активироваться – иными словами запуститься. По методу активации все черви можно разделить на две большие группы – на тех, которые требуют активного участия пользователя и тех, кто его не требует. На практике это означает, что бывают черви, которым необходимо, чтобы владелец компьютера обратил на них внимание и запустил зараженный файл, но встречаются и такие, которые делают это сами, например, используя ошибки в настройке или бреши в системе безопасности операционной системы. Отличительная особенность червей из первой группы – это использование обманных методов. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добровольно открывает вложение с почтовым червем, тем самым его активируя.
- Сетевые черви могут кооперироваться с вирусами – такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

Трояны

- ***Троян*** *(троянский конь) – программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе.*
- Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают на компьютеры вместе с вирусом либо червем – то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.
- Следовательно, жизненный цикл троянов состоит всего из двух стадий:
  1. Проникновение в систему
  2. Активация

Типы троянов

- **Клавиатурные шпионы**, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.
- **Похитители паролей** предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.
- **Утилиты скрытого удаленного управления** – это трояны, которые обеспечивают своему автору или другому осведомленному лицу несанкционированный удаленный контроль над инфицированным компьютером. Перечень действий, которые позволяет выполнять тот или иной троян, определяется его функциональностью, заложенной автором. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных.

- **Анонимные SMTP-сервера и прокси-сервера** – такие трояны на зараженном компьютере организовывают несанкционированную отправку электронной почты, часто используется для рассылки спама.
- **Утилиты дозвона** в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.
- **Модификаторы настроек браузера** меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.
- **Логические бомбы** характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.

Другие вредоносные программы

- Условно опасные программы.
- Шпионские программы (spyware).
- Хакерские утилиты.
- Злые шутки.
- Шутки и мистификации.

Условно опасные программы

- **Условно опасные программы**, то есть такие, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:
  - Riskware
  - Рекламные утилиты (adware)
  - Pornware

Riskware

- **Riskware** – вполне легальные программы и сами по себе не опасны, однако обладают таким функционалом, что в случае получения злоумышленником доступа к управлению ими, могут нанести серьезный вред. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и другие.

Рекламные утилиты

- **Рекламные утилиты** (**adware**9) – условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема adware кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме. Однако среди adware-программ есть и вполне заслуживающие доверия – например, клиент ICQ.

Pornware

- **Pornware** – к этому классу относятся утилиты, так или иначе связанные с показом пользователям информации порнографического характера. На сегодняшний день это программы, которые самостоятельно дозваниваются до порнографических телефонных служб, загружают из Интернет порнографические материалы или утилиты, предлагающие услуги по поиску и показу такой информации. Отметим, что к вредоносным программам относятся только те утилиты класса pornware, которые устанавливаются на компьютер пользователя несанкционированно – через уязвимость в операционной системы или браузера или при помощи троянов. Обычно это делается с целью насильственного показа рекламы платных порнографических сайтов или служб.

Шпионские программы

- **Шпионские программы** (**spyware**), которые скрытно собирают различную информацию о пользователе и передают своему автору или хозяину. Spyware могут проникать на компьютер, например, под видом adware-компонентов других программ и не удаляться после регистрации основной утилиты. Отличие шпионской программы от троянов-похитителей информации методов состоит в том, что трояны проникают при помощи других вредоносных программ, обманных или используя различные уязвимости, а spyware – в виде скрытых модулей к известным программам.

Хакерские утилиты

- **Хакерские утилиты**. К этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

Злые шутки

- **Злые шутки** – программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений о, например, форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений целиком и полностью отражает фантазию автора.

Шутки и мистификации

- Отдельно от перечисленных выше программ стоит также отметить такой класс вредоносных явлений как **шутки и мистификации**. Они представляют из себя непроверенную или даже изначально однозначно неправдивую информацию о якобы новых вирусах или вирусных угрозах, которая в виде предупреждений передается по всем друзьям и знакомым. Если не выполнять указанные в таком сообщении рекомендации, шутки и мистификации явного вреда компьютеру не несут. Однако при достижении некоторой массовости они способным существенно увеличить нагрузку на сетевое оборудование вследствие резко возросшего количества пересылаемых сообщений. К тому же при пересылке такой шутки часто страдает репутация человека и компании, в которой он работает, что для ряда организаций есть непозволительная роскошь.

Eicar

- Существует еще один класс программ, имеющих прямое отношение к вредоносным, однако по действию и функциям прямо им противоположный. Это специальные программы для тестирования антивирусных средств на предмет работоспособности. То есть обнаружив такую программу, антивирус должен среагировать так, как будто нашелся вирус – тогда пользователь сможет сделать вывод, что антивирусная защита работает и компьютер в безопасности. В этот класс официально входит только одна программа – EICAR, названная так в честь своего разработчика, Европейского института компьютерных антивирусных исследований EICAR (European Institute for Computer Anti-virus Research). На сегодняшний день все известные антивирусные программы поддерживают детектирование EICAR. На ряду с EICAR некоторые антивирусные компании ввели собственные модификации тестового вируса, позволяющие более точно протестировать работу своих программ.

Trojan.Encoder

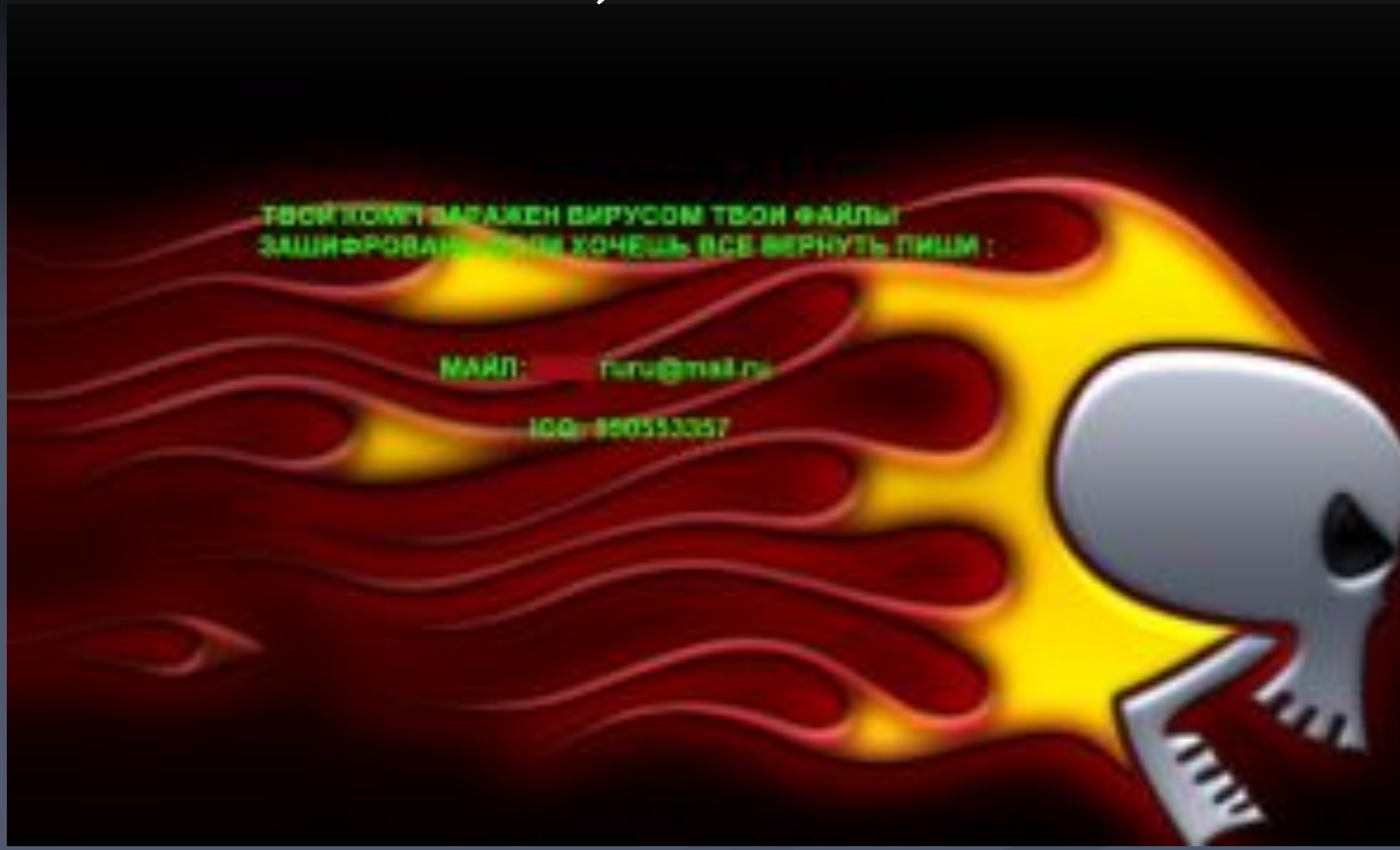
В Рунете началась очередная эпидемия вируса Trojan.Encoder (Trojan.Encoder.34, а также модификации 37, 38, 39, 40 и 41), шифрующего данные на компьютерах пользователей и требующего деньги за расшифровку. Последние модификации Trojan.Encoder принадлежат перу одного автора, иногда называющего себя «Корректор». Они шифруют большинство документов, делая невозможной работу с ними. Исключение составляют файлы, относящиеся к системе и установленным в ней программам — таким образом компьютер продолжает работать, позволяя жертве мошенничества связаться со злоумышленником и перечислить ему требуемую сумму денег.

Особенностью последних модификаций Trojan.Encoder является то, что они добавляют к зараженным файлам окончание vscrypt — к примеру, вместо pic.jpg файл получает имя pic.jpg.vscrypt.

Trojan.Encoder

Trojan.Encoder в настоящее время распространяется посредством ссылок на вредоносный сайт в почтовых сообщениях. Пользователю предлагается просмотреть открытку, якобы присланную от имени сервиса открыток Mail.ru. При открытии соответствующей страницы предлагается установить кодек, который на самом деле оказывается троянской программой. После окончания процесса шифрования файлов Trojan.Encoder выводит на Рабочий стол Windows сообщение о том, что документы зашифрованы, а также приводит контактные данные злоумышленника.

Trojan.Encoder



Один из вариантов отображения контактной информации злоумышленника

Trojan.Encoder

Напомним, что в декабре, августе и сентябре 2008 года наблюдались эпидемии других модификаций того же вируса — Trojan.Encoder.33, Trojan.Encoder.20 и Trojan.Encoder.19. Большинство модификаций Trojan.Encoder предлагают пользователю воспользоваться дешифровщиком, для чего требуют перевести на счёт киберпреступников от $10 до $89. Аппетит «Корректора» сопоставим с запросами авторов предыдущих модификаций — в настоящий момент пользователи-жертвы сообщают о цене в 600 рублей за один экземпляр расшифровщика.

В настоящее время решение проблемы зашифрованных файлов найдено. Если вы столкнулись с Trojan.Encoder, вместо того, чтобы платить выкуп преступнику, обратитесь, например, к специалистам компании «Доктор Веб». Они предоставят вам специальные утилиты (предварительно вам нужно будет выслать образец зашифрованных файлов, чтобы специалисты могли определить версию Trojan.Encoder). При этом ни в коем случае не пытайтесь переустановить систему или восстановить её из резервных копий. А ещё лучше — всегда пользуйтесь актуальными версиями антивирусных программ. Это позволит избежать множества проблем.