2017

Компьютерные угрозы безопасности и основы антивирусной защиты

ВЫПОЛНИЛ:
ЦИРУЛИК ИВАН

Оглавление

ВСТУПЛЕНИЕ

Под понятием «вредоносного программного обеспечения» подразумевается любая программа, созданная и используемая для осуществления несанкционированных и часто вредоносных действий. Как правило, к нему относят разного рода вирусы, черви, троянцы, клавиатурные шпионы, программы для кражи паролей, макровирусы, вирусы сектора загрузки, скриптовые вирусы, мошенническое ПО, шпионские и рекламные программы. К сожалению, этот далеко неполный список, который с каждым годом пополняется все новыми и новыми видами вредоносных программ, которые в данном материале мы часто будем называть общим словом - вирусы.

Мотивы написания компьютерных вирусов могут быть самыми разными: от банального желания проверить свои силы в программировании до желания навредить или получить незаконные доходы. Например, некоторые вирусы не приносят почти никакого вреда, а только замедляют работу машины за счет своего размножения, замусоривая при этом, жесткий диск компьютера или производят графические, звуковые и другие эффекты. Иные же могут быть очень опасными, приводя к потере программ и данных, стиранию информации в системных областях памяти и даже к выходу из строя частей жесткого диска.

КЛАССИФИКАЦИЯ ВИРУСОВ

В настоящий момент, какой-либо четкой классификации вирусов не существуют, хотя определенные критерии их разделения есть.

Среда обитания вирусов

В первую очередь вредоносное ПО разделяют по своей среде обитания (по поражаемым объектам). Самым распространенным типом вредоносных программ можно назвать ***файловые вирусы***, которые заражают исполняемые файлы и активизируются при каждом запуске инфицированного объекта. Недаром некоторые почтовые сервисы (например, сервис Gmail), не допускают отправку электронных писем с прикрепленными к ним исполняемыми файлами (файлами с расширением .EXE). Это делается с целью обезопасить получателя от получения письма с вирусом. Попадая на компьютер через сеть или любой носитель информации, такой вирус не ждет, пока его запустят, а запускается автоматически, и выполняет вредоносные действия, на которые он запрограммирован.

Это совсем не означает, что все исполняемые файлы являются вирусами (например, установочные файлы тоже имеют расширение .exe), или, что вирусы имеют только расширение exe. У них может быть расширение inf, msi, и вообще они могут быть без расширения или прикрепляться к уже существующим документам (инфицировать их).

Следующий тип вирусов имеет свою характерную особенность, они прописываются в загрузочных областях дисков или секторах, содержащих системный загрузчик. Как правило, такие вирусы активируются в момент загрузки операционной системы и называются ***вирусами загрузочного сектора***.

Объектами заражения ***макровирусов*** служат файлы-документы, к которым относятся как текстовые документы, так и электронные таблицы, разработанные на макроязыках. Большинство вирусов этого типа написано для популярнейшего текстового редактора MS Word.

И наконец, ***сетевые или скриптовые вирусы***, чтобы размножаться, используют протоколы компьютерных сетей и команды скриптовых языков. В последнее время такого типа угрозы получили очень широкое распространение. Например, часто для заражения компьютера злоумышленники используют уязвимости JavaScript, который активно используется практически всеми разработчиками веб-сайтов.

Алгоритмы работы вирусов

Еще одним критерием разделения вредоносных программ служат особенности алгоритма их работы и используемые при этом технологии. В общем, все вирусы можно разделить на два типа - резидентные и нерезидентные. Резидентные находятся в оперативной памяти компьютера и ведут активную деятельность вплоть до его выключения или перезагрузки. Нерезидентные, память не заражают и являются активными лишь в определенный момент времени.

Вирусы-спутники (вирусы-компаньоны) не изменяют исполняемые файлы, а создают их копии с тем же самым названием, но другим, более приоритетным расширением. Например, файл xxx.COM будет всегда запущен раньше, чем xxx.EXE, в силу специфики файловой системы Windows. Таким образом, вредоносный код выполняется перед исходной программой, а уже за тем только она сама.

- ***Вирусы-черви*** самостоятельно распространяются в каталогах жестких дисков и компьютерных сетях, путем создания там собственных копий. Использование уязвимостей и различных ошибок администрирования

в программах позволяет червякам распространяться полностью автономно, выбирая и атакуя машины пользователей в автоматическом режиме.

- ***Вирусы-невидимки*** (стелс-вирусы) стараются частично или полностью скрыть свое существование в ОС. Для этого они перехватывают обращение операционной системы к зараженным файлам и секторам дисков и подставляют незараженные области диска, что сильно мешает их обнаружению.

- ***Вирусы-призраки*** (полиморфные или самошифрующиеся вирусы) имеют зашифрованное тело, благодаря чему две копии одного вируса не имеют одинаковых частей кода. Это обстоятельство довольно сильно усложняет процедуру детектирования такого рода угроз и поэтому данная технология используется практически всеми типами вирусов.

- ***Руткиты*** позволяют злоумышленникам скрывать следы своей деятельности во взломанной операционной системе. Такого рода программы занимаются сокрытием вредоносных файлов и процессов, а так же собственного присутствия в системе.

Дополнительная функциональность

Многие вредоносные программы содержать в себе дополнительные функциональные возможности, не только затрудняющие их обнаружение в системе, но и позволяющие злоумышленникам управлять вашим компьютером и получать нужные им данные. К таковым вирусам можно отнести бэкдоры (взломщик системы), кейлоггеры (клавиатурный перехватчик), программы-шпионы, ботнеты и другие.

Поражаемые операционные системы

Различные вирусы могут быть рассчитаны на действия в определенных операционных системах, платформах и средах (Windows, Linux, Unix, OS/2, DOS). Конечно, абсолютное большинство вредоносного ПО написано для самой популярной в мире системы Windows. При этом некоторые угрозы работают только в среде Windows 95/98, некоторые только в Windows NT, а некоторые только в 32-битных средах, не заражая 64-битные платформы.

ИСТОЧНИКИ УГРОЗ

Одна из первостепенных задач злоумышленников – найти способ доставки зараженного файла на ваш компьютер и заставить его там активироваться. Если ваш компьютер не подсоединен к компьютерной сети и не производит обмен информацией с другими компьютерами посредством съемных носителей, можете быть уверены, компьютерные вирусы ему не страшны. Основными источниками вирусов являются:

- Флоппи-диск, лазерный диск, флэш-карта или любой другой съемный носитель информации, на котором находятся зараженные вирусом файлы;
- Жесткий диск, на который попал вирус в результате работы с зараженными программами;
- Любая компьютерная сеть, в том числе локальная сеть;
- Системы электронной почты и обмена сообщениями;
- Глобальная сеть Интернет;

ВИДЫ КОМПЬЮТЕРНЫХ УГРОЗ

Наверное, для вас не секрет, что на сегодняшний день основным источником вирусов является всемирная глобальная сеть. С какими же

видами компьютерных угроз может столкнуться любой рядовой пользователь глобальной сети интернет?

- ***Кибервандализм***. Распространение вредоносного ПО с целью повреждения данных пользователя и вывода компьютера из строя.
- ***Мошенничество***. Распространение вредоносного ПО для получения незаконных доходов. Большинство программ используемых с этой целью позволяют злоумышленникам собирать конфиденциальную информацию и использовать ее для кражи денег у пользователей.
- ***Хакерские атаки***. Взлом отдельных компьютеров или целых компьютерных сетей с целью кражи конфиденциальных данных или установки вредоносных программ.
- ***Фишинг***. Создание подложных сайтов, которые являются точной копией существующих (например, сайта банка) с целью кражи конфиденциальных данных при их посещении пользователями.
- ***Спам***. Анонимные массовые рассылки электронной почты, которые засоряют электронные ящики пользователей. Как правило, используются для рекламы товаров и услуг, а так же фишинговых атак.
- Рекламное программное обеспечение. Распространение вредоносного ПО, запускающего рекламу на вашем компьютере или перенаправляющего поисковые запросы на платные (часто порнографические) веб-сайты. Нередко бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя без его ведома.
- ***Ботнеты***. Зомби-сети, состоящие из зараженных с помощью троянца компьютеров (среди которых может быть и ваш ПК), управляемых одним хозяином и используемых для его целей (например, для рассылки спама).

ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

Обнаружить вирус, попавший в ваш компьютер на ранней стадии очень важно. Ведь пока он не успел размножиться и развернуть систему самозащиты от обнаружения, шансы избавиться от него без последствий, очень велики. Определить наличие вируса на компьютере можно и самому, зная ранние признаки его заражения:

- Уменьшение объема свободной оперативной памяти;
- Сильное замедление загрузки и работы компьютера;
- Непонятные (без причин) изменения в файлах, а также изменение размеров и даты их последнего изменения;
- Ошибки при загрузке операционной системы и во время ее работы;
- Невозможность сохранять файлы в определенных папках;
- Непонятные системные сообщения, музыкальные и визуальные эффекты.

Если же вы обнаружили, что некоторые файлы исчезли или не открываются, невозможно загрузить операционную систему или произошло форматирование жесткого диска, значит, вирус перешел в активную фазу и простым сканированием компьютера специальной антивирусной программой уже не отделаешься. Возможно, придется переустанавливать операционную систему. Или запускать средства лечения с аварийного загрузочного диска, так как установленный на компьютер антивирус наверняка утратил свою функциональность из-за того, что также был изменен или заблокирован вредоносным ПО.

Правда, даже если вам удастся избавиться от зараженных объектов, часто восстановить нормальную функциональность системы уже не удается, так как могут быть безвозвратно утеряны важные системные файлы. При этом, помните, что под угрозой уничтожения могут оказаться

ваши важные данные, будь то фотографии, документы или коллекция музыки.

Что бы избежать всех этих неприятностей, необходимо постоянно следить за антивирусной защитой вашего компьютера, а так же знать и соблюдать элементарные правила информационной безопасности.

АНТИВИРУСНАЯ ЗАЩИТА

Для обнаружения и обезвреживания вирусов применяются специальные программы, которые так и называются «антивирусные программы» или «антивирусы». Они блокируют несанкционированный доступ к вашей информации извне, предотвращают заражение компьютерными вирусами и в случае необходимости, ликвидируют последствия заражения.

Технологии антивирусной защиты

Теперь, давайте ознакомимся с используемыми технологиями антивирусной защиты. Наличие той или иной технологии в составе антивирусного пакета, зависит от того, как позиционируется продукт на рынке и влияет на его конечную стоимость.

- Файловый антивирус**.** Компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере. В случае обнаружения известных вирусов, как правило, вам предлагается вылечить файл. Если по каким-то причинам это невозможно, то он удаляется или перемещается на карантин.
- ***Почтовый антивирус.*** Обеспечивает защиту входящей и исходящей почты и осуществляет ее проверку на наличие опасных объектов.

- Вэб антивирус**.** Осуществляет антивирусную проверку трафика, передающегося по интернет протоколу HTTP, что обеспечивает защиту вашего браузера. Контролирует все запускающиеся скрипты на предмет вредоносного кода, включая Java-script[1]ы VB-script.

- ***IM-антивирус.*** Отвечает за безопасность работы с интернет-пейджерами (ICQ, MSN, Jabber, QIP, Mail.RUАгент и т. д.) проверяет и защищает информацию, поступающую по их протоколам.

- ***Контроль программ.*** Этот компонент регистрирует действия программ, запущенных в вашей операционной системе, и регулирует их деятельность на основе установленных правил. Эти правила регламентируют доступ программ к различным ресурсам системы. ***Сетевой экран*** (брандмауэр). Обеспечивает безопасность вашей работы в локальных сетях и интернет, отслеживания во входящем трафике активность, характерную для сетевых атак, использующих уязвимости операционных систем и программного обеспечения. Ко всем сетевым соединениям применяются правила, которые разрешают или запрещают те или иные действия на основании анализа определенных параметров.

- ***Проактивная защита.*** Этот компонент призван выявлять опасное программное обеспечение на основе анализа его поведения в системе. К вредоносному поведению может относиться: активность, характерная для троянских программ, доступ к реестру системы, самокопирование программ в различные области файловой системы, перехват ввода данных с клавиатуры, внедрение в другие процессы и т. д. Таким образом осуществляется попытка защитить компьютер не только от уже известных вирусов, но и от новых, еще не исследованных.

- ***Анти-Спам.*** Фильтрует всю входящую и исходящую почту на предмет нежелательных писем (спама) и сортирует ее в зависимости от настроек пользователя.

---

[1] JavaScript — мультипарадигменный язык программирования. Поддерживает объектно-ориентированный, императивныйи функциональный стили.

- ***Анти-Шпион.*** Важнейший компонент, призванный бороться с мошенничеством в сети интернет. Защищает от фишинг-атак, «бэкдор[2]»-программ, загрузчиков, уязвимостей, взломщиков паролей, захватчиков данных, перехватчиков клавиатуры и прокси-серверов, программ автоматического дозвона на платные вэб-сайты, программ-шуток, программ-реклам и назойливых баннеров.
- ***Родительский контроль.*** Это компонент, позволяющий установить ограничения доступа использования компьютера и интернета. С помощью этого инструмента вы сможете контролировать запуск различных программ, использование интернета, посещение вэб-сайтов в зависимости от их содержимого и многое другое, тем самым ограждая детей и подростков от негативного влияния при работе на компьютере.
- ***Безопасная среда*** или песочница (Sandbox). Ограниченное виртуальное пространство, перекрывающее доступ к ресурсам системы. Обеспечивает защищенную работу с приложениями, документами, интернет-ресурсами, а также с веб-ресурсами интернет-банкинга, где особое значение имеет безопасность при вводе конфиденциальных данных. Так же позволяет внутри себя запускать небезопасные приложения без риска заражения системы.

Основные правила антивирусной защиты

Строго говоря, универсального способа борьбы с вирусами не существует. Даже если на вашем компьютере стоит самая современная антивирусная программа – это абсолютно не гарантирует тот факт, что ваша система не будет заражена. Ведь сначала появляются вирусы, а лишь потом только лекарство от них. И не смотря на то, что многие современные антивирусные решения имеют системы обнаружения еще

[2] **Бэкдор** — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом

неизвестных угроз, их алгоритмы несовершенны и не обеспечивают вам 100% защиту. Но, если придерживаться основных правил антивирусной защиты, то есть возможность существенно снизить риск заражения вашего компьютера и утраты важной информации.

1. В вашей операционной системе должна быть установлена регулярно обновляющаяся хорошая антивирусная программа.
2. Наиболее ценные данные должны быть подвержены резервному копированию.
3. Разбивайте жесткий диск на несколько разделов. Это позволит изолировать важную информацию и не держать ее на системном разделе, куда была установлена ваша ОС. Ведь именно он является основной мишенью злоумышленников.
4. Не посещайте веб-сайты сомнительного содержания и особенно те, которые занимаются незаконным распространением контента, ключей и генераторов ключей к платным программам. Как правило, там, помимо бесплатной «халявы», находится огромное количество вредоносных программ всех разновидностей.
5. При использовании электронной почты не открывайте и не запускайте почтовые вложения из писем от незнакомых адресатов.
6. Всем любителям общения с помощью интернет-пейджеров (QIP, ICQ) так же следует остерегаться скачивания файлов и переходов по ссылкам, присланными незнакомыми контактами.
7. Пользователям социальных сетей следует быть внимательными вдвойне. В последнее время именно они становятся главными объектами кибермошенников, которые придумывают множественные схемы, позволяющие похищать деньги пользователей. Просьба указать свои конфиденциальные данные в сомнительных сообщениях должна немедленно вас насторожить.

ЗАКЛЮЧЕНИЕ

Думаем, после прочтения данного материала, вы теперь понимаете, насколько важно со всей серьезностью отнестись к вопросу безопасности и защищенности вашего компьютера от вторжений злоумышленников, и воздействий на него вредоносными программами. На данный момент существует огромное количество компаний, которые занимаются разработкой антивирусного ПО и как вы понимаете, запутаться с его выбором не составит труда. А ведь это очень ответственный момент, так как именно антивирус является стеной, ограждающей вашу систему от потока заразы, льющейся из сети. И если у этой стены будет много брешей, то и толку-то в ней ноль.

Рисунок 1) Виды угроз

Таблица 1) Источники и виды угроз

Источники	**Виды угроз**
Флоппи-диск	Вредоносное ПО
Жесткий диск	Вредоносное ПО
Локальная сеть	Фишинг
Глобальная сеть Интернет	Фишинг, спам, хакерские атаки

Рисунок 2) Как выглядит хакер в 90-х

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos \frac{n\pi x}{L} + b_n \sin \frac{n\pi x}{L} \right)$$

Рисунок 3) Как выглядит хакер в 2015

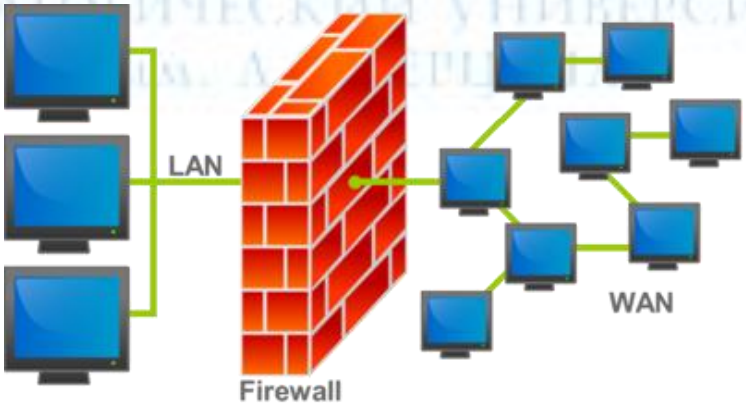

Рисунок 4) Принцип работы брандмауэра