Компьютерные вирусы.

Типы, виды, пути заражения

Компьютерный вирус —

- **Это специально написанная программа или сборка алгоритмов которые пишутся с целью: пошутить, навредить чьему либо компьютеру, получение доступа к вашему компьютеру, для перехвата паролей или вымогания денег. Вирусы могут само-копироваться и заражать вредоносным кодом ваши программы и файлы, а так же загрузочные сектора.**

Виды вредоносных программ.

- **Разделить вредоносные программы можно на два основных вида. Вирусы и черви.**

Вирусы -

- - распространяются через вредоносный файл, который вы могли скачать в интернете, или может оказаться на пиратском диске, или часто передают их по скайпу под видом полезных программ (заметил что на последнее часто попадаются школьники, им передают якобы мод для игры или читы а на самом деле может оказаться вирусом который может навредить).
  Вирус вносит свой код одну из программ, либо маскируется отдельной программой в том месте куда обычно пользователи не заходят (папки с операционной системой, скрытые системные папки).
  Вирус не может запуститься сам, пока вы сами не запустите зараженную программу.

Черви

- *заражают уже множество файлов вашем компьютере, например все exe файлы, системные файлы, загрузочные сектора и тд.*
- *Черви чаще всего проникают в систему уже сами, используя уязвимости вашей ОС, вашего браузера, определенной программы.*
- *Они могут проникать через чаты, программы для общения такие как skype, icq , могут распространяться через электронную почту.*
- *Так же они могут быть на сайтах, и используя уязвимость вашего браузера проникнуть в вашу систему.*
- *Черви могут распространяться по локальной сети, если один из компьютеров в сети окажется заражен он может распространяться на остальные компьютеры заражая все файлы на своём пути.*
- *Черви стараются писать под самые популярные программы. Например сейчас самый популярный браузер «Chrome», поэтому мошенники будут стараться писать под него, и делать вредоносный код на сайты под него. Потому что часто интереснее заразить тысячи пользователей которые используют популярную программу чем сотню с непопулярной программой. Хотя chrome и постоянно улучшает защиту.*
- *Лучшая защита от сетевых червей это обновлять ваши программы и вашу операционную систему. Многие пренебрегают обновлениями о чем часто жалеют.*
- *Несколько лет назад я замечал следующий червь.*
- *Но он явно попал не через интернет а скорее всего через пиратский диск. Суть его работы была таковой — он создавал будто бы копию каждой папки в компьютере или на флешке. Но на самом деле он создавал не похожую папку а exe файл. При нажатии на такой exe файл он распространялся ещё сильнее по системе. И вот было только избавишься от него, придешь к другу с флешкой, скинуть у него музыку а возвращаешься с зараженной таким червем флешку и снова приходилось его выводить. Наносил ли этот вирус какой то ещё вред*

Основные разновидности вирусов.

- На самом деле существует множество видов и разновидностей компьютерных угроз. И все рассмотреть просто невозможно. Поэтому мы рассмотрим самые распространенные в последнее время и самые неприятные.
  Вирусы бывают :
  — **Файловые** — находятся в зараженном файле, активируются когда пользователь включает эту программу, сами не могут активироваться.
  — **Загрузочные** — могут загружаться при загрузке windows попав в автозагрузку, при вставке флешки или подобное.

- Макро вирусы

- **- это различные скрипты которые могут находиться на сайте, могут прислать их вам по почте или в документах Word и Excel , выполняют определенные функции заложенные в компьютере. Используют уязвимости ваших программ.**

ОПРЕДЕЛЕНИЕ!!!

- **Типы вирусов.**
  -Троянские программы
  - **Шпионы**
  - **Вымогатели**
  - **Вандалы**
  - **Руткиты**
  - **Botnet**
  - **Кейлогеры**

Это самые основные виды угроз которые могут вам встретиться. Но на самом деле их намного больше.

Некоторые вирусы могут даже комбинироваться и содержать в себе сразу несколько видов этих угроз.

— Троянские программы.

- Название происходит от троянского коня. Проникает в ваш компьютер под видом безвредных программ, потом может открыть доступ к вашему компьютеру или переслать ваши пароли хозяину.
  В последнее время распространены такие трояны которые называются стилеры (stealer). Они могут воровать сохраненные пароли в вашем браузере, в почтовых игровых клиентах. Сразу после запуска копирует ваши пароли и отправляет ваши пароли на email или на хостинг злоумышленнику. Ему остается собрать ваши данные, потом их либо продают либо используют в своих целях.

— Шпионы (spyware)

-) отслеживают действия пользователя. Какие сайты посещает или что делает пользователь на своём компьютере.

— Вымогатели

- . К ним относятся Винлокеры (winlocker). Программа полностью, или полностью блокирует доступ к компьютеру и требует деньги за разблокировку, на пример положить на счет или тд . Ни в коем случае если вы попали на такое не стоит пересылать деньги. Компьютер вам не разблокируется , а деньги вы потеряете. Вам прямая дорога на сайт компании Drweb , там можно найти как разблокировать многие винлокеры , за счет ввода определенного кода или выполнения некоторых действий. Некоторые винлокеры могут пропасть например через день.

— Вандалы

- могут блокировать доступы к сайтам антивирусов и доступ к антивирусам и многим другим программам.

— Руткиты

- (rootkit) — вирусы гибриды. Могут содержать в себе различные вирусы. Могут получать доступ к вашему пк, и человек будет полностью иметь доступ к вашему компьютеру, причем могут слиться на уровень ядра вашей ОС. Пришли из мира Unix систем. Могут маскировать различные вирусы, собирать данные о компьютере и обо всех процессах компьютера.

— Botnet

- достаточно неприятная вещь. Ботнеты это огромные сети из зараженных компьютеров «зомби», которые могут использоваться для ддоса сайтов и прочих кибер атак, используя зараженные компьютеры. Этот вид очень распространен и его тяжело обнаружить, даже антивирусные компании могут долго не знать о их существовании. Очень многие могут быть ими заражены и даже не подозревать об этом. Не исключении вы и даже может и я.

— **Кейлогеры** (keylogger)

- – клавиатурные шпионы . Перехватывают всё что вы вводите с клавиатуры (сайты, пароли) и отправляет их хозяину.

Пути заражения компьютерными вирусами.

- Основные пути заражения.
- — Уязвимость операционной системы.
- — Уязвимость в браузере
- — Качество антивируса хромает
- — Глупость пользователя
- — Сменные носители.
- Уязвимость ОС — как бы не старались клепать защиту для ОС со временем находятся дыры безопасности. Большинство вирусов пишется под windows так как это самая популярная операционная система. Лучшая защита это постоянно обновлять вашу операционную систему и стараться использовать более новую версию.
- Браузеры — Здесь происходит за счёт уязвимостей браузеров, особенно если они опять же старые. Лечится так же частым обновлением. Так же могут быть проблемы если вы качаете плагины для браузера со сторонних ресурсов.
- Антивирусы — бесплатные антивирусы которые имеют меньший функционал в отличие от платных. Хотя и платные не дают 100 результата в защите и дают осечки. Но желательно иметь всё же хотя бы бесплатный антивирус. Я уже писал про бесплатные антивирусы в этой статье.
- Глупость пользователя — клики по баннерам, переходи по подозрительным ссылкам из писем и тд, установка софта из подозрительных мест.
- Сменные носители — вирусы могут устанавливаться автоматически с зараженных и специально подготовленных флешек и прочих сменных носителей. Не так давно мир услышал про уязвимость BadUSB.

Виды заражаемых объектов.

- **Файлы — Заражают ваши программы, системные и обычные файлы. Загрузочные секторы — резидентные вирусы. Заражают как понятно из названия загрузочные сектора компьютера, приписывают свой код в автозагрузку компьютера и запускаются при запуске операционной системе. Порою хорошо маскируются что трудно убрать из автозагрузки.**
  Макрокоманды — Документы word, excel и подобные. Использую макросы и уязвимости средств Microsoft office вносит свой

Признаки заражения компьютерными вирусами.

- Не факт что при появлении некоторых из этих признаков означает наличие вируса в системе. Но если они имеются рекомендуется проверить свой компьютер антивирусом или обратиться к специалисту.
- Один из распространенных признаков — это сильная перегрузка компьютера. Когда у вас медленно работает компьютер, хотя у вас ничего вроде бы не включено, программ которые могут сильно нагружать компьютер. Но если у вас антивирус заметьте антивирусы сами по себе нагружают компьютер очень хорошо. А в случае отсутствия такого софта который может грузить то скорее тут вирусы. Вообще советую по уменьшить для начала количество

Медленная загрузка программ, так же может быть одним из признаков заражения.
Но не все вирусы могут сильно нагружать систему, некоторые практически трудно заметить изменения.
Системные ошибки. Перестают работать драйвера, некоторые программы начинают работать не правильно или часто вылетают с ошибкой но раньше допустим такого не замечалось. Или начинают часто перезагружаться программы. Конечно такое бывает из за антивирусов, например антивирус удалил по ошибке посчитав системный файл вредоносным, либо удалил действительно зараженный файл но

Появление рекламы в браузерах или даже на рабочем столе начинают появляться баннеры.

Появление не стандартных звуков при работе компьютера (писк, щелчки ни с того ни с сего и подобное).

Открывается сам по себе CD/DVD привод, или просто начинает словно читать диск хотя диска там нет.

Длительное включение или выключение компьютера.

Угон ваших паролей. Если вы заметили что от вашего имени рассылается различный спам, с вашего почтового ящика или странички социальной сети, как вероятность что вирус проник в ваш компьютер и передал пароли хозяину, если вы заметили такое рекомендую провериться антивирусом в обязательном порядке (хотя не факт что именно так злоумышленник получил ваш пароль).

Частое обращение к жесткому диску. У каждого компьютера есть индикатор, который мигает когда используют различные программы или когда копируете, скачиваете, перемещаете файлы. Например у вас просто включен компьютер но не используется никаких программ, но индикатор начинает часто мигать якобы используются программы. Это уже вирусы на уровне жесткого диска.

Вот собственно и рассмотрели **компьютерные вирусы** которые могут вам встретиться в интернете. Но на самом деле их в разы больше, и полностью защититься не возможно, разве что не пользоваться интернетом, не покупать диски и вообще не включать компьютер.