5. Shields, Earl B. 1982. Raising Earthworms for Profit.

КОМПЬЮТЕРНЫЕ ВИРУСЫ

Н.А. Панова, М.А.Маркова , 2 курс, факультет математики и информационных технологий
Научный руководитель - к.п.н, доцент кафедры немецкого и французского языков С.Ю. Баракина
ФГОУ ВПО «Ульяновский государственный университет»

Перевод статьи «Computervirus»

Компьютерный вирус *(вирус* lat. "яд", "слизь", в разговорной речи употребляется "компьютерный вирус", множественное число "компьютерные вирусы") является самораспространяющейся компьютерной программой, которая проникает в другие компьютерные программы и таким образом, воспроизводится. По классификации вирус относится к самораспространяющейся инфекционной функции.

Как только вирус запущен, пользователь не может контролировать изменения в техническом обслуживании (для примера: сеть связи) операционной системы или программного обеспечения (вредная функция). Компьютерные вирусы могут вмешиваться в желаемые или не желаемые функции компьютера пользователя и считаются вредоносными программами.

Термин «компьютерный вирус» используется для компьютерных червей и троянских лошадей, для пользователя переход от одних к другим, между тем, зачастую не заметен. Компьютерные вирусы и черви распространяются на компьютерах и в системах, но они частично основаны на совершенно различных концепциях и методах.

Вирус распространяется, в то время как копирует себя самого еще на не зараженные файлы, а затем настраивает их таким образом, что вирус запускается при запуске программы - носителя. К зараженным файлам относятся нормальные программные файлы, программы библиотек, скрипты, документы с макросами и другим выполнимым содержанием, а так же загрузочные секторы (даже, если последние не представляются операционной системой как файл).

Распространение на новые системы осуществляется путем копирования зараженного файла, при приёме пользователем новых систем. При этом несущественно на каком пути скопирован хост файл: первоначально, основные каналы распределения съёмных носителей были дискеты, сейчас существуют компьютерные сети (например через электронную почту, отправленную по FTP, web-серверы или места обмена). Существуют так же вирусы, которые инфицируют файлы в освобожденных регистрах в сетях LAN, если они владеют соответствующими правами.

Загрузочные вирусы входят в число старейших компьютерных вирусов. До 1995 года эти вирусы считались самыми распространенными. Загрузочный

вирус заражает загрузочные сектора дискет и разделы жестких дисков, или Master Boot Record (MBR). С 2005 года существуют вирусы загрузочного сектора на CD-ROM.

Не все компьютерные вирусы явно относятся к особой категории. Есть также гибриды, которые заражают как файлы, так и загрузочные секторы (например, ядро), вирусы и макро-вирусы, которые также заражают программу файлов.

Тестовый файл EICAR представляет собой файл, который используется для тестирования антивирусных сканеров. Он не является вирусом. Каждый антивирусный сканер должен определить этот файл. Поэтому он может быть использован для доступа к системе, которая была заражена каким-либо вирусом - будь то вирус, сканер работает нормально.

Антивирусные программы имеют защиту, по существу только от известных вирусов. Таким образом, важно при использовании такой программы вводить регулярно предоставленные производителями обновления, которые не могут быть обнаруженны активирусным программным обеспечением.

С помощью этих программ осматривается память и диски на наличие вредных программ.

Антивирусы предлагаются в 2-х режимах: в ручном, при котором антивирус проверяет все файлы однократно, и автоматически только по приглашению пользователя, и автомат, при котором все письменные доступы и доступы чтения к жесткому диску и часть памяти будут рассмотрены. Существуют антивирусные программные модули для более точного сканирования на наличие вирусов.

Антивирусные программы никогда не предлагают полную защиту, так как уровень обнаружения вирусов не 100%. Неизвестные вирусы, могут быть обнаружены на основе их поведения (большинство из этих программ, „эвристические“), эти функции работают очень ненадежно.Также антивирус не обнаруживает вирусы после инфекции и не может удалять вирус при определенных обстоятельствах в нормальном режиме.

Там, где есть разумные основания подозревать, инфекцию, программы on-demand применяется по-очереди. При этом имеет смысл обращать внимание на то, чтобы программы использовали разные двигатели, чтобы уровень узнавания увеличивался. Есть антивирусные программы разных производителей, которые применяют те же методы сканирования, в основном имеют высокую вероятность обнаружения и вместе с тем также похожий риск обозревать определенные вирусы.

Пользователи не должны запускать неизвестные файлы или программы из небезопасных источников и при открытии файлов проявлять осторожность. Это считается, в частности, для файлов, которые принимаются по E-Mail.Такие файлы даже, казалось бы, безобидные документы, такие как изображения или PDF документы – могут через уязвимости в защите, в соответствующих приложениях, активировать разными способами вредоносные программы. Поэтому нужно рекомендовать их перепроверку с актуальным антивирусом.

Операционная система и приложения должны быть регулярно обновлены и вводиться, производителем представленного сервиса, пакеты обновления и патчи/управления.При этом нужно обращать внимание, что установка патча может занять некоторое время. Несколько операционных систем упрощают эту

процедуру, в то время как они поддерживают автоматическое сгружение и установку модернизации.

Встроенные функции защиты операционной системы должны быть использованы. Для этого работать , в частности, не как администратор со всеми правами, как пользователь с ограниченными правами, так как он в маштабах системы он не может устанавливать программное обеспечение.

Персональные брандмауэры не показывают против вирусов никакого эффекта, поскольку их функциональность с учетом функционирования червей и вирусов не затрагиваются.

Литература:

1. Amberg Eric - *Sicherheit im Internet*.- Hamburg. - 2004 (перевод).

2. [электронный ресурс] http://www.computec.ch/download.php?list.14 Computervirus (дата обращения: 25.02.2010)

ОБЩИЕ ПОНЯТИЯ О МЕТАЛЛУРГИИ

В.А. Фрилинг, аспирант, инженерный факультет
Научный руководитель – к.п.н., доцент С.Ю. Баракина
ФГОУ ВПО «Ульяновская ГСХА»

Перевод статьи « Allgemeines über Metallurgie »

Металлургия охватывает все технические процессы по производству металлических материалов: железо, сталь, алюминий, медь, свинец, цинк, олово и благородные металлы, а также их дальнейшую обработку по отливкам или полуфабрикатам.

Металлические материалы во всех отраслях экономики, в частности, в машиностроении, транспортном машиностроении, в электронной индустрии и строительстве являются основой созданных товаров широкого потребления. Для обеспечения необходимых качеств различного назначения металлические материалы производятся в результате множества различных процессов, при которых речь всегда идет о высоких процессах температуры, связанных с высокой затратой энергии в форме горючего или электроэнергии.

Производство чугуна и стальное производство занимается добычей чугуна в доменной печи и его дальнейшим превращением в сталь в различных стальных агрегатах путем обработки оксидирующими газами, а также последующим отливанием.

Чугуном называется железо - углеродистый сплав с содержанием углерода > 2%, а также кремния, марганца, фосфора и серы разного значения. Сегодня чугун производится исключительно в доменной печи и превращается в результате разных процессов в сталь. Только 10% чугуна используются вместе с железным ломом для производства. Производство стали при обработке в доменной печи (чугун) путём измельчения руды в твердом состоянии и её дальнейшей обработки в электрических печах составляет только 1,5% всемирного