прямо рассказывающие об ее содержании, а лишь ассоциативно связанные с ним.

В изданиях с художественными иллюстрациями рисунок на обложке или суперобложке имеет особое значение — он открывает всю сюиту иллюстраций. Броскость помогает заметить книгу на витрине книжного магазина, и это имеет рекламное значение, но в наших условиях в настоящее время это далеко не всегда существенно. Все графические элементы — шрифтовые надписи, изображения, помещенные на обложке,— должны быть композиционно объединены. Печать на обложке и переплете очень часто делается в несколько красок, и их удачное сочетание с цветом и фактурой бумаги и переплетных материалов позволяет получить большой художественный эффект.

УДК 004.491.22

КОМПЬЮТЕРНЫЕ ВИРУСЫ. ВОЗНИКНОВЕНИЕ И МЕТОДЫ БОРЬБЫ

Онуфриенко С.Г., ст. преп., Сотникова Д.С., студ.

Витебский государственный технологический университет,
г. Витебск, Республика Беларусь

Реферат. *В статье рассматриваются вопросы создания, распространения и борьбы против компьютерных вирусов.*

Ключевые слова: компьютерный вирус, спам, черви-ботнеты.

Компьютеры в наше время выполняют множество задач. Рынок IT процветает и развивается, появляются новые интернет-проекты и сервисы. Сегодня массовое применение персональных компьютеров, оказалось связанным с появлением программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению (саморепликация). Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, становится неработоспособной или же окажется под полным контролем злоумышленника.

Вирусы не возникают сами по себе, а создаются людьми. Наиболее вероятными причинами, толкающими вирусо-писателей на создание и распространение вредоносного программного обеспечения являются:

- обычное юношеское хулиганство, попытки самоутверждения на основе достигнутого интеллектуального уровня;
- мошенничество с целью присвоения ресурсов жертвы: незаметное управление пораженным компьютером, воровство паролей доступа в Интернет, средств с "кошельков" WebMoney и кодов доступа к персональным банковским. В случае, если атакой подверглись корпоративные сети, то речь идет уже о шпионаже.

Основную массу вирусов создают студенты и школьники, которые только что изучили язык программирования и хотят попробовать свои силы.

Вторую группу составляют также молодые люди (чаще - студенты), которые решили посвятить себя написанию и распространению вирусов. Как правило, они создают многочисленные модификации "классических" вирусов, либо вирусы крайне примитивные. Часто они используют конструкторы вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе. Став старше и опытнее, многие из этих вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир "профессиональные" вирусы. Это тщательно продуманные и отлаженные программы.

Четвертая группа авторов вирусов - "исследователи". Эта группа состоит из талантливых программистов, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради "исследования" потенциалов "компьютерной вирусологии".

На сегодняшний день компьютерному вирусу уже более тридцати лет. Первыми известными вирусами являются Virus 1,2,3 и ElkClonerдля ПК Apple II, появившиеся в 1981 году. Первые вирусные эпидемии относятся к 1987 - 1989 годам: Brain(более 18 тысяч зараженных компьютеров, (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске)), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).В несколько последующих лет были испробованы самые необычные способы проникновения в систему и заражения файлов (Dir II — 1991, PMBS, Shadowgard, Cruncher— 1993). Кроме того, появились вирусы, заражающие объектные файлы (Shifter, 1994) и исходные тексты программ (SrcVir, 1994). С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (Melissa, 1999 - макровирус и сетевой червь, побивший все рекорды по скорости распространения).В 2004 году беспрецедентные по масштабам эпидемии вызывают черви-эксплоиты, MsBlast (по данным Microsoft - более 16млн систем), Sasser и Mydoom(оценочные ущербы 500 млн и 4 млрд долл.).

Самый современный вид вирусов - черви-ботнеты всё больше набирают обороты (Rustock, 2006, ок. 150 тыс. ботов; Conficker, 2008-2009, более 7 млн ботов; Kraken, 2009, ок. 500 тыс. ботов). Вирусы в числе прочего вредоносного ПО окончательно оформляются как средство киберпреступности. Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы MicrosoftWord и Excel, содержащие макросы. Кроме того, для проникновения на компьютер, вирус может использовать уязвимости в популярном программном обеспечении (например, AdobeFlash, InternetExplorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

Способы распространения компьютерных вирусов разнообразны, однако существуют все же наиболее распространенные, от которых можно уберечься, соблюдая элементарные меры предосторожности.

Флеш-накопители (флешки). В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы).

Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код.

Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. Интернет и локальные сети (черви). Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама.

Для предотвращения заражения необходимо соблюдать элементарные меры предосторожности: стараться использовать только проверенные ресурсы в сети Интернет; не скачивать сомнительные программы, а также не нажимать сомнительных картинок;при получении писем от неизвестного адресата, обращать внимание на расширение приложенных файлов. Если они имеют такие типы как:*.bat,*.vbs,*.scr,*.exe, то не стоит скачивать эти приложения, они могут быть заражены или попросту являются вирусом трояном.

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;

- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размера файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Заразиться компьютерным вирусом можно только в определенных случаях:

- запуск на компьютере исполняемой программы, заражённой вирусом;
- загрузка компьютера с диска (дискеты), содержащего загрузочный вирус;
- подключение к системе заражённого драйвера;
- открытие документа, заражённого макровирусом;
- установка на компьютере заражённой операционной системы.

Главным оружием в борьбе с вирусами являются антивирусные программы. Они позволяют не только обнаружить вирусы, но и удалить их из компьютера. Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем, на процессорах различных типов.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Антивирус Касперского - обеспечивает защиту в реальном времени от вирусов, червей, троянских коней, руткитов, adware, шпионских программ, в том числе и неизвестных угроз, используя проактивную защиту.

Eset NOD32 -представляет полную защиту компьютера. Комплексная защита компьютера функционирует в реальном времени и обеспечивает надежную защиту от вирусов и вредоносных программ, а так же других угроз, таких как фишинг-атаки, черви, spyware, adware и другие.

Norton (Symantec)-базовая антивирусная защита, блокирующая вирусы и программы-шпионы и позволяющая безопасно работать в Интернете и обмениваться информацией .

Доктор Веб - базовая антивирусная защита, блокирующая вирусы и программы-шпионы и позволяющая безопасно работать в Интернете и обмениваться информацией.

Avira - AAviraAntivirusPremium - защита от вирусов для персональных компьютеров, работающих под управлением ОС Windows .

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

УДК 659.12

ВИЗУАЛЬНАЯ ПОДДЕРЖКА КАФЕДРЫ ИЗОБРАЗИТЕЛЬНОГО ИСКУССТВА ХУДОЖЕСТВЕННО-ГРАФИЧЕСКОГО ФАКУЛЬТЕТА ВГУ ИМ. П.М. МАШЕРОВА

Кириллова И.Л., ст. преп., Власенков М.И., студ.

Витебский государственный технологический университет,
г. Витебск, Республика Беларусь

Реферат. *В статье рассмотрены концепции для разработки информационно-*