Компьютерные вирусы

ОПРЕДЕЛЕНИЕ

- ***Компью́терный ви́рус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.***

ИСТОРИЯ

- Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.[3]
- Первыми известными собственно вирусами являются Virus 1.2.3 и Elk Cloner для ПК Apple II, появившиеся в1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторстваЭнди Хопкинса (англ. *Andy Hopkins*). В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу DPROTECT — первый резидентный антивирус.
- Первые вирусные эпидемии относятся к 1987—1989 годам: Zotkin.A, Kharitonov.D (более 18 тысяч зараженных компьютеров, по данным McAfee[*источник не указан 1602 дня*]), Jerusalem (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске[4]), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).
- Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989[5]), полиморфные вирусы\\ (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).
- Параллельно оформляются организованные движения как про-, так и антивирусной направленности: в 1990 году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton AntiVirus.
- В 1992 году появились первый конструктор вирусов для PC — VCL (для Amiga конструкторы существовали и ранее), а также готовые полиморфные модули (MtE, DAME и TPE) и модули шифрования для встраивания в новые вирусы.

- *В несколько последующих лет были окончательно отточены стелс- и полиморфные технологии (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а также 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 пакета Microsoft Office получили распространение макровирусы (Concept, 1995).*
- *В 1996 году появился первый вирус для Windows 95 — Win95.Boza, а в декабре того же года — первый резидентный вирус для неё — Win95.Punch.*
- *С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (ShareFun, 1997 — макровирус MS Word, использующий MS-Mail для распространения; Win32.HLLP.DeTroie, 1998 — семейство вирусов-шпионов; Melissa, 1999 — макровирус и сетевой червь, побивший все рекорды по скорости распространения). Эру расцвета «троянских коней» открывает утилита скрытого удаленного администрирования BackOrifice (1998) и последовавшие за ней аналоги (NetBus, Phase).*
- *Вирус Win95.CIH достиг апогея в применении необычных методов, перезаписывая FlashBIOS зараженных машин (эпидемия в июне 1998 считается самой разрушительной за предшествующие годы).*
- *В конце 1990-х — начале 2000-х годов с усложнением ПО и системного окружения, массовым переходом на сравнительно защищенные Windows семейства NT, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий в обнаружении вирусов, построенных по сложным алгоритмам, последние стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный автозапуск, руткиты) и подменять полиморфизм огромным количеством видов (число известных вирусов растет экспоненциально).*

Этимология названия

- Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах»[8], опубликованном в журнале Venture в мае 1970 года.
- Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в подпрограмме PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер и, вероятно, это и было то, что впервые было правильно обозначено как вирус.

Классификация

- Нынче существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.
- В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:
- по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

РАСПРОСТРОНЕНИЕ
МЕХАНИЗМЫ

- 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 документыMicrosoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer,Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе сэксплоитом, использующим уязвимость.

Каналы

- Дискеты. Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.
- 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). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windowsпри открытии такого накопителя. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.
- 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. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

- ***Системы обмена мгновенными сообщениями**. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другиепрограммы мгновенного обмена сообщениями.*
- ***Веб-страницы**. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.*

- ***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. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.*