Лекция 15. Защита от вредоносных программ

1. Вредоносные программы и их классификация.
2. Загрузочные и файловые вирусы.
3. Методы обнаружения и удаления вредоносных программ.

Вредоносные программы

- К *вредоносным программам* (иначе называемым *разрушающими программными воздействиями*, malware) относятся компьютерные вирусы и программные закладки.
- Впервые термин *компьютерный вирус* ввел в употребление специалист из США Ф.Коэн в 1984 г.

Компьютерный вирус

Автономно функционирующая программа, обладающая одновременно тремя свойствами:

- способностью к включению своего кода в тела других файлов и системных областей памяти компьютера;
- последующему самостоятельному выполнению;
- самостоятельному распространению в компьютерных системах.

Программная закладка

- Внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными разрушительными функциями по отношению к этой системе.
- Внесенный в ПО функциональный объект, который может инициировать выполнение недокументированных функций, позволяющих осуществлять несанкционированное воздействие на информацию (ГОСТ Р 51275-99).

Классификация компьютерных вирусов

1. По способу распространения в компьютерной системе:
   - файловые вирусы, заражающие файлы одного или нескольких типов;
   - загрузочные вирусы, заражающие загрузочные сектора жестких дисков и дискет;
   - комбинированные вирусы, способные заражать и файлы, и загрузочные сектора дисков.

Классификация компьютерных вирусов

2. По способу заражения других объектов компьютерной системы:
   - резидентные вирусы, часть кода которых постоянно находится в оперативной памяти компьютера и заражает другие объекты;
   - нерезидентные вирусы, которые заражают другие объекты в момент открытия уже зараженных ими объектов.

Классификация компьютерных вирусов

3. По деструктивным возможностям:
   - безвредные вирусы, созданные в целях «обучения», однако снижающие эффективность работы компьютерной системы за счет потребления ее ресурсов;
   - неопасные вирусы, создающие различные звуковые и видеоэффекты;
   - опасные и очень опасные вирусы, вызывающие сбои в работе программного и (или) аппаратного обеспечения компьютера, потерю программ и данных, а потенциально – вывод из строя аппаратуры КС и нанесение вреда здоровью пользователей.

Классификация компьютерных вирусов

4. По особенностям реализуемого алгоритма:
   - вирусы-спутники, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы (при открытии зараженного файла фактически открывается файл с кодом вируса, в котором после выполнения предусмотренных автором действий открывается исходный файл);
   - паразитические вирусы, которые обязательно изменяют содержимое заражаемых объектов;

Классификация компьютерных вирусов

- вирусы-невидимки («стелс»-вирусы), в которых путем перехвата обращений операционной системы к зараженным объектам скрывается факт присутствия вируса в компьютерной системе (при собственном обращении к дисковой памяти вирусы-невидимки также используют нестандартные средства для обхода средств антивирусной защиты);

Классификация компьютерных вирусов

- вирусы-призраки (полиморфные вирусы), каждая следующая копия которых в зараженных объектах отличается от предыдущих (не содержит одинаковых цепочек команд за счет применения шифрования на различных ключах базового кода вируса).

Программные закладки

- «логические бомбы» – уничтожение или внесение изменений в функционирование программного обеспечение компьютерной системы, уничтожение или изменение обрабатываемых в ней данных после выполнения некоторого условия или получения некоторого сообщения извне;
- «троянские» программы – предоставление нарушителю доступа к конфиденциальной информации других пользователей компьютерной системы путем ее копирования и (или) передачи по сети;

Программные закладки

- мониторы – перехват потока информации, передаваемой между объектами распределенной компьютерной системы;
- компьютерные «черви» – распространение в распределенных компьютерных системах с целью реализации той или иной угрозы безопасности информации (в отличие от компьютерных вирусов не должны обладать свойством включения своего кода в тела других файлов);

Программные закладки

- перехватчики паролей пользователей компьютерной системы – имитация приглашения к их вводу или перехват всего ввода пользователей с клавиатуры;
- программы, подменяющие отдельные функции подсистемы защиты компьютерной системы;
- программы-«злые шутки», затрудняющие работу с компьютером и сообщающие пользователю заведомо ложную информацию о своих действиях в компьютерной системе;

Программные закладки

- «ботнеты», предназначенные для создания зомби-сетей и рассылки спама, распределенных атак с вызовом отказа в обслуживании (DDoS-атак), внедрения троянских прокси-серверов;
- «руткиты», предназначенные для скрытия следов присутствия нарушителя или вредоносной программы в системе;
- «эксплойты» (общий термин для программного кода, используемого для атаки на КС) и др.

Загрузочные вирусы

Заражают главный загрузочный сектор жесткого диска (Master Boot record, MBR) или загрузочный сектор раздела жесткого диска, системной дискеты или загрузочного компакт-диска (Boot Record, BR), подменяя находящиеся в них программы начальной загрузки и загрузки операционной системы своим кодом.

Загрузочные вирусы

Получают управление сразу по завершении работы процедуры проверки оборудования (POST), программы BIOS Setup (если она была вызвана пользователем), процедур BIOS и его расширений.

Загрузочный вирус

После получения управления выполняет следующие действия:

- копирование своего кода в конец оперативной памяти компьютера;
- переопределение «на себя» нескольких прерываний BIOS, в основном связанных с обращением к дискам;

Загрузочный вирус

- загрузка в оперативную память компьютера истинной программы начальной загрузки, в функции которой входит просмотр таблицы разделов жесткого диска, определение активного раздела, загрузка и передача управления программе загрузки операционной системы активного раздела;
- передача управления истинной программе начальной загрузки.

«Буткиты»

«Руткиты» с функцией загрузки из загрузочных секторов любых устройств. Их опасность состоит в том, что вредоносный код получает управление еще до старта ОС, а значит и антивирусной программы.

Файловые вирусы

Заражают файлы различных типов:

- программные файлы, файлы драйверов устройств и других модулей операционной системы;
- файлы документов, которые могут содержать внутри себя макросы;
- файлы документов, которые могут содержать внутри себя сценарии (скрипты) или отдельные файлы сценариев и др.

Файловые вирусы

Записывают свой код в начало, середину или конец файла либо сразу в несколько мест. Исходный файл изменяется таким образом, чтобы после открытия файла управление было немедленно передано коду вируса.

Вирусы в макросах

Условия, благоприятствующие их созданию:

- Возможность включения в документ макроса.
- Языки программирования макросов, особенно VBA, являются универсальными языками, позволяющими создавать достаточно сложные процедуры.
- Поддержка автоматически выполняемых макросов, связанных с определенными событиями (например, открытием документа) или определенными действиями.

Основные каналы распространения вредоносных программ

- электронная почта, сообщения которой могут быть заражены или содержать зараженные присоединенные файлы;
- свободное и условно свободное программное обеспечение, размещенное на общедоступных узлах сети Интернет и случайно или намеренно зараженное вредоносным кодом;

Основные каналы распространения вредоносных программ

- размещенные на общедоступных узлах сети Интернет информационные ресурсы, содержащие ссылки на зараженные файлы с элементами управления Active-X;
- локальные компьютерные сети организаций, создающие удобную среду для заражения вирусами объектов на других рабочих станциях и серверах;

Основные каналы распространения вредоносных программ

- обмен зараженными файлами на съемных носителях между пользователями компьютерной системы;
- использование нелицензионного программного обеспечения и других информационных ресурсов.

Методы предупреждения вирусного заражения

- физическое или логическое (для отдельных учетных записей) отключение накопителей для съемных дисков;
- разграничение прав отдельных пользователей и групп на доступ к папкам и файлам операционной системы и других пользователей;
- ограничение времени работы в компьютерной системе привилегированных пользователей;

Методы предупреждения вирусного заражения

- использование, как правило, только лицензионного программного обеспечения, приобретенного у официальных представителей фирм-правообладателей;
- выделение не подсоединенного к локальной сети компьютера для тестирования полученного из ненадежных источников программного обеспечения;

Методы предупреждения вирусного заражения

- использование встроенной в Microsoft Office защиты от потенциально опасных макросов, разрешающей в зависимости от установленного уровня выполнение макросов, содержащихся в документах из надежных расположений, подписанных доверенными издателями или разрешенных пользователем после получения соответствующего предупреждения.

Методы обнаружения компьютерных вирусов

1. Просмотр (сканирование) проверяемых объектов (системных областей дисковой и оперативной памяти, а также файлов заданных типов) в поиске сигнатур (уникальных последовательностей байтов) известных вирусов. Недостатки: необходимость постоянного обновления баз данных сигнатур известных вирусов, неспособность обнаружить новые компьютерные вирусы.

Методы обнаружения компьютерных вирусов

2. Инспекция (обнаружение изменений в объектах компьютерной системы) путем сравнения их вычисленных при проверке хеш-значений с эталонными (или проверки ЭЦП для этих объектов). Недостатки: не все изменения проверяемых объектов вызываются вирусным заражением, не может помочь при записи на жесткий диск компьютера пользователя уже зараженного файла.

Методы обнаружения компьютерных вирусов

3. Эвристический анализ – проверка системных областей памяти и файлов с целью обнаружения фрагментов исполнимого кода, характерного для компьютерных вирусов. Недостатки: длительность процедуры проверки, возможность ложных сообщений о найденных вирусах.

Методы обнаружения компьютерных вирусов

4. Мониторинг – постоянное присутствие в оперативной памяти компьютера с целью сканирования всех открываемых или получаемых извне файлов и контроля всех «подозрительных» действий других программ. Недостатки: снижение эффективности работы системы, возможность выполнения контролируемых действий незараженными программами.

Методы обнаружения компьютерных вирусов

5. Вакцинирование – присоединение к защищаемому файлу специального модуля контроля, следящего за целостностью данного файла с помощью вычисления его хеш-значения и сравнения с эталоном. Недостатки: возможность обхода вирусами-невидимками , неприменимость для защиты файлов документов.

Методы обнаружения компьютерных вирусов

6. Блокирование потенциально опасных действий пользователя:
   - Установка параметров безопасности и конфиденциальности в обозревателе Интернета.
   - Установка защиты от записи в загрузочные сектора с помощью программы BIOS Setup.
   - Определение недоступных для изменения областей дисковой памяти с помощью драйвера PCI-контроллера.

Удаление обнаруженных вирусов

1. Автоматическое – с помощью заранее разработанного алгоритма «лечения» зараженных известным вирусом объектов.
2. Автоматическое или «ручное» удаление зараженного объекта (с его последующим восстановлением по сохраненной незараженной резервной копии). Иногда возможно автоматическое восстановление объекта соответствующей программой (например, файла normal.dot программой Microsoft Office Word).

Удаление обнаруженных вирусов

3. Полная переустановка системы, включая форматирование дисковой памяти, восстановление главного загрузочного сектора, установку операционной системы и прикладного программного обеспечения, восстановление файлов данных с резервных носителей информации.