

Классификация вредоносных продуктов с точки зрения AVT Group.

Нохрин Матвей Сергеевич

ПС-194

AVT Group

Пути решения

1. Воспользоваться готовой классификацией.
2. Создать собственную на основе существующих.

Первоначальный список

1. Вирусы – программа, написанная таким образом, что она саму себя встраивает в операционную систему и повреждает файлы или мешает работе компьютера.
2. Черви – небольшая программа, подключаемая кем-либо к программе, чтобы привести к сбою в системе.
3. Трояны – программа, которая имеет внешние признаки обычной, но при запуске начинает изменять файлы или стирать их.

Классификация вирусов

1. Среда обитания
 - A. Файловые вирусы
 - B. Загрузочные вирусы
 - C. Макровирусы
 - D. Сетевые
2. Особенности алгоритма работы
 - A. Резидентные
 - B. «Стелс»-алгоритмы
 - C. Самошифрование и полиморфичность
3. По деструктивным возможностям
 - A. Безвредные
 - B. Неопасные
 - C. Опасные
 - D. Очень опасные

Классификация вирусов

«Дропперы» – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют вируса в файле. Например, файл шифруется каким-либо специальным образом или упаковывается редко используемым архиватором, что не позволяет антивирусу "увидеть" заражение.

Intended-вирусы

К таким вирусам относятся программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножиться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер) и т. д.

Конечный список

1. Различные вирусы
2. Трояны
3. Черви
4. Логические бомбы
5. Intended-вирусы
6. Программы для спама
7. Конструкторы вирусов
8. Полиморфные генераторы
9. Программы шутки

Вопросы

?