Вредоносное Программное Обеспечение

Кирпиченков О.А
Гр.113

Вредоносная программа-это

- любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации.

Классификация вредоносных программ

- Вредоносное П.О. делится на:
- **По вредоносной нагрузке**
- **По методу размножения**

По вредоносной нагрузке

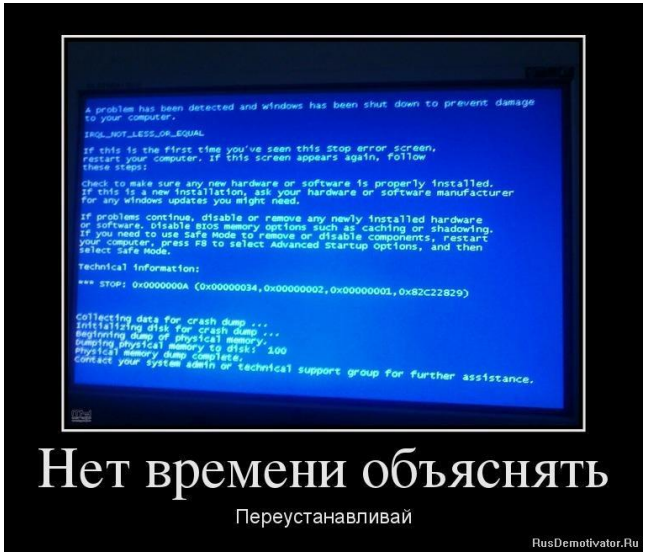
- Помехи в работе заражённого компьютера: начиная от открытия-закрытия поддона CD-ROM и заканчивая уничтожением данных и поломкой аппаратного обеспечения. Поломками известен, в частности, Win32.CIH.
- Инсталляция другого вредоносного ПО.
- Кража, мошенничество вымогательство и шпионаж за пользователем . Для кражи может применяться сканирование жёсткого диска, регистрация нажатий клавиш и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы.
- Прочая незаконная деятельность:
- Менее опасные *в зависимости от конкретной ситуации* ПО или данные:
- Иногда вредоносное ПО для собственного распространения или вредоносной деятельности устанавливает дополнительные утилиты: IRC-клиенты, программные маршрутизаторы, открытые библиотеки перехвата клавиатуры, программы удалённого администрирования… Такое ПО вредоносным не является, но из-за того, что за ним часто стоит истинно вредоносная программа, о нём могут предупреждать антивирусы. Бывает даже, что вредоносным является только скрипт из одной строчки, а остальные программы вполне легитимны.
- Данные от ПО могут передаваться как через компьютерную сеть, так и через «воздушный зазор»: при использовании накопителей, наличии микрофонов и (или) динамиков, и даже без каких-либо нестандартных устройств.

По методу размножения

- Эксплойт — теоретически безобидный набор данных (например, графический файл или сетевой пакет), некорректно воспринимаемый программой, работающей с такими данными. Здесь вред наносит не сам файл, а неадекватное поведение ПО с ошибкой, приводящее к уязвимости. Также эксплойтом называют программу для генерации подобных «отравленных» данных.
- Логическая бомба — вредоносная часть компьютерной программы (полезной или нет), срабатывающая при определённом условии.
- Троянская программа не имеет собственного механизма размножения и устанавливается «в придачу» к полезной. Часто «в придачу» ставят ПО, которое не является истинно вредоносным, но нежелательное.
- Компьютерный вирус размножается в пределах компьютера и через сменные диски. Размножение через сеть возможно, если пользователь сам выложит заражённый файл в сеть. Вирусы, в свою очередь, делятся по типу заражаемых файлов (файловые, загрузочные, макро-, автозапускающиеся); по способу прикрепления к файлам (паразитирующие, «спутники» и перезаписывающие) и т. д.
- Сетевой червь способен самостоятельно размножаться по сети. Делятся на IRC-, почтовые, размножающиеся с помощью эксплойтов и т. д.

Признаки заражения ПК

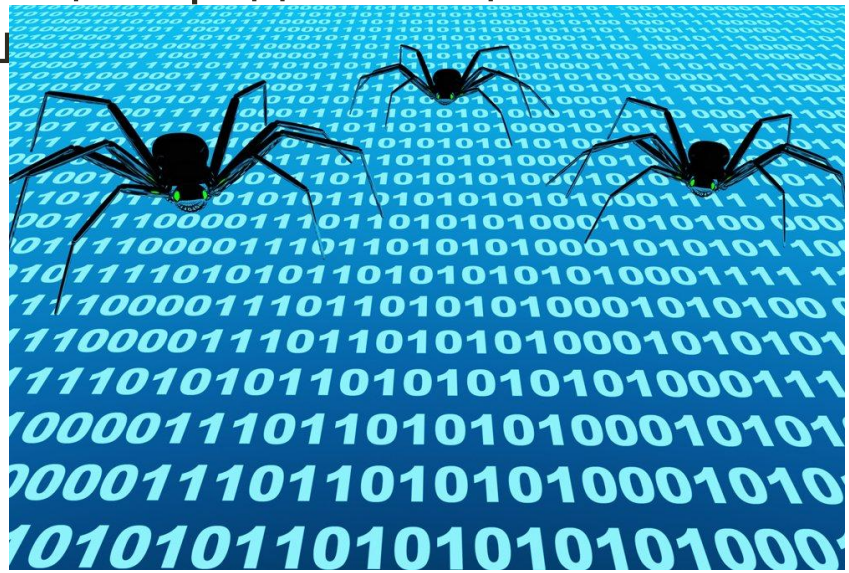
- автоматическое открытие окон с незнакомым содержимым при запуске компьютера;
- появление новых неизвестных процессов в выводе диспетчера задач (например, окне «Процессы» диспетчера задач Windows);
- появление в ветках реестра, отвечающих за автозапуск, новых записей;
- запрет на изменение настроек компьютера в учётной записи администратора;



Способы защиты от вредоносных программ

- 1.Установить антивирус
- 2.Не переходить по подозрительным ссылкам
- 3.Не устанавливать файлы из сомнительных источников

- Распространение вредоносного ПО является незаконным Согласно статье 273 Уголовного Кодекса Российской Федерации («Создание, использование и распространение вредоносных компьютерных программ») определение вредоносных программ выглядит следующим образом: «… заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информац



Источники:

- https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0

Спасибо за внимание!