Вирусология

Вредоносная программа: скрытая угроза

Вредоносная программа (также: зловредная программа, вредонос, зловред; malware—

контаминация слов malicious и software)— любое программное обеспечение, предназначенное дляполучения 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

Многофункциональные вредоносные программы

Существует вредоносная программа, которая занимается сбором адресов электронной почты на зараженном компьютере без ведома пользователя.

При этом она распространяется как в виде вложений электронной почты, так и в виде файлов через сети **P2P.**

Тогда программу можно классифицировать и как **Email-Worm,** и как **P2P-Worm** или **Trojan-Mailfinder**

Какие бывают?

- Вирус (Virus)
- Червь (Worm, Net-Worm)
- Троян (Trojan)
- Руткит (Rootkit)
- Логическая бомба (Logic Bomb)
- Клавиатурный шпион (Key logger)
- Рекламные закладки (Adware)
- Вымогатели (Ransomware)
- Шпионские программы (Spyware)
- Бэкдор (RAT- remote administration tool)
- Загрузчики (Drive-By-Download)

и множество других...

Вредоносная программа: Вирус

Вирус – самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя.

• Внедрение вируса происходит путём вставки своей копии в части существующих документов.

• Вирусы можно «подцепить» разными способами: от нажатия вредоносной ссылки или файла в неизвестном письме до заражения на вредоносном сайте.

• Вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда операционной системе.

• В настоящее время вирусы встречаются довольно редко в основном по двум причинам:

➢ широкое распространение вирусного кода приводит к скорому попаданию в руки антивирусных компаний;

➢ по большей части вытеснены другими видами вредоносных программ, такими как черви и трояны.

Вредоносная программа: Черви

Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ, однако не могут заражать уже существующие файлы.

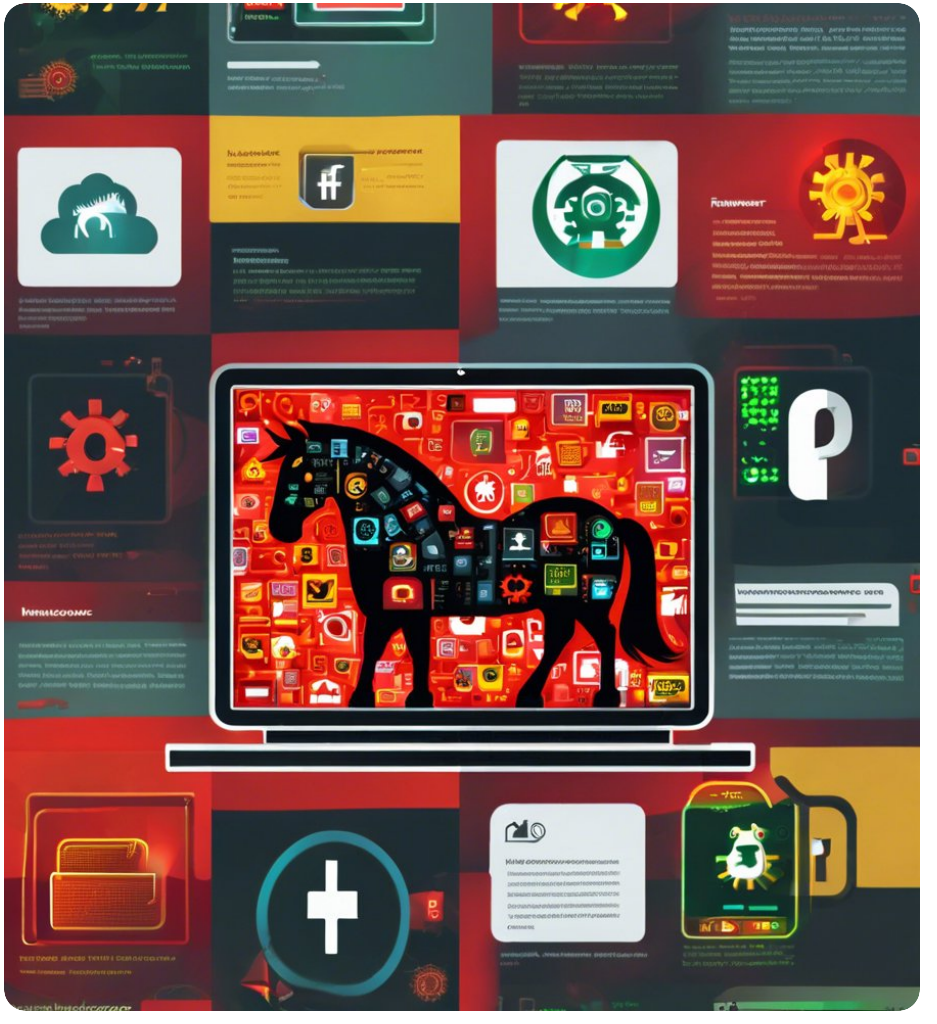
- Червь поселяется в компьютер отдельным файлом и ищет уязвимости в системе для дальнейшего распространения себя
- Для распространения черви используют сеть (локальную или Интернет), поэтому могут заражать компьютеры разыми способами
- Единицей заражения является компьютер целиком, а не отдельный файл на нём
- Червь представляет собой своего рода транспорт для других вредоносных программ. Например, после успешного заражения червь может «принести» на компьютер троян и активировать его.

Примеры червей:

1. Mydoom
2. Bagle
3. Warezov - почтовый червь

Вредоносная программа: Трояны

По своему действию троян является противоположностью вирусам и червям:
его предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности (а часто вместе с ней!) он делает то, что нужно злоумышленникам.



- Трояны не самовоспроизводятся и не распространяются сами по себе.
- Троян может не только выдавать себя за полезную программу, но и в реальности предоставлять

полезные функции, в качестве прикрытия для деструктивных действий.

- Также троян может скрывать от системы выполнение каких-либо вредоносных действий.

Вредоносная программа: Трояны

Как трояны попадают на ПК?

Трояна активирует пользователь.

Подхватить троянскую программу можно несколькими способами:

- фишинговая атака
- фальши сообщение не экране
- малварь

Дропперы и загрузчики - это вспомогательные программы, через которые вредоносное ПО, в том числе трояны, попадает на устройство.

Вредоносная программа: Бэкдор, Эксплойт и другие

Бэкдор - пытающийся взять на себя администрирование компьютера

Эксплойты – это программы, содержащие данные или код, которые позволяют использовать уязвимость в приложении на компьютере

Trojan-Banker предназначены для кражи учетных данных систем интернет-банкинга

Clampi - направлен на получение банковских данных

Cryxos - выдает фальшивые сообщения об угрозах или перенаправляет пользователей в фейковую службу техподдержки

Трояны, выполняющие DDoS-атаки

Троян-загрузчик - способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ

Троян-дроппер - используются, чтобы установить троянские программы или вирусы или предотвратить обнаружение вредоносных программ

FakeAV - имитируют работу антивирусного программного обеспечения

GameThief - крадут информацию об учетных записях участников сетевых игр

Вредоносная программа: Руткит

Руткит – особый вид вредоносных программ, разработанных специально для маскирования присутствия вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения.

- С целью «спрятаться» руткиты тесно интегрируются с операционной системой и пользуются её механизмами
- Некоторые руткиты, называемые буткитами, могут начать свою работу прежде, чем загрузится операционная система
- Руткиты достаточно трудно обнаружить и уничтожить

Вредоносная программа: Вымогатель

Вымогатель (вирус-вымогатель) создаётся с целью вымогательства: блокирует доступ к компьютерной системе или предотвращает считывание записанных в нём данных (чаще всего с помощью шифрования), а затем требует от жертвы выкуп для восстановления исходного состояния

• Основными способами воздействия на жертву являются:

➢ блокировка или помеха работе в системе, в частности

➢ блокировка или помеха работе в браузерах

➢ шифрование файлов в системе.

• Технически, не редко такие программы используют только разрешенные и безопасные функции системы, из-за чего средства безопасности просто не обращают на них внимания.

• В случае применения средств шифрования, данные могут быть потеряны безвозвратно...

Вредоносная программа:
Логическая бомба и Клавиатурный шпион

• **Логическая бомба** – специфический вид вредоносных программ, который проявляет себя только при определенных действиях или событиях, а остальную часть времени бездействует. Как и сетевые черви, логические бомбы могут содержать другие вредоносные программы.

• **Клавиатурный шпион** (Key logger) – особый вид трояна, который записывает все нажатия кнопок клавиатуры и/или действия мышки на вашем компьютере. Чаще всего клавиатурный шпион применяется для кражи паролей и личной информации.

Вредоносная программа: Adware - Рекламное ПО

Adware - рекламное программное обеспечение, рекламная программа – тип лицензионного ПО.

Само программное обеспечение распространяется бесплатно, однако автор или распространитель приложения получает доход за счет показа рекламы. В таких бесплатнораспространяемых программах могут быть спрятаны другие программы...

Вредоносная программа: Еще вредители

• **Макросы цифровых документов**

множество форматов документов содержит механизмы динамического формирования и

модифицирования содержания, которые по сути представляют собой исполняемый код

• **Фишинг и веб**

веб-страницы также содержат механизмы динамического формирования «конткнта»

помимо этого, загружаемые из сети файлы - один из самых простых способов проникновения в локальную систему

• **Исполняемые файлы (*.exe, ELF, etc.)**

вы уверены, что запущенный вами исполняемый файл действительно делает то, что вы от него ожидаете?..

Чем опасны трояны? Трояны прекрасно прячутся.

Замедление работы компьютера, частые сбои, неожиданные изменения в настройках, появление нежелательной рекламы и подозрительных всплывающих окон - все это может быть признаками заражения вашего устройства вредоносной программой. Будьте бдительны и регулярно проверяйте устройство на наличие угроз.

Вредоносная программа: скрытая угроза

Основные ошибки:

- Переход по сомнительным ссылкам
- Использование неизвестных флэш-накопителей
- Скачивание фальшивого антивирусного ПО
- Атаки через веб-камеру
- Использование одного пароля для разных сайтов при отсутствии двухфакторной аутентификации
- Использование слабых паролей
- Несвоевременное обновление программного обеспечения
- Ответы на фишинговые письма
- Отключение функций управления учетными записями пользователей
- Использование публичных Wi-Fi сетей

Бонус :)

Короткие ссылки