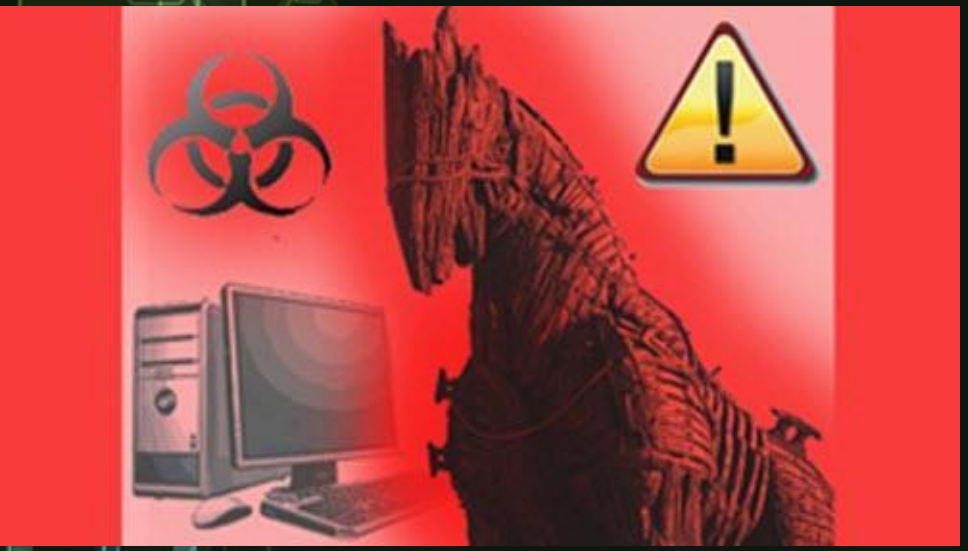
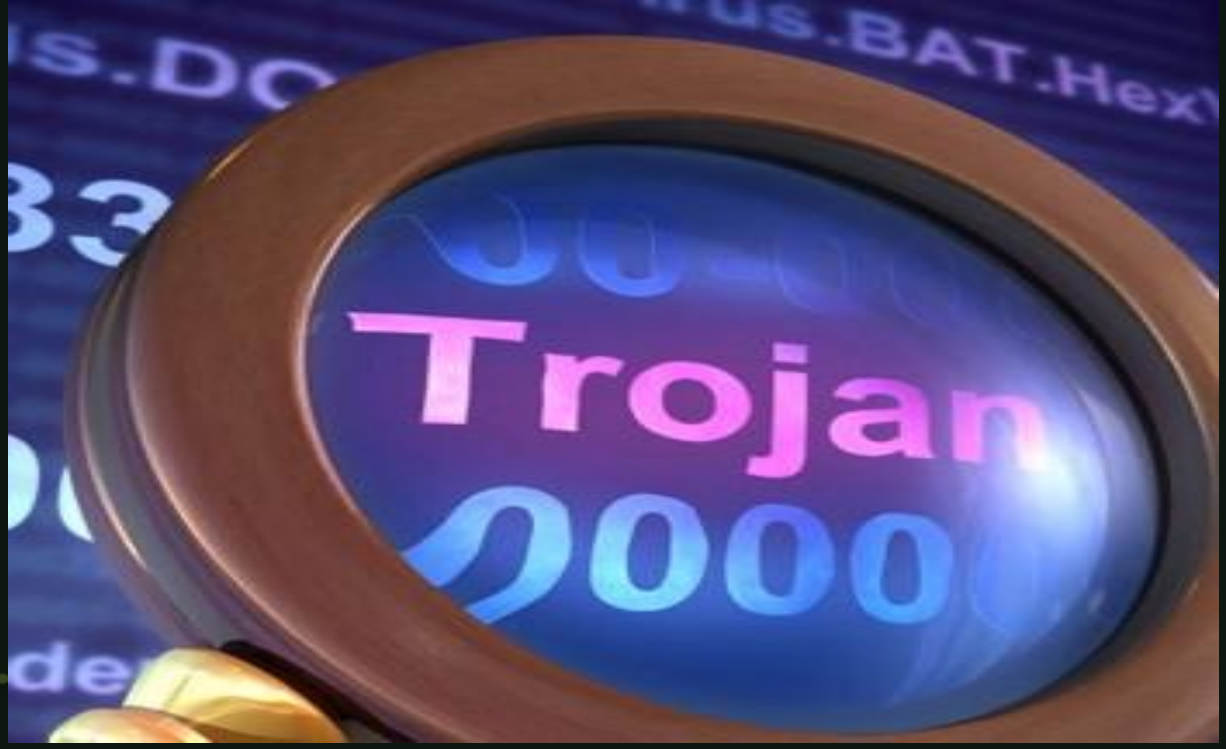
Троянская программа

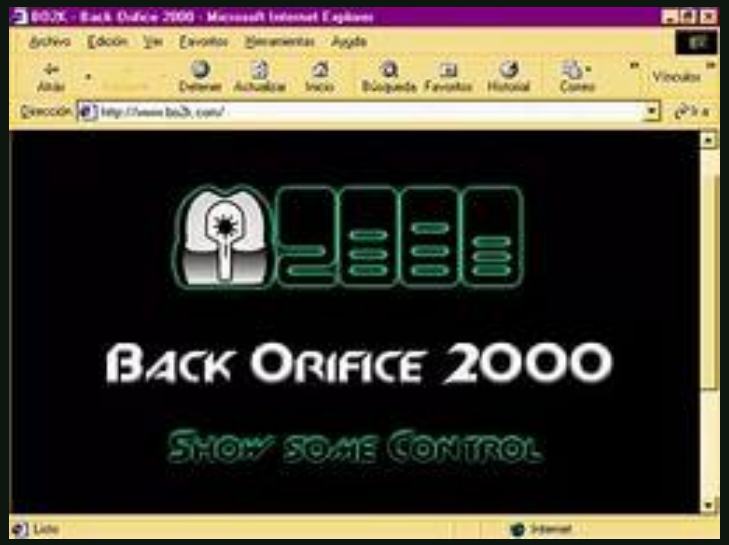


Выполнили:
Лясина Анастасия,
Палажова Анастасия,
Борщ Анастасия,
Батуева Екатерина,
Соловьева Александра

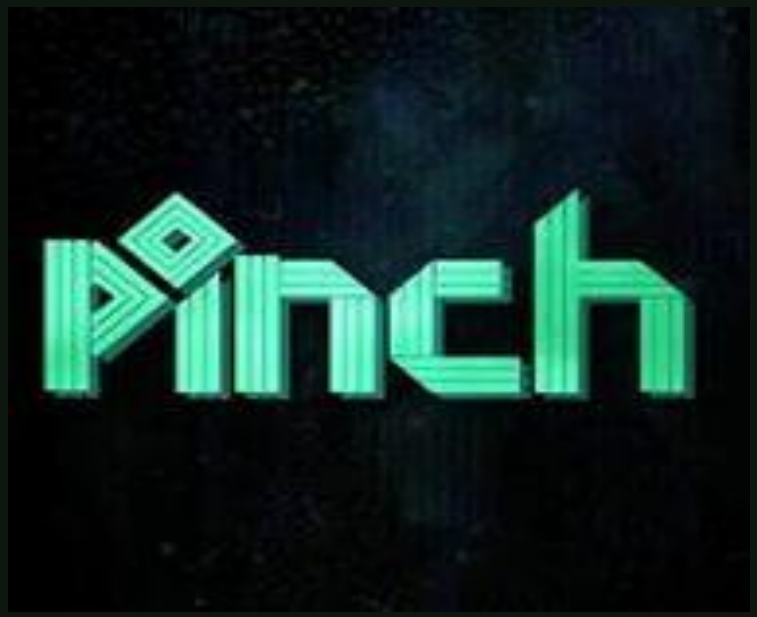


«Трояны» — самый простой вид вредоносных программ, сложность которых зависит исключительно от сложности истинной задачи и средств маскировки.

Back Orifice, Backdoor.BO — троянская программа удаленного администрирования, созданная известной группой хакеров «Культ дохлой коровы» (англ.) в 1998 году.

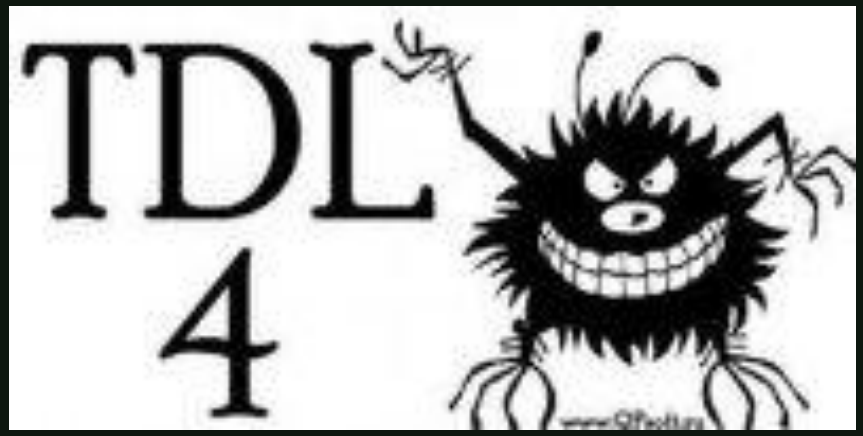


Pinch — одна из наиболее активно используемых троянских программ в Рунете. Автором программы является программист Александр Демченко в 2003 году.



Структура и принцип работы программы: Pinch состоит из двух частей: клиента и сервера. Серверная часть написана на языке ассемблера (MASM) и после компиляции и упаковки обладает небольшим размером — около 20 кб.

- TDL — троянская программа предназначена для удаленного контроля над компьютером с операционной системой Windows.

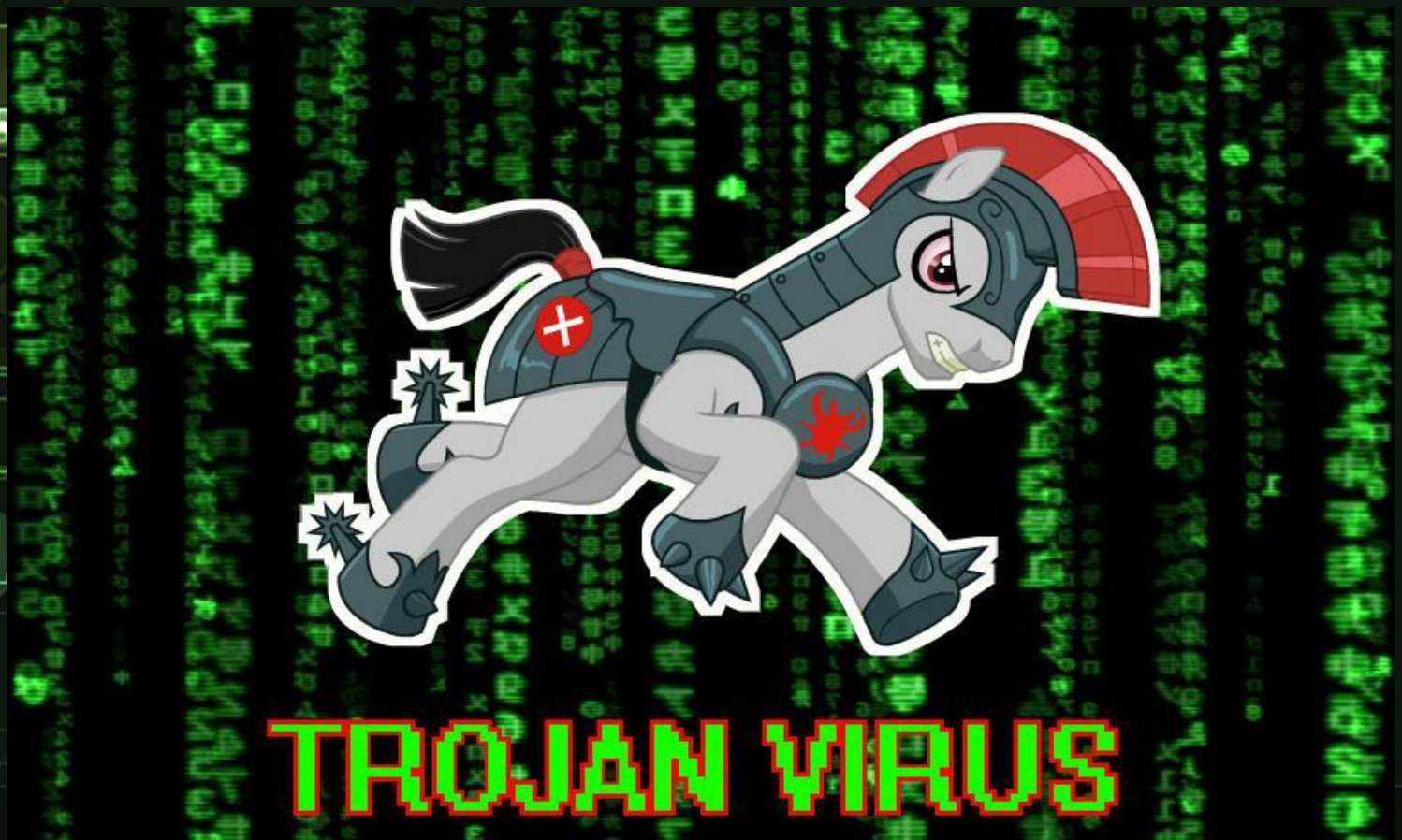


Trojan.Winlock (Винлокер) — семейство вредоносных программ, блокирующих или затрудняющих работу с операционной системой, и требующих перечисление денег злоумышленникам за восстановление работоспособности компьютера, частный случай Ransomware (программ-вымогателей).

Принцип действия:

Троянские программы обычно состоят из двух частей:

- клиент
- сервер



Распространение

Троянские программы распространяются людьми — как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и/или запускать их на своих системах.

классификация

1. удалённый доступ
2. уничтожение данных
3. загрузчик
4. сервер
5. дезактиватор программ безопасности

Маскировка

- Троянская программа может имитировать имя и иконку существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных (например картинки), как для запуска пользователем, так и для маскировки в системе своего присутствия.

Большинство троянских программ не афиширует своего присутствия на компьютере пользователя

Симптомы заражения троянской программой:

- появление в реестре автозапуска новых приложений;
- показ фальшивой закачки видеопрограмм, игр, которые вы не закачивали и не посещали;
- создание снимков экрана;
- открывание и закрывание консоли CD-ROM;
- проигрывание звуков и/или изображений, демонстрация фотоснимков;
- перезапуск компьютера во время старта инфицированной программы;
- случайное и/или беспорядочное отключение компьютера.

Спасибо за внимание!!!