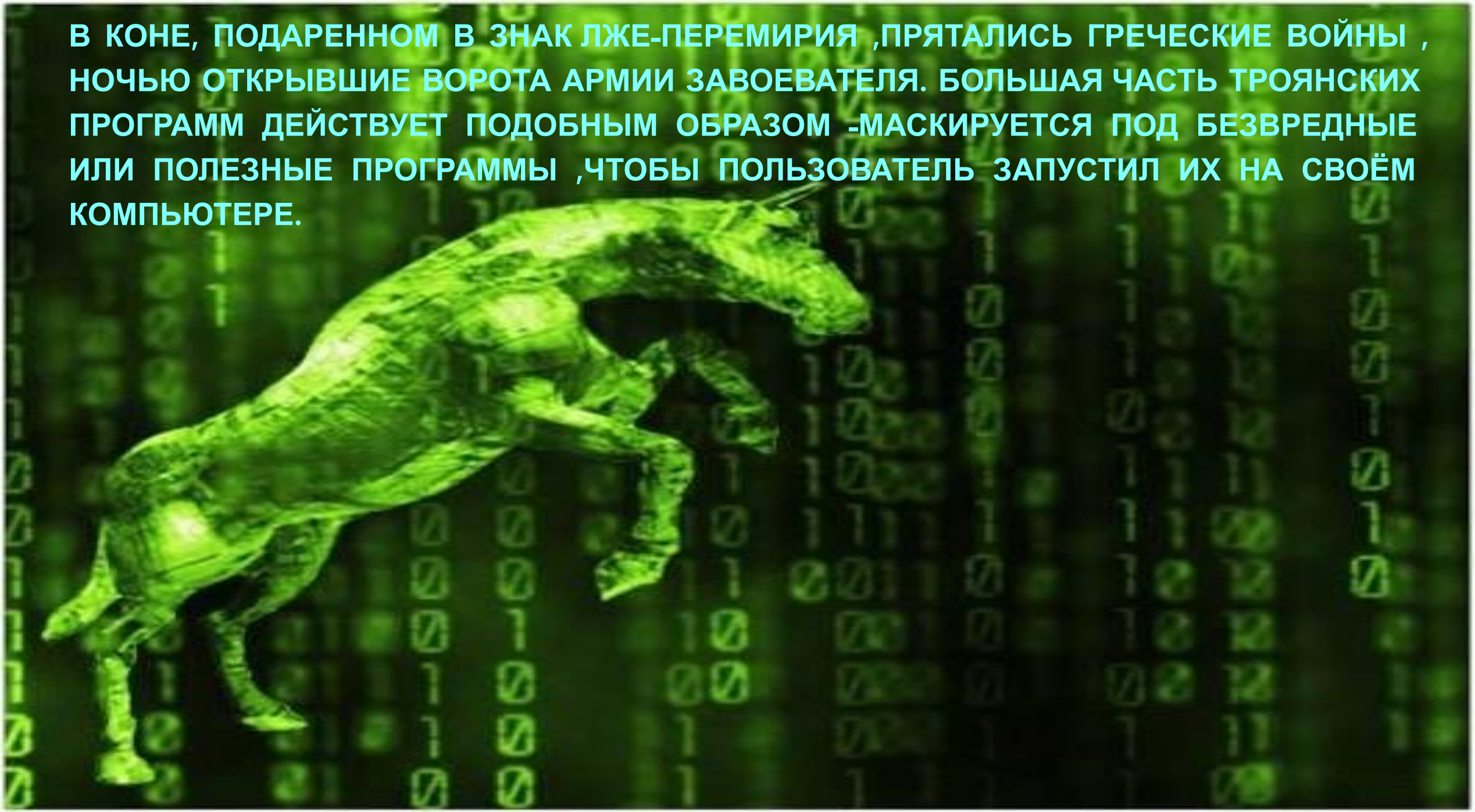
ТРОЯНЫ (TROJANS)

ЧТО ТАКОЕ ТРОЯНСКАЯ ПРОГРАММА?

- **Троя́н, троя́нец, троя́нский конь**— разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, её разрушение или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.


В КОНЕ, ПОДАРЕННОМ В ЗНАК ЛЖЕ-ПЕРЕМИРИЯ ,ПРЯТАЛИСЬ ГРЕЧЕСКИЕ ВОЙНЫ , НОЧЬЮ ОТКРЫВШИЕ ВОРОТА АРМИИ ЗАВОЕВАТЕЛЯ. БОЛЬШАЯ ЧАСТЬ ТРОЯНСКИХ ПРОГРАММ ДЕЙСТВУЕТ ПОДОБНЫМ ОБРАЗОМ -МАСКИРУЕТСЯ ПОД БЕЗВРЕДНЫЕ ИЛИ ПОЛЕЗНЫЕ ПРОГРАММЫ ,ЧТОБЫ ПОЛЬЗОВАТЕЛЬ ЗАПУСТИЛ ИХ НА СВОЁМ КОМПЬЮТЕРЕ.

ТИПЫ ТРОЯНСКИХ ПРОГРАММ

- Троянские программы чаще всего разрабатываются для вредоносных целей. Существует классификация, где они разбиваются на категории, основанные на том, как трояны внедряются в систему и наносят ей вред. Существует 5 основных типов:

- удалённый доступ
- уничтожение данных
- загрузчик
- сервер
- дезактиватор программ безопасности

ЦЕЛИ

- Целью троянской программы может быть:

•закачивание и скачивание файлов;

•копирование ложных ссылок, ведущих на поддельные вебсайты, чаты или другие сайты с регистрацией;

•создание помех работе пользователя;

•кража данных, представляющих ценность или тайну, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам, выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях;

•распространение других вредоносных программ, таких как вирусы;

•уничтожение данных (стирание или переписывание данных на диске, труднозамечаемые повреждения файлов) и оборудования, выведения из строя или отказа обслуживания компьютерных систем, сетей;

•сбор адресов электронной почты и использование их для рассылки спама;

•слежка за пользователем и тайное сообщение третьим лицам сведений, таких как, например, привычка посещать конкретные сайты;

•регистрация нажатий клавиш с целью кражи информации такого рода как пароли и номера кредитных

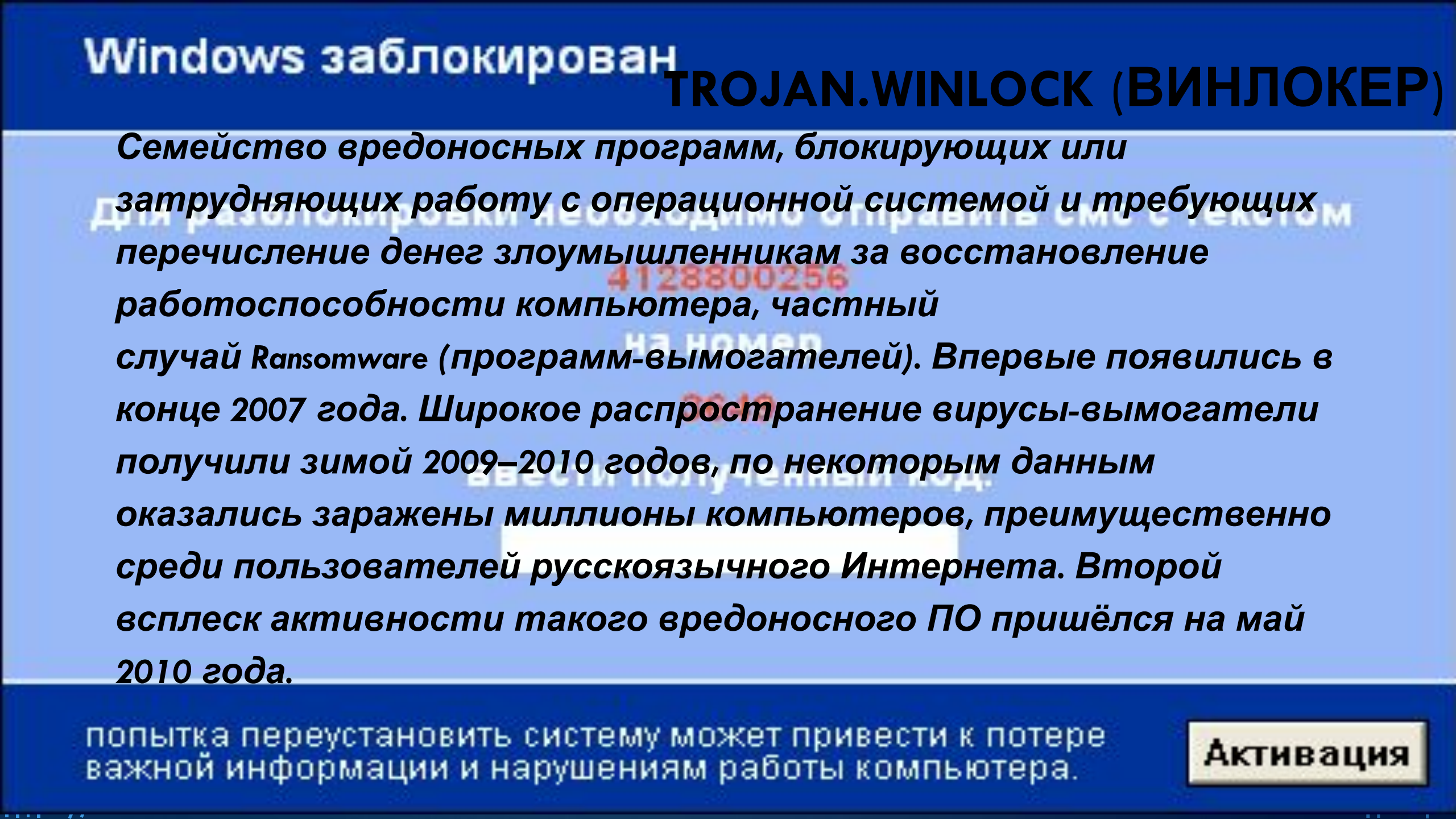
РАБОТА

- Задачи, которые могут выполнять троянские программы, бесчисленны (как бесчисленны и существующие ныне в мире компьютерные вредоносные программы), но в основном они идут по следующим направлениям:

- нарушение работы других программ (вплоть до зависания компьютера, решаемого лишь перезагрузкой, и невозможности их запуска);
- настойчивое, независимое от владельца предлагание в качестве стартовой страницы спам-ссылок, рекламы или порносайтов;
- распространение по компьютеру пользователя порнографии;
- превращение языка текстовых документов в бинарный код;
- мошенничество (например, при открывании определённого сайта пользователь может увидеть окно, в котором ему предлагают сделать определённое действие, иначе произойдёт что-то труднопоправимое — бессрочная блокировка пользователя со стороны сайта, потеря банковского счета и т. п., иногда за деньги, получение доступа к управлению компьютером

УДАЛЕНИЕ ТРОЯНОВ

- В целом, троянские программы обнаруживаются и удаляются антивирусным и антишпионским ПО точно так же, как и остальные вредоносные программы.
- Троянские программы хуже обнаруживаются контекстными методами антивирусов (основанных на поиске известных программ), потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с бóльшей задержкой, нежели самопроизвольно распространяемые вредоносные программы. Однако эвристические (поиск алгоритмов) и проактивные (слежение) методы для них столь же эффективны.



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). Впервые появились в конце 2007 года. Широкое распространение вирусы-вымогатели получили зимой 2009–2010 годов, по некоторым данным оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета. Второй всплеск активности такого вредоносного ПО пришёлся на май 2010 года.

TDL

Программа предназначена для удаленного контроля над компьютером с операционной системой Windows. Троян, используя службу печати для повышения привилегий и обхода проактивных средств детектирования, модифицирует master boot record(MBR). Создатели трояна придумали свою собственную систему кодировки для защиты способов связи между теми, кто управляет ботнетом и зараженными компьютерами.

На август 2011 года появилась четвертая версия трояна, TDL4 aka TDSS . На данный момент, из-за выставления исходников TDL4 на продажу, появилось еще два, не менее опасных руткита: SST и Zeroaccess aka Max++

Сам по себе, TDL только присоединяет пораженный компьютер к ботнету TDL. Но при этом предоставляет платформу для установки других вредоносных программ.

BACK ORIFICE, BACKDOOR.BO

троянская программа удаленного администрирования, созданная известной группой хакеров «Культ дохлой коровы (англ.) в 1998 году. Программа предназначена для удаленного контроля над компьютером с операционной системой Windows 95/Windows 98. Программа построена на основе клиент-серверной архитектуры. На компьютере жертвы устанавливается небольшой серверный компонент BOSERV, представляющий собой exe-файл. С помощью специальной утилиты BOCONFIG последний можно прикрепить к любому .exe файлу. Клиентская часть реализуется программой BOGUI. Обмен данных по сети между BOGUI и BOSERV осуществляется с использованием TCP/IP через порт 31337.