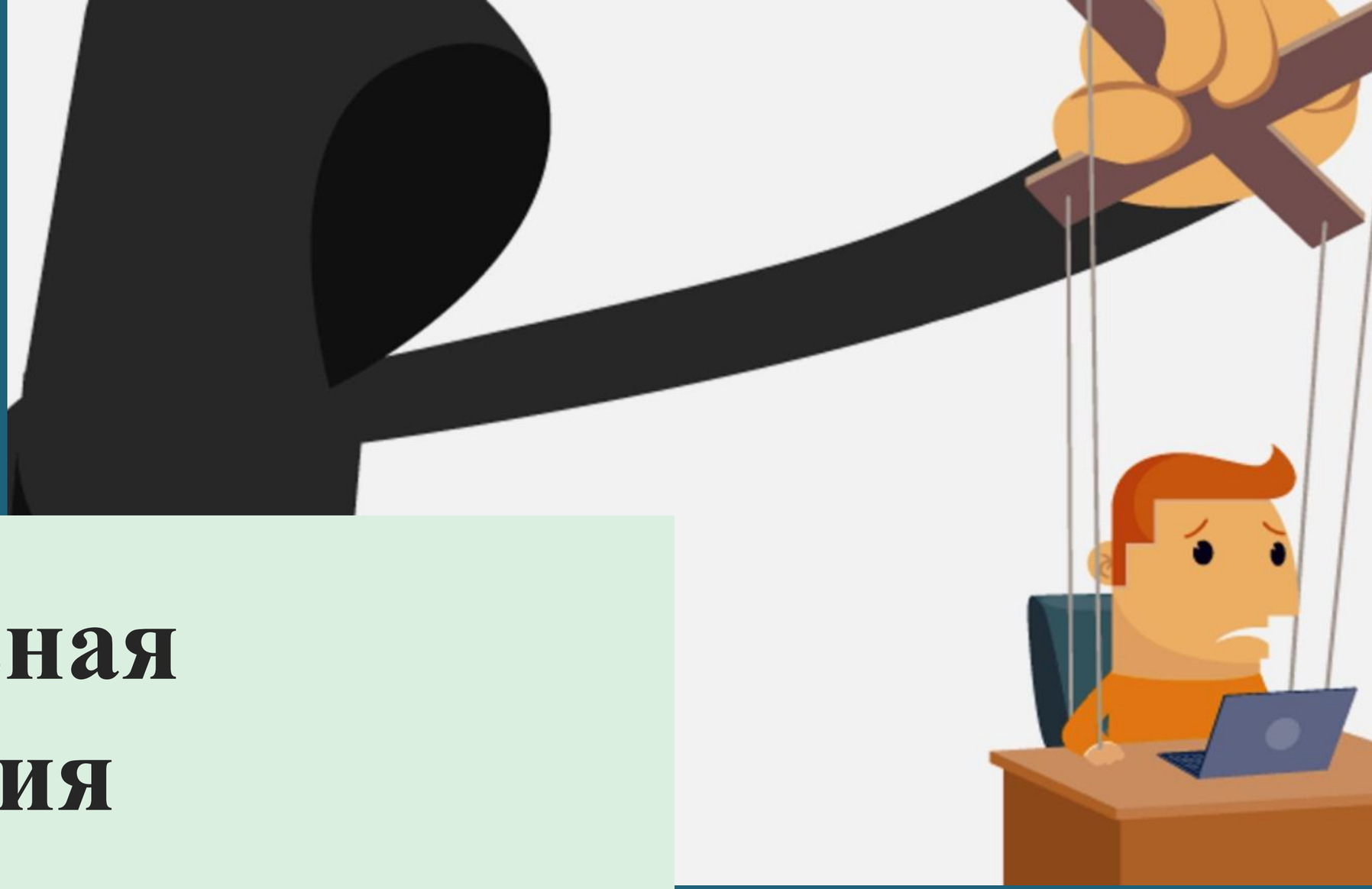
САМАЯ БОЛЬШАЯ ДЫРА В БЕЗОПАСНОСТИ СИДИТ НАПРОТИВ МОНИТОРА



Социальная инженерия

Спикер: Чиковский Антон

Сейчас наши девайсы хранят очень много информации. От безобидных заметок до персональных данных, секретных файлов и банковских карт.

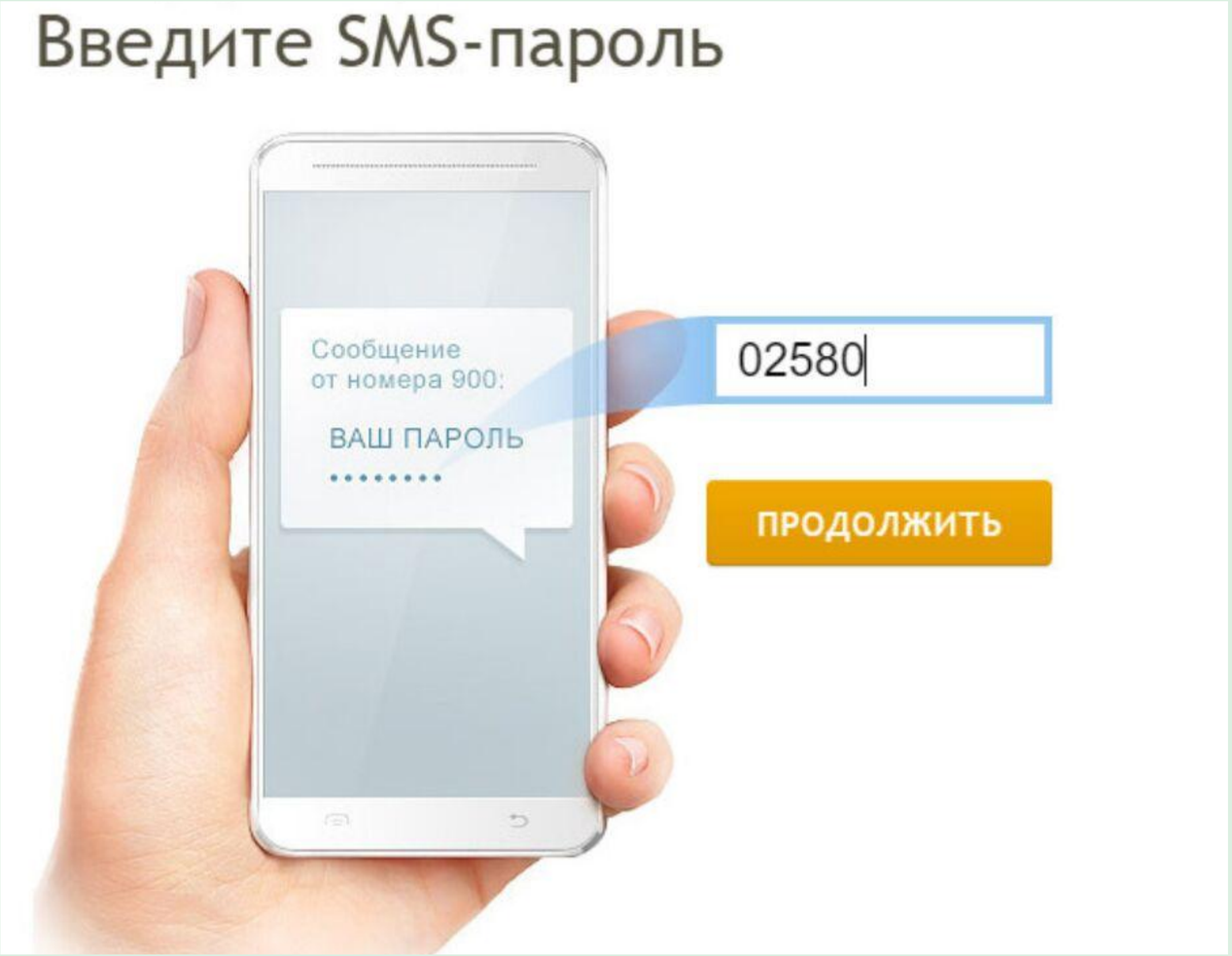
Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей

Претекстинг – по сути это техника актерской игры, где всё происходит по сценарию. В результате жертва самая даёт нужную злоумышленнику информацию сам того не подозревая.

pretext

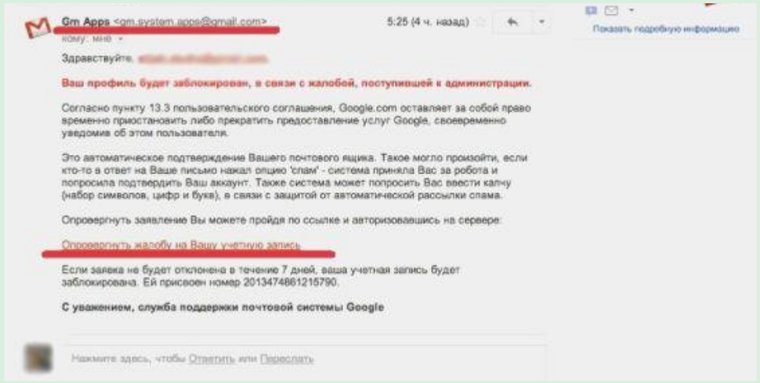
Допустим если злоумышленник играй роль сотрудника банка, он должен знать ФИО жертвы и примерно знать операции, которые он недавно совершал. И имея такой базовый набор, человек по ту сторону вполне может узнать пинкод карты, пароль из смс, реквизиты и многое другое, что даст ему полный доступ к карте жертвы.

Так как этот метод очень неэффективен, то и защита от этого техника тоже проста, просто не сообщать важные данные операторам так, как настоящий оператор никогда не попросит информацию, которую нельзя разглашать

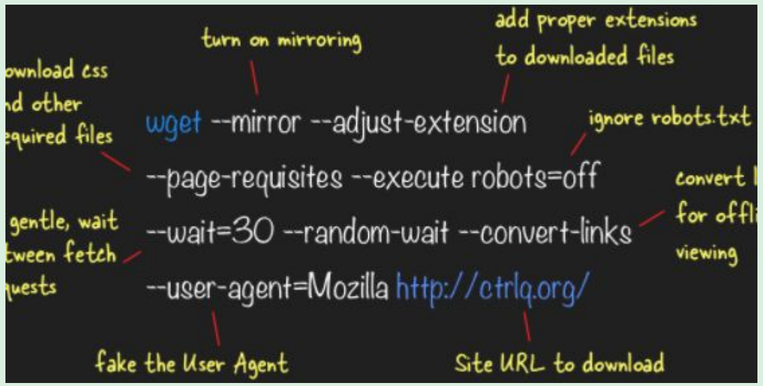


Фишинг – очень распространённая техника, она направлена на то, что злоумышленник, зная интересы и потребности жертвы, заставляет передать жертву её конфиденциальную информацию.

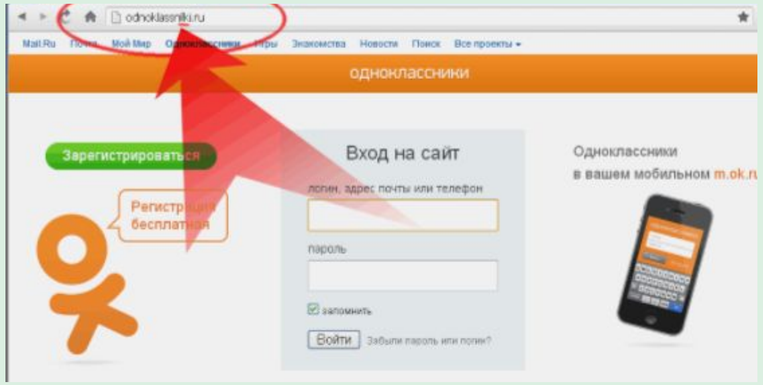
Самый распространенный способ, это поддельное письмо из банка или оператора по смс или почте, при котором перейдя по ссылке в письме жертва вводит в подменный сайт настоящие данные и после чего переходит на стоящий ресурс.



Письмо якобы от google с ссылкой на подменный сайт, с просьбой подтвердить данные аккаунта

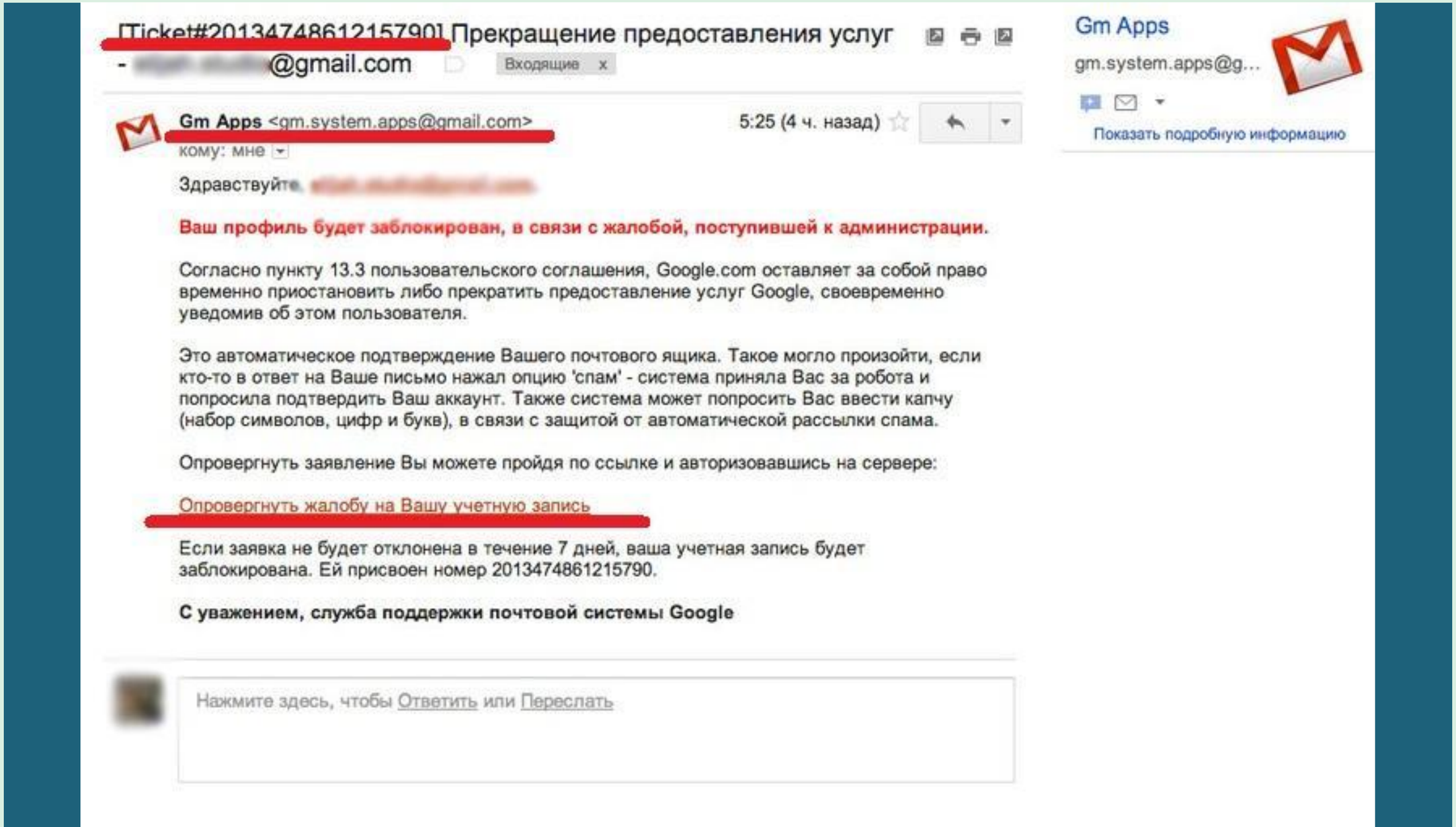


Строка программы wget скачивающая официальный сайт, затем этот сайт после манипуляций будет поддельным и данные будут отправляться не только на сервер сервиса но и злоумышленнику



Сам подменный сайт адрес которого отличается, лишь на одну букву

Подменное письмо



[Ticket#2013474861215790] Прекращение предоставления услуг - [redacted]@gmail.com Входящие x

Gm Apps <gm.system.apps@gmail.com> 5:25 (4 ч. назад)

кому: мне

Здравствуйте, [redacted]

Ваш профиль будет заблокирован, в связи с жалобой, поступившей к администрации.

Согласно пункту 13.3 пользовательского соглашения, Google.com оставляет за собой право временно приостановить либо прекратить предоставление услуг Google, своевременно уведомив об этом пользователя.

Это автоматическое подтверждение Вашего почтового ящика. Такое могло произойти, если кто-то в ответ на Ваше письмо нажал опцию 'спам' - система приняла Вас за робота и попросила подтвердить Ваш аккаунт. Также система может попросить Вас ввести капчу (набор символов, цифр и букв), в связи с защитой от автоматической рассылки спама.

Опровергнуть заявление Вы можете пройдя по ссылке и авторизовавшись на сервере:

Опровергнуть жалобу на Вашу учетную запись

Если заявка не будет отклонена в течение 7 дней, ваша учетная запись будет заблокирована. Ей присвоен номер 2013474861215790.

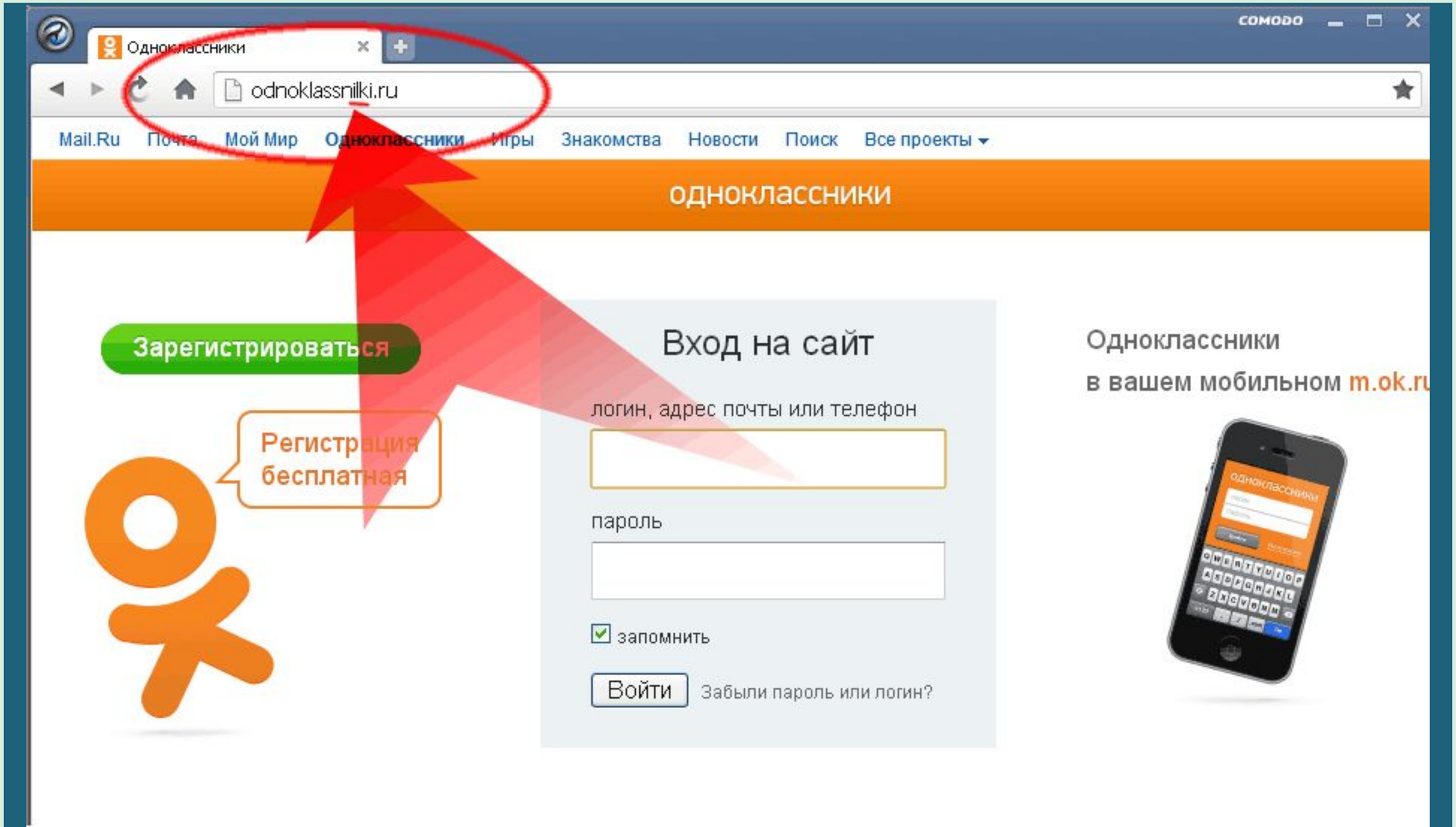
С уважением, служба поддержки почтовой системы Google

Нажмите здесь, чтобы Ответить или Переслать

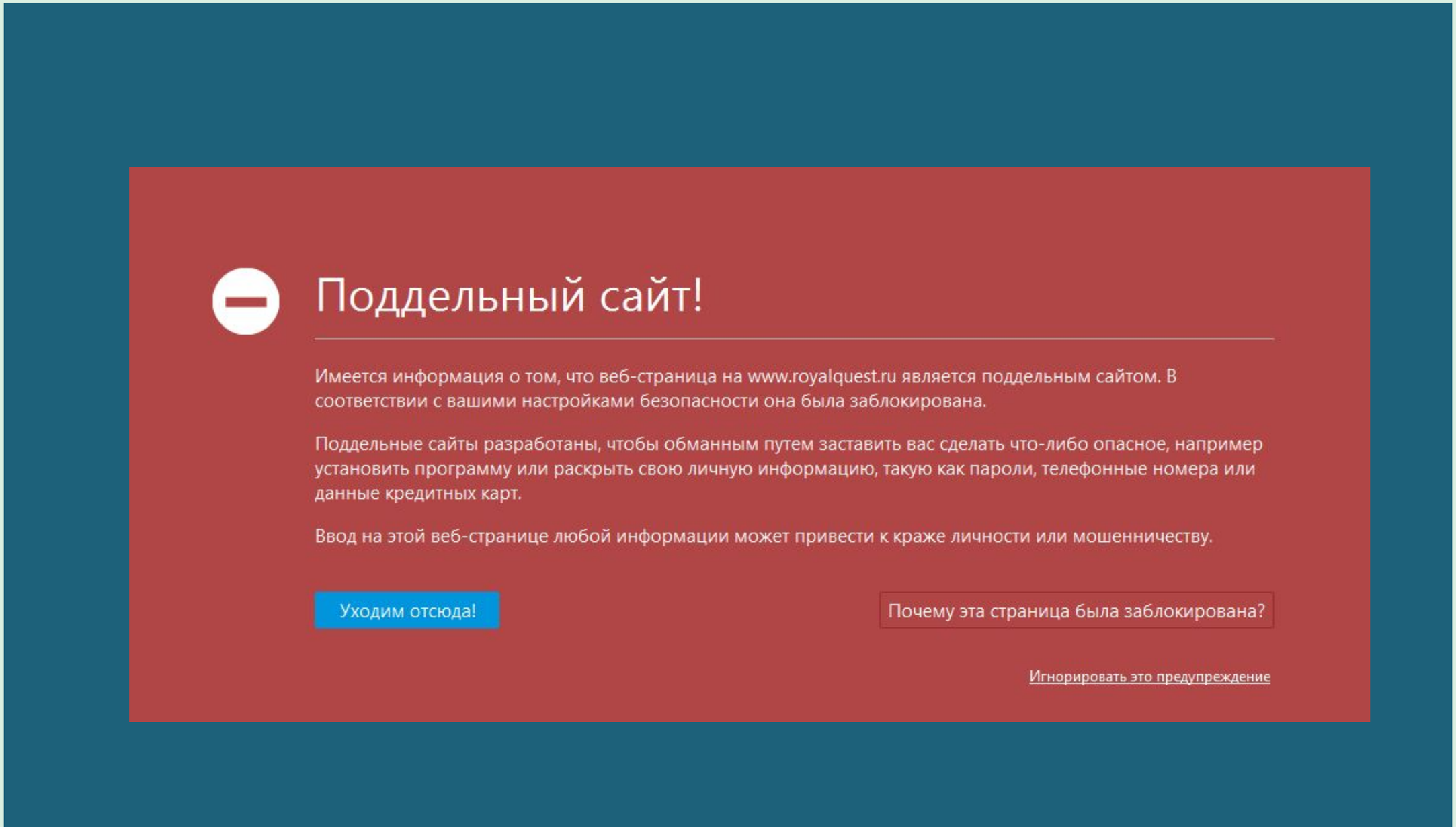
Gm Apps
gm.system.apps@g...

Показать подробную информацию

Подменный сайт

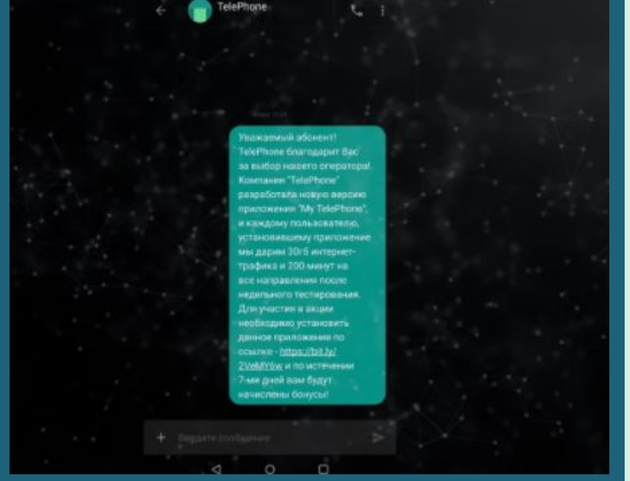


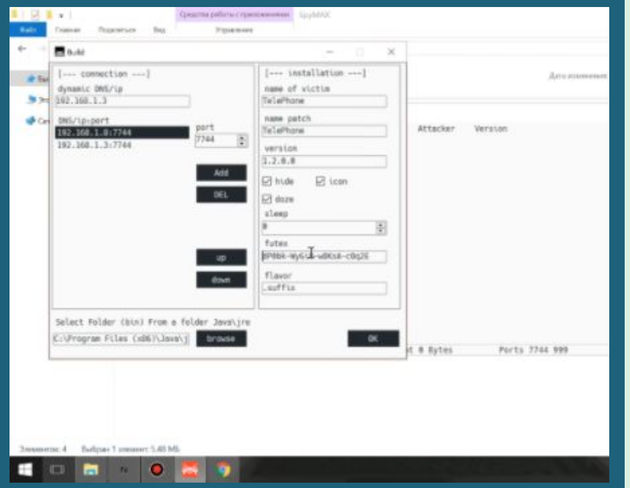
Защита браузера

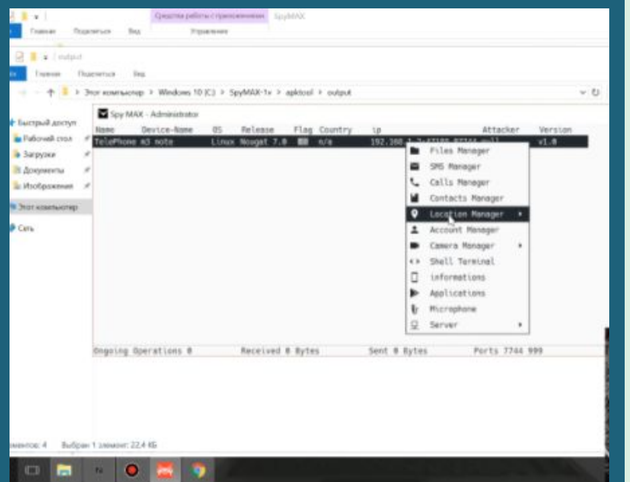


Троянский конь – Это техника использует такие нехорошие качества человека как алчность и любопытство в совокупности с невнимательностью. Чаще всего при такой технике под видом обновления или дополнения к программе злоумышленник добавляет эксплойт (вирус), который дают либо полный доступ к устройству жертвы

Эксплойты — это подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.





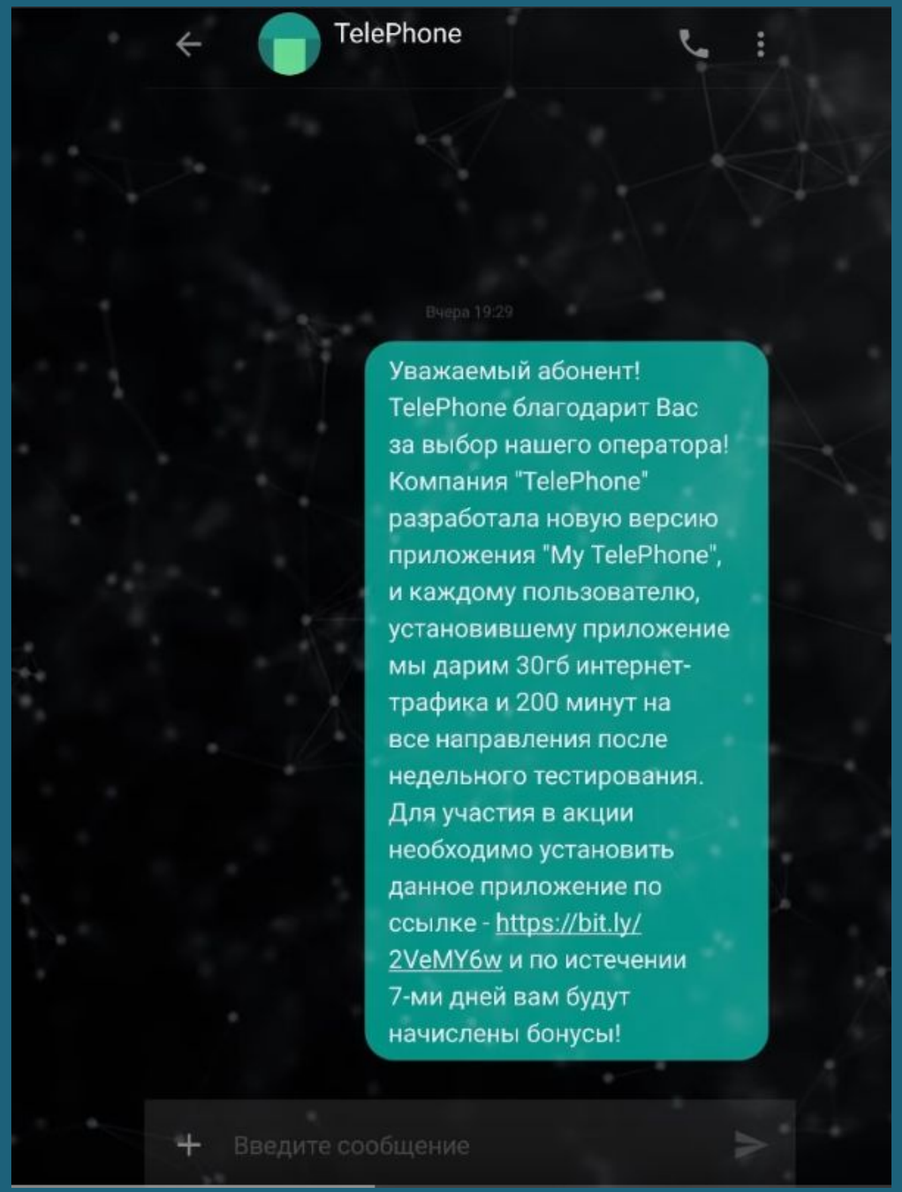


Сообщения с подменного номера о проходящей акции с ссылкой на вредоносное приложение.

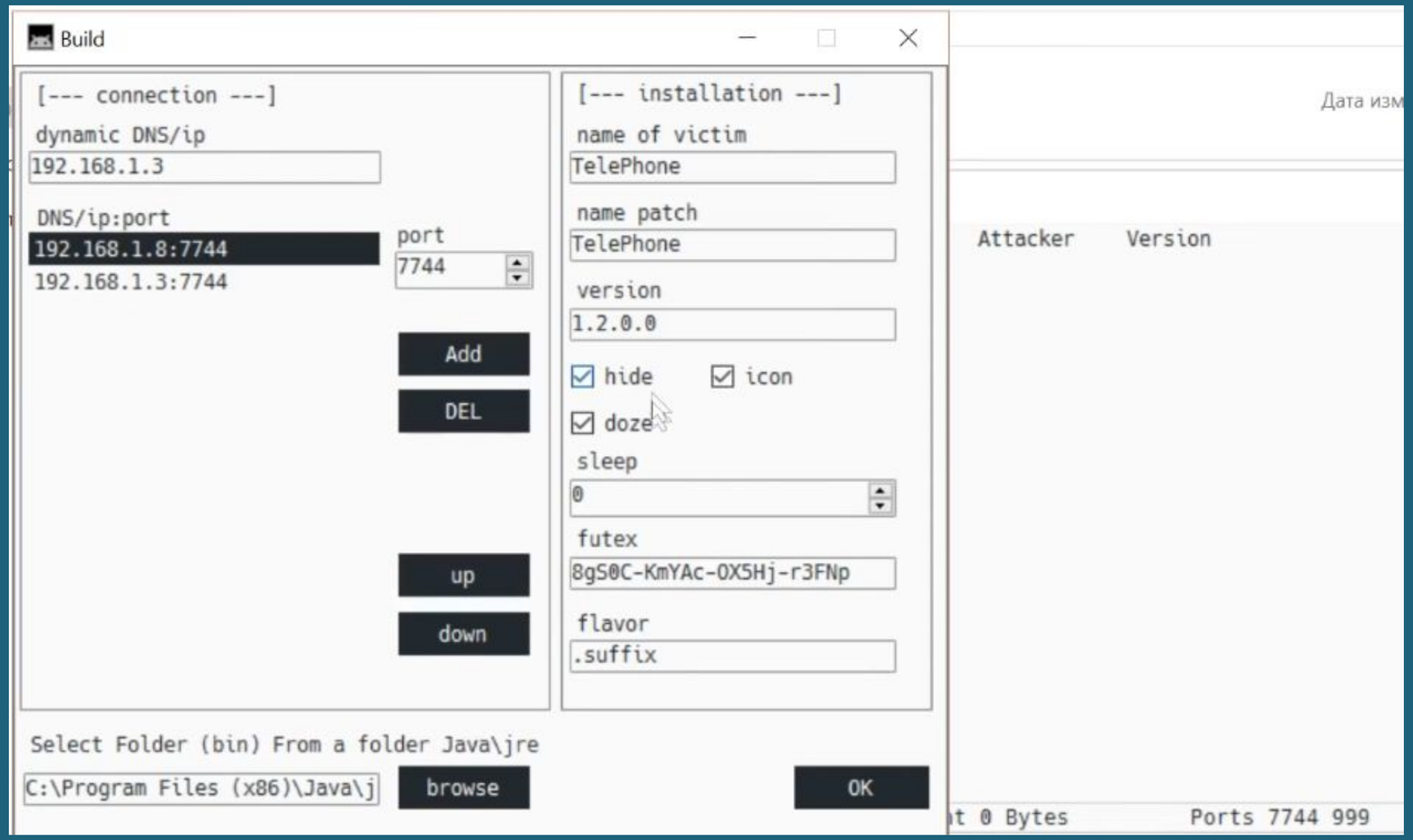
Само приложение Spymax, встраивающее вредоносный код в программу.

Что вообще может приложение при успешной атаке

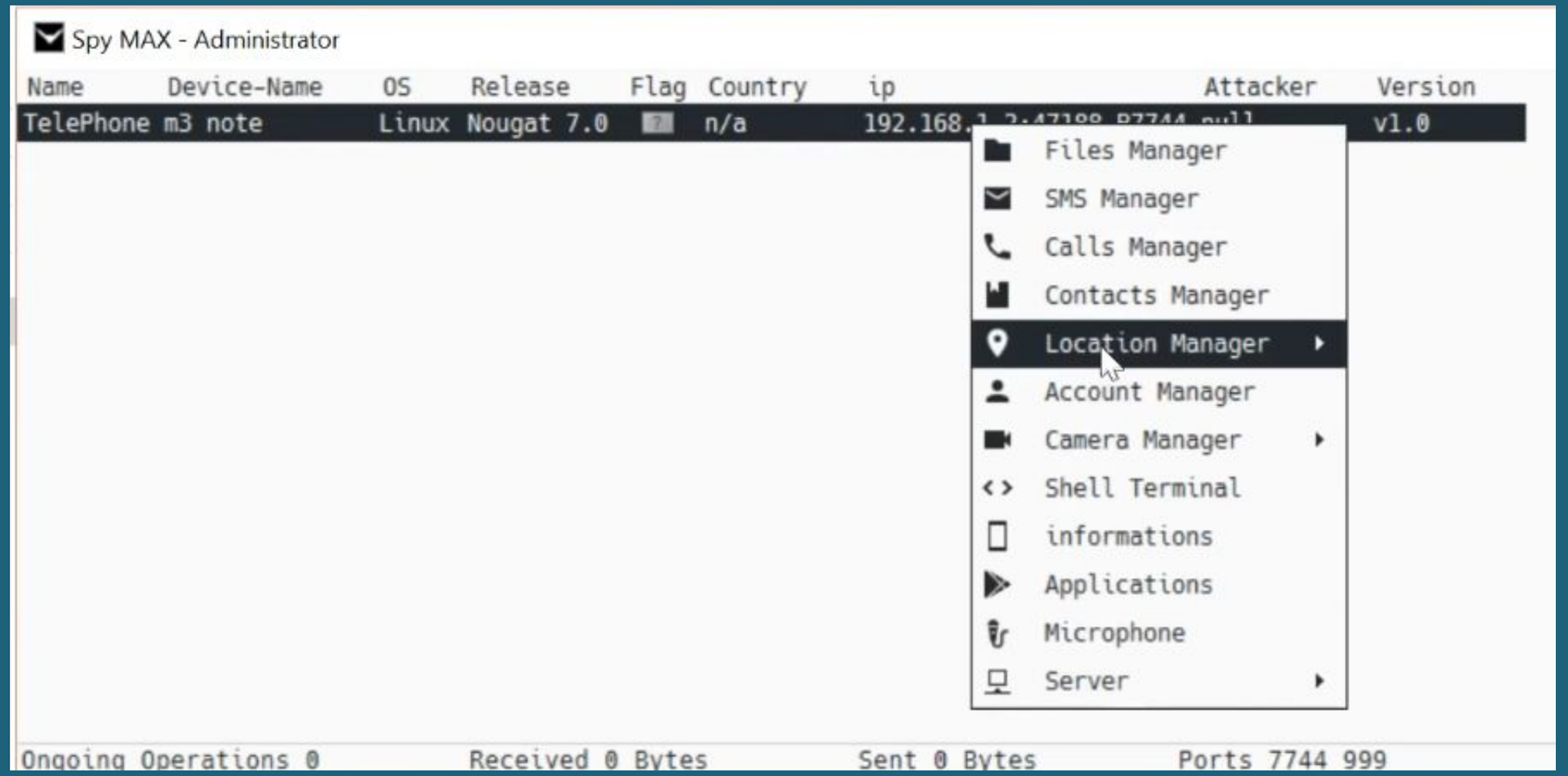
Смс с ссылкой

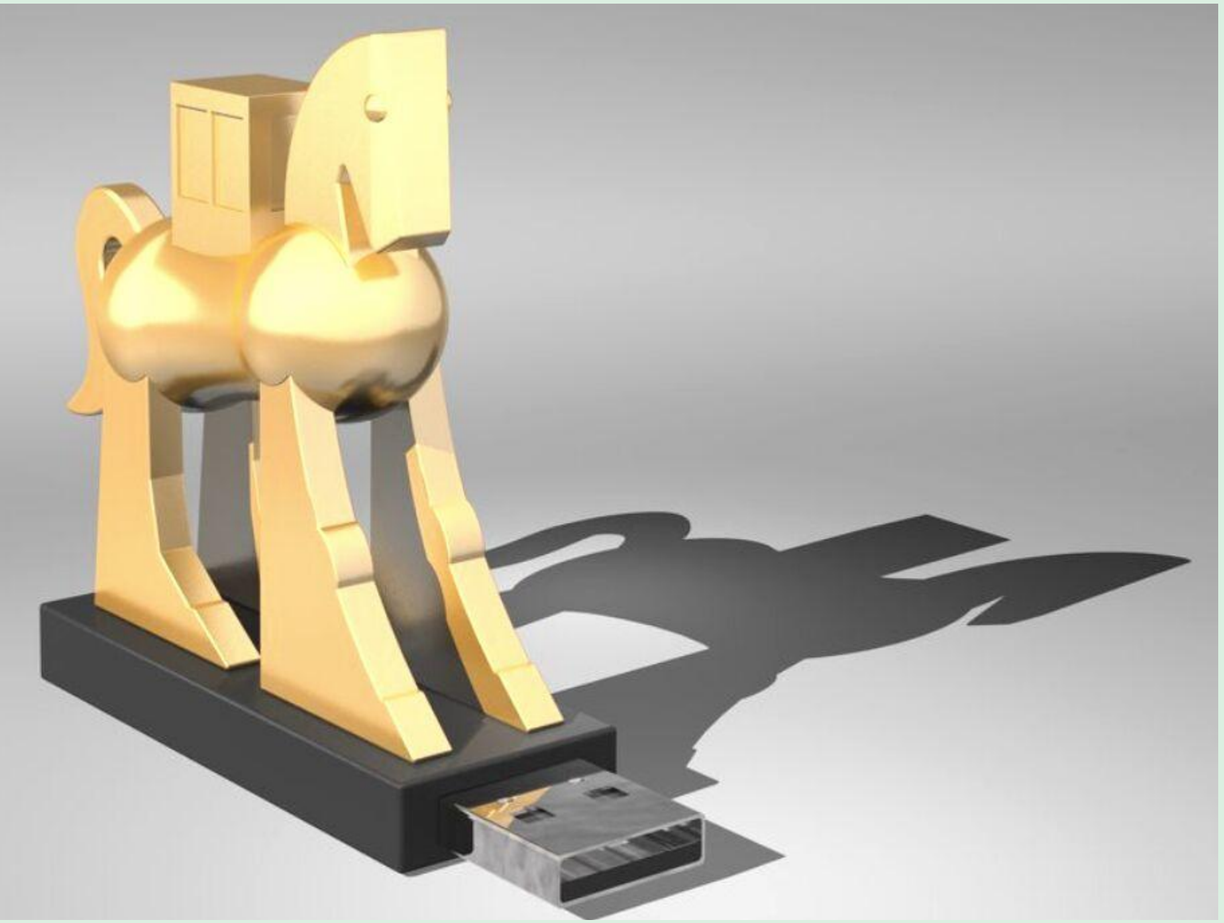


Смс с ссылкой



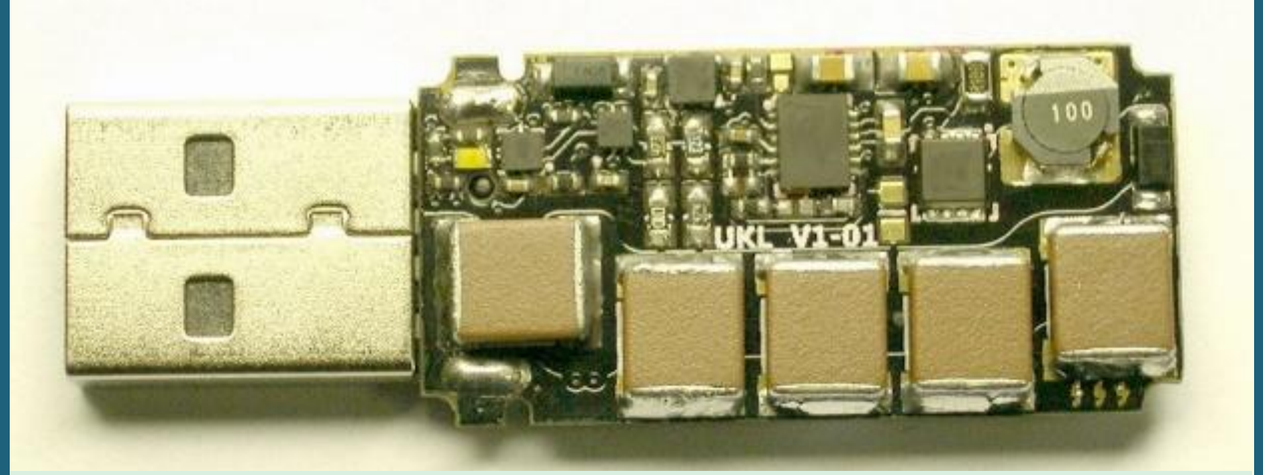
Смс с ссылкой



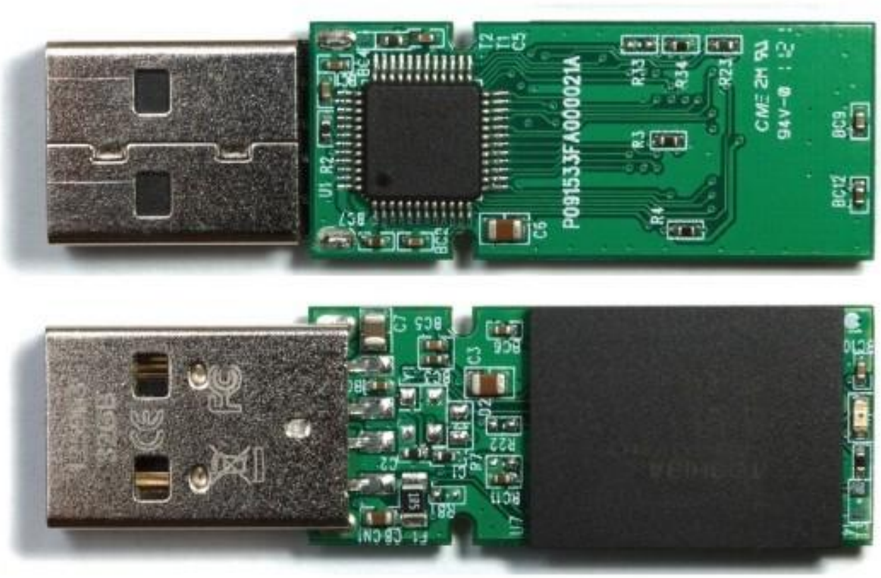


Дорожное яблоко – техника, до боли похожая на троянский конь. Только принцип передачи вируса здесь немного другой. Злоумышленник специально бросает флэшку с вирусом

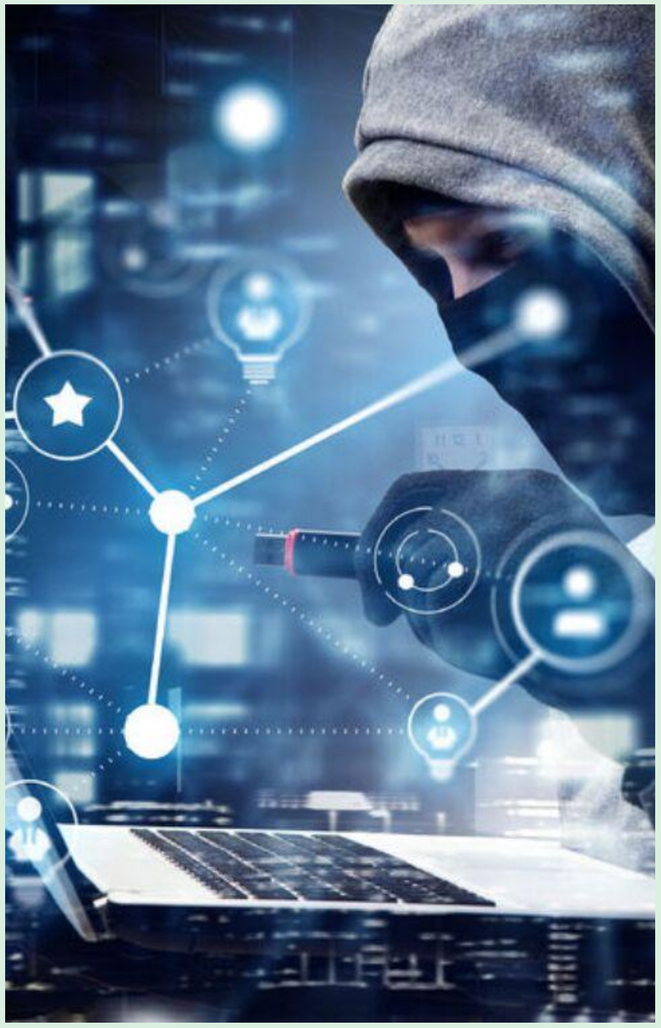
USB Killer – это на первый взгляд обычная флешка которая заставит вас плакать когда вы вставите ее в usb порт вашего персонального компьютера. После не громкого щелчка, который вы запомните на всю жизнь, вашему ПК понадобится в лучшем случае замена порта usb, а в худшем целых комплектующих.



BadUSB – метод атаки, включающий перепрошивку USB-устройства так, чтобы оно воспринималось компьютером как иное устройство. Например, USB-флешку компьютер будет видеть как клавиатуру или внешнюю сетевую карту, тем самым BadUSB сможет исполнять на компьютере заложенный в нее вредоносный код.



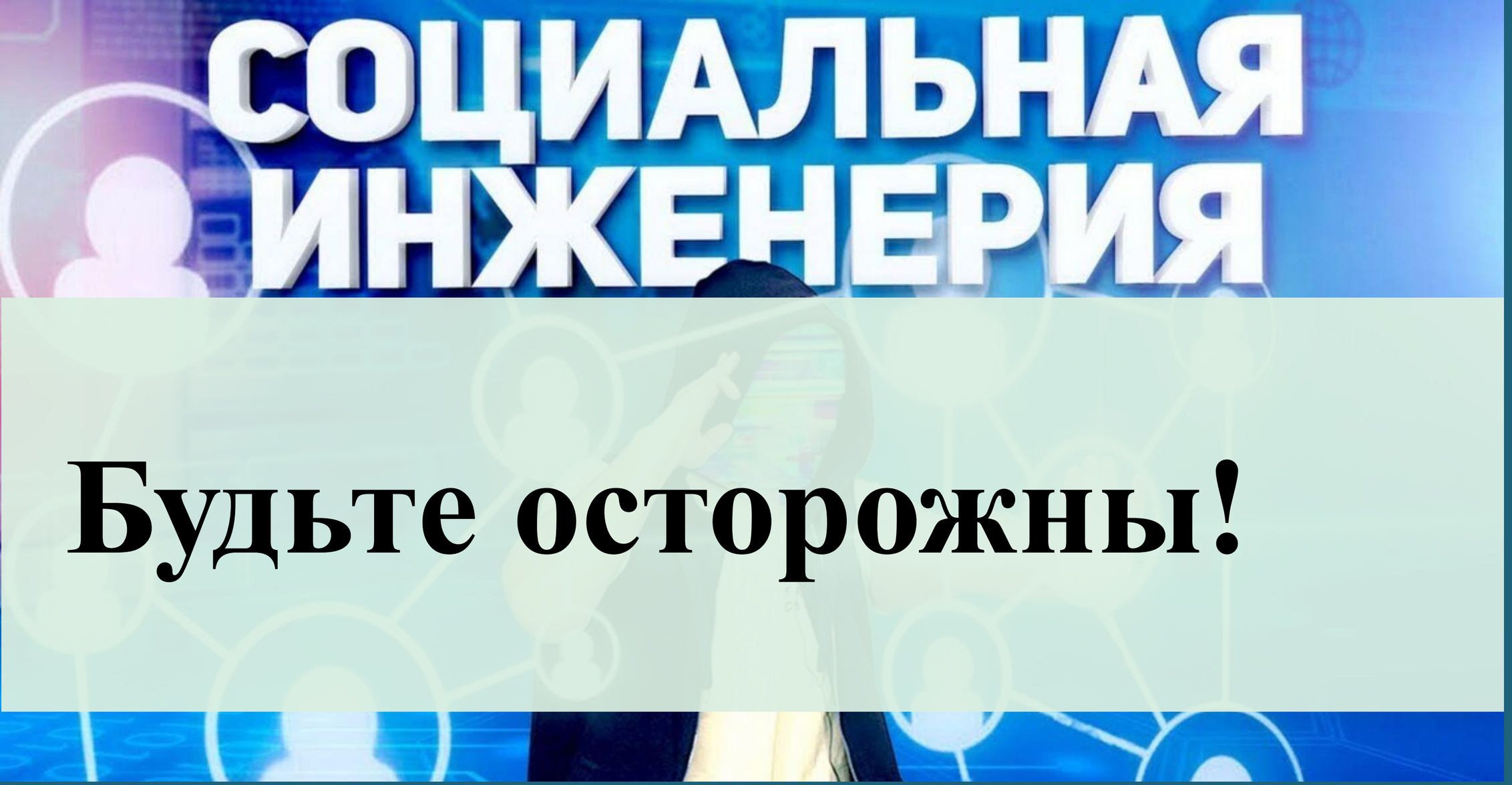
Usbkiller в действие



Обратная социальная инженерия

Техника при который злоумышленник сам заставляет идти жертву к себе, будь то реклама или же диверсия.

По сути, keylogger фиксирует все действия пользователя на клавиатуре, т.е. это некий «репитер» (повторитель), готовый в любой момент «слить» (куда следует) все то, что он за Вами нафиксировал.



Будьте осторожны!