ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ НЕПРОФЕССИОНАЛОВ

АНДРЕЙ ИГНАТОВ

ANDREY@IGNATOV.EMAIL

МИР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПОЛОН ОПАСНОСТЕЙ СМИРИТЕСЬ…

- **Против вас строят козни:**
- Профессионалы
- Обиженные (бывшие) сотрудники
- Агенты зарубежных разведок
- Мамкины хакеры
- Протестуны

- ***Важно!*** *Для причинения вреда не нужно быть «крутым хакером»*

ЧЕГО ОНИ ХОТЯТ
(И ОНИ МОГУТ ЭТОГО ДОБИТЬСЯ)

- Украсть ваши пароли от почты, внешних сервисов (типа файловых хранилищ) и внутренней ИТ-инфраструктуры
- Скопировать ваши файлы из внешних и корпоративных хранилищ
- Уничтожить ваши данные и ИТ-инфраструктуру
- Получить максимально возможный уровень прав к корпоративной ИТ-инфраструктуре для причинения максимального вреда
- Украсть номера кредитных карт и / или заставить вас перевести деньги
- Выложить от вашего имени компрометирующую вас информацию в публичные сервисы (типа VK)

КАКОЙ ВРЕД ВАМ ПРИЧИНЯТ

- Вы потеряете деньги
- Вы потеряете данные
- Вы станете объектом шантажа
- Вы потеряете репутацию

КАКИЕ ИНСТРУМЕНТЫ ЕСТЬ У ЗЛОУМЫШЛЕННИКОВ

- Специализированные устройства
- Портативные устройства общего назначения
- Свободно распространяемое программное обеспечение для тестирования на проникновение (взлома), например Kali Linux
- Мобильная версия Kali Nethunter
- Специализированное ПО, типа шифровальщиков
- Ваша доверчивость, невнимательность и лень

ВИДЫ УГРОЗ

- Кража паролей
- Кража передаваемой информации
- Кража номеров кредитных карт и денежных средств
- Доступ к ИТ-инфраструктуре организации с последующей кражей данных и уничтожением самой ИТ-инфраструктуры
- Установка зловредного ПО – троянов и шифровальщиков

КАК ЗЛОУМЫШЛЕННИКИ АТАКУЮТ ВАС

ПРЕДУПРЕЖДЕН – ЗНАЧИТ ЗАЩИЩЕН

ФИШИНГ

- Цель злоумышленника – заставить пользователя добровольно передать свой пароль или выполнить какое-либо действие
- Варианты реализации:
  - Письмо полностью повторяющее оформление известной организации компании или банка
  - Web-ресурс, для доступа к которому нужно ввести пароль
  - Копия интернет-магазина
  - Программа, которую необходимо запустить на ПК

КАК ЗАЩИТИТЬСЯ

- Обучение сотрудников
- Тренинги с использованием почтовых симуляторов
- Ограничение доступа сотрудников к ресурсам организации
- Максимальное подписание почтовых сообщений

ФАЛЬШИВЫЕ ТОЧКИ ДОСТУПА

- Фальшивые точки доступа могут встретиться
  - в аэропорту и на возале
  - в кафе и ресторане
  - в поезде и метро
  - на улице или в бизнес-центре
- Они могут называться:
  - название и/или модель роутера: **DIR-300**, **ASUS**
  - название по-умолчанию: **default**, **%provider_name%**
  - бесплатный Wi-Fi: **MosMetro_Free**, **Beeline_Free_Wi-Fi**
  - точки доступа различных заведений: **%airport_name_free%, McDonalds_WiFi_Free**
  - якобы частные точки доступа, где «по незнанию» не включено шифрование

ПРИМЕР КРАЖИ ДАННЫХ И ПАРОЛЕЙ С ИСПОЛЬЩЗОВАНИЕМ ФАЛЬШИВОЙ ТОЧКИ ДОСТУПА

- Иван находился в командировке и сейчас летит домой. Он ждет своего рейса в терминале, решил немного поработать, для этого ему нужен доступ к сети организации
- Иван хочет использовать бесплатный Wi-Fi аэропорта. Он видит доступную сеть **Airport_WIFI** и подключается к ней
- Но на самом деле эта сеть не имеет отношения к аэропорту. Это фальшивая точка доступа, которую организовал хакер с помощью своего ноутбука, либо специального устройства

СХЕМА РАБОТЫ ФАЛЬШИВОЙ ТОЧКИ ДОСТУПА

Иван отправляет запрос на получение данных с сервера своей организации, при этом он указывает свой пароль

Точка доступа хакера принимает запрос и пересылает его в сеть компании. Теперь пароль известен злоумышленнику

Сервер организации получает запрос и возвращает запрошенную информацию

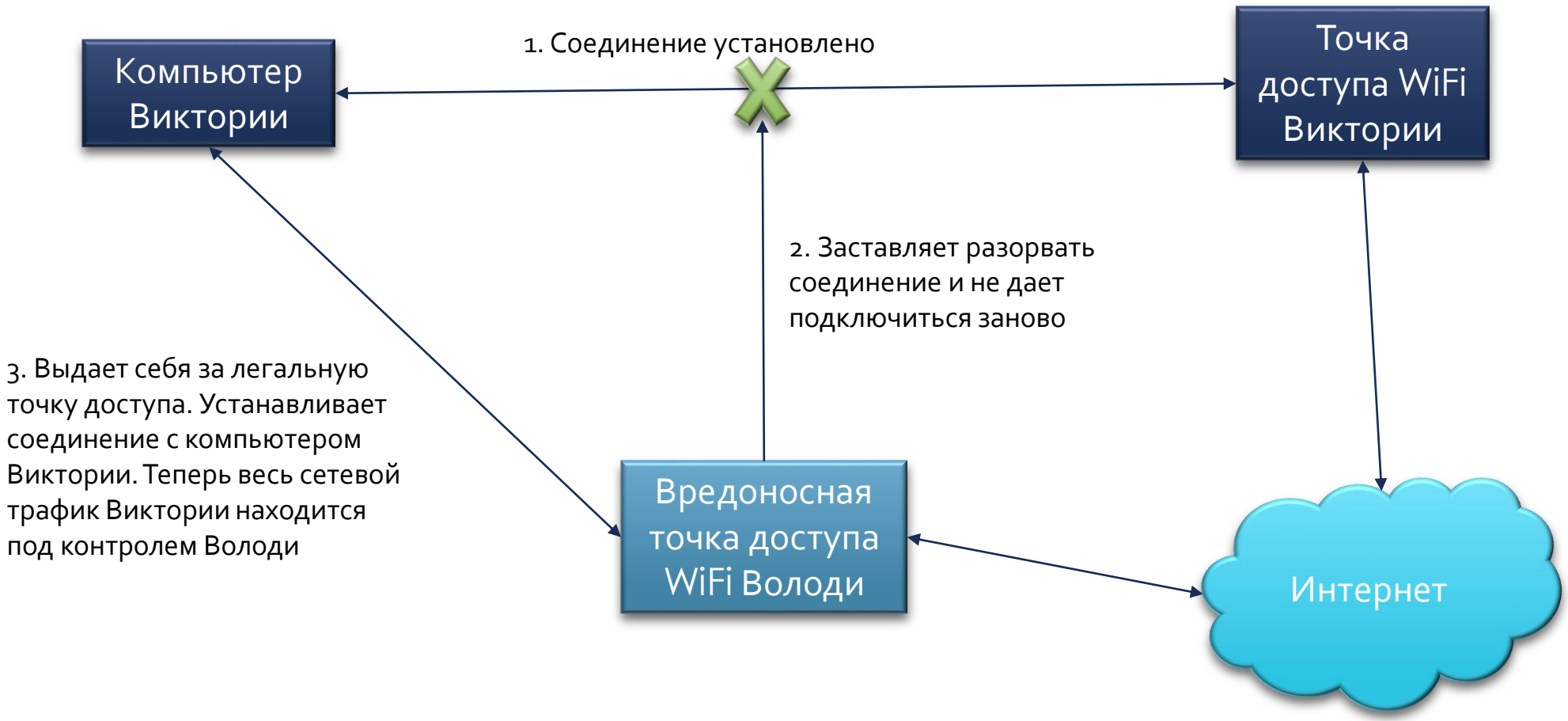
Теперь у хакера есть еще и информация Точка доступа возвращает результат запроса

Иван работает с информацией, не подозревая, что поделился данными и паролем (!) с хакером

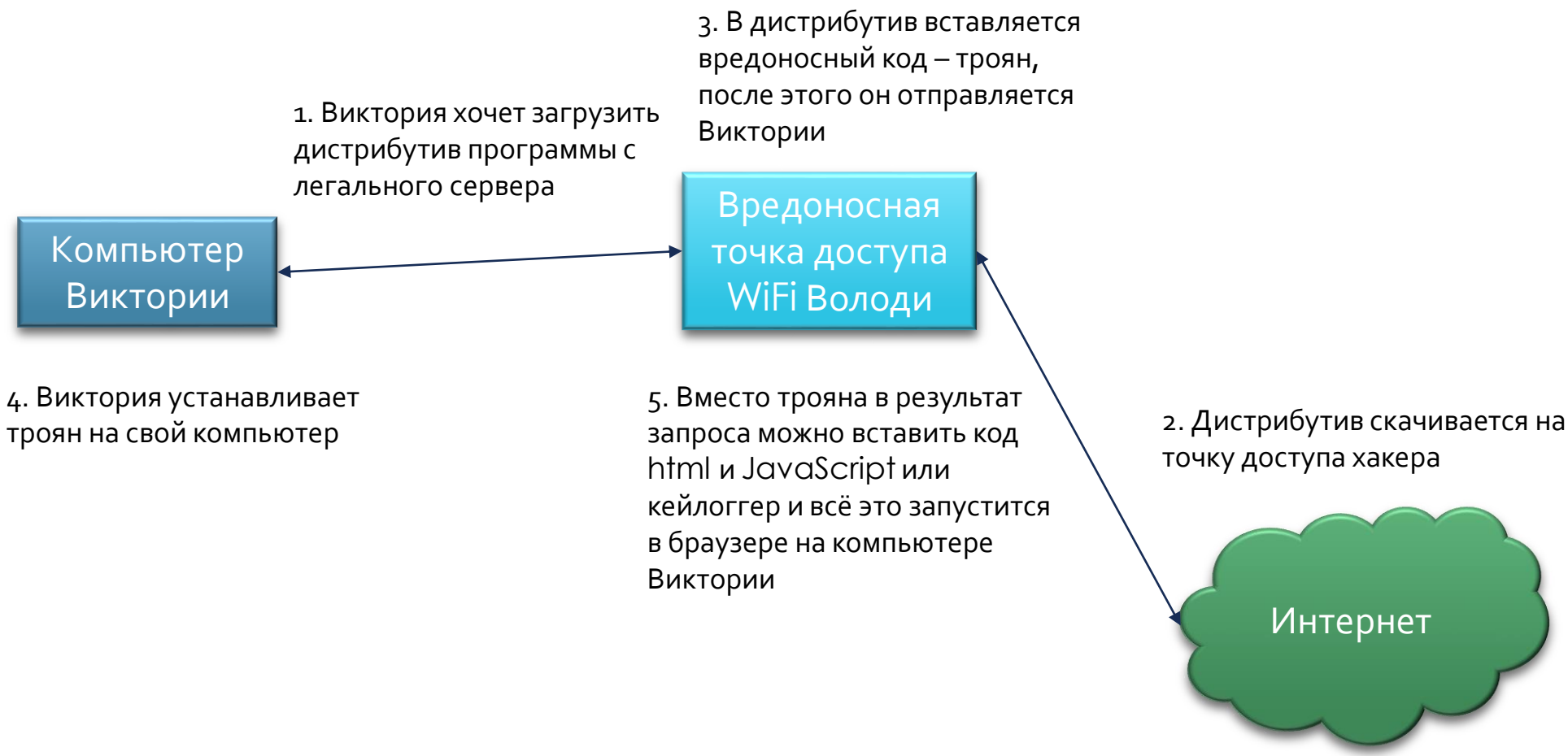
РАБОТА ИЗ ДОМА – НЕ МЕНЕЕ ОПАСНА

- Виктория работает из дома удаленно подключаясь к сети организации. Она использует подключение интернет провайдера и WiFi в своей квартире
- В соседней квартире живет подросток Володя, который считает себя крутым хакером
- Используя общедоступный инструментарий, Володя настраивает систему для взлома WiFi Виктории

СХЕМА ЗАМЕНЫ ЛЕГАЛЬНОЙ ТОЧКИ ДОСТУПА WIFI НА ТОЧКУ ДОСТУПА ЗЛОУМЫШЛЕННИКА

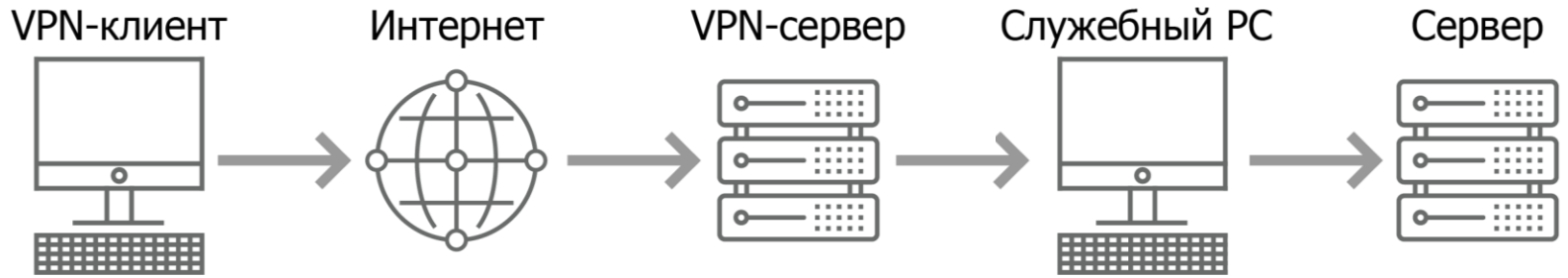


ЧТО ПРОИСХОДИТ ДАЛЬШЕ



КАК ЗАЩИТИТЬСЯ

- Использование виртуальной частной сети (VPN) для подключения к ИТ-ресурсам организации вне офиса
- Все передаваемые данные зашифрованы и не могут быть перехвачены злоумышленником
- Все передаваемые данные подписаны и не могут быть изменены



ПЕРВАЯ ПРОБЛЕМА ПАРОЛЕЙ

- Паролей стало слишком много:
  - Пароль на вход в операционную систему
  - Пароли к корпоративным системам
  - Пароли к социальным сетям
  - Пароли к личной почте
- В идеальном мире они должны быть разными
- На самом деле все ставят один и тот же пароль
- Если этот пароль узнает взломщик, то сможет получить доступ к любому ресурсу

ВТОРАЯ ПРОБЛЕМА ПАРОЛЕЙ

- В идеальном мире люди придумывают длинные, сложные пароли из произвольного набора букв разных регистров, цифр и знаков препинания
- На самом деле все пароли создаются по нескольким простым схемам (12345678qQ, P@ssw0rd, Misha1981 и т.п.)
- В идеальном мире люди помнят все свои пароли, а если и записывают, то в блокнот, который хранят в сейфе
- На самом деле пароли часто записывают на мониторах и клавиатурах, передают коллегам и знакомым

ТРЕТЬЯ ПРОБЛЕМА ПАРОЛЕЙ

- В идеальном мире пароль нельзя перехватить
- На самом деле уже давно существуют кейлоггеры, записывающие все введенные на клавиатуре символы
- В идеальном мире кейлоггер может сделать только опытный бородатый хакер, а краже пароля тут же узнает пользователь
- На самом деле кейлоггер сейчас доступен простому школьнику, а факт его использования, как и факт перехвата пароля отследить невозможно

И ГЛАВНАЯ ПРОБЛЕМА ПАРОЛЕЙ

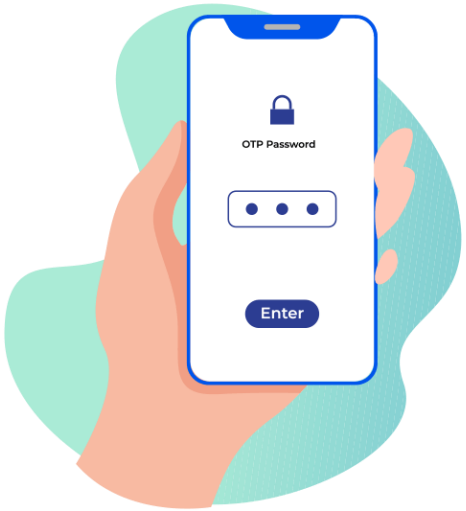
- Пароль не материален
- Его можно украсть и пользоваться без ведома владельца
- Владельцу будет сложно оказать, что деструктивные действия совершил не он, а тот, кто украл его пароль

КАК ЗАЩИТИТЬСЯ

- Использовать многофакторную аутентификацию
  - Первый фактор – **владение** каким-либо устройством
  - Второй фактор – **знание** пароля (в т.ч. к данному устройству)
  - Третий фактор – **биометрия** (отпечаток пальца, лицо и пр.)
- В большинстве случаев используют двухфакторную аутентификацию на основе двух из трех факторов
- Требуется операторам персональных данных

ВАРИАНТЫ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

- Криптографический токен
- Смартфон
- Биометрический считыватель



Для прохождения опроса перейдите по ссылке или сканируйте QR-код:

ПРОГРАММЫ ШИФРОВАЛЬЩИКИ

- Один из видов вирусов
- Шифрует все файлы на локальном ПК и / или в сети предприятия
- За расшифровку требует перечисления денежных средств

КАК ЗАЩИТИТЬСЯ

- Не устанавливать непроверенное ПО
- Не давать сотрудникам не права на ИТ инфраструктуру, которые им не нужны
  - Для этого используется ПО типа IDM и PAM
- Регулярно выполнять резервное копирование с возможностью быстрого восстановления
- Разработать регламент быстрого восстановления

СПАСИБО ЗА ВНИМАНИЕ!

ANDREY@IGNATOV.EMAIL