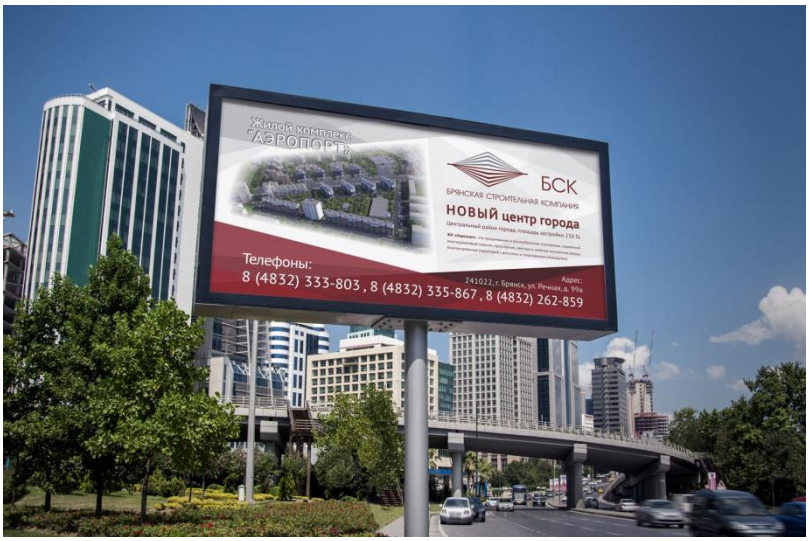
ЛЕКЦИЯ 12. АТАКИ НА БИЛБОРДЫ (РЕКЛАМНЫЕ ЩИТЫ) И БОКСЫ ДЛЯ ПОЛУЧЕНИЯ ПОЧТЫ

12.1. Рекламные LED экраны

Рекламный щит (также билборд от англ. billboard) — щит большого размера для размещения наружной рекламы, устанавливаемый вдоль трасс, улиц. Билборды, которые всегда были основой рынка наружной рекламы, выходят на просторы high-tech, приняв форму электронного светодиодного билборда – светодиодного видеоэкрана. Когда смотришь на электронный билборд, то он выглядит как обычный статичный щит, за исключением одной детали: каждые 6-8 секунд изображение на нем меняется, представляя взору публики новое рекламное сообщение.



Обычно билборд – это стенд из нескольких больших мониторов, подключенных к неттопу, на котором стоит ОС с Windows или Linux. Этот неттоп не подключен к сети и на него загружается видео-реклама непосредственно с флешки. На неттопе задаются задания в планировщике, которые запускают нужные видео в нужное время на воспроизведение. Неттоп физически находится в стенде билборда и закрыт на ключ.

Билборд также может обслуживаться и через интернет по удаленному доступу.

12.2. Уязвимости билбордов

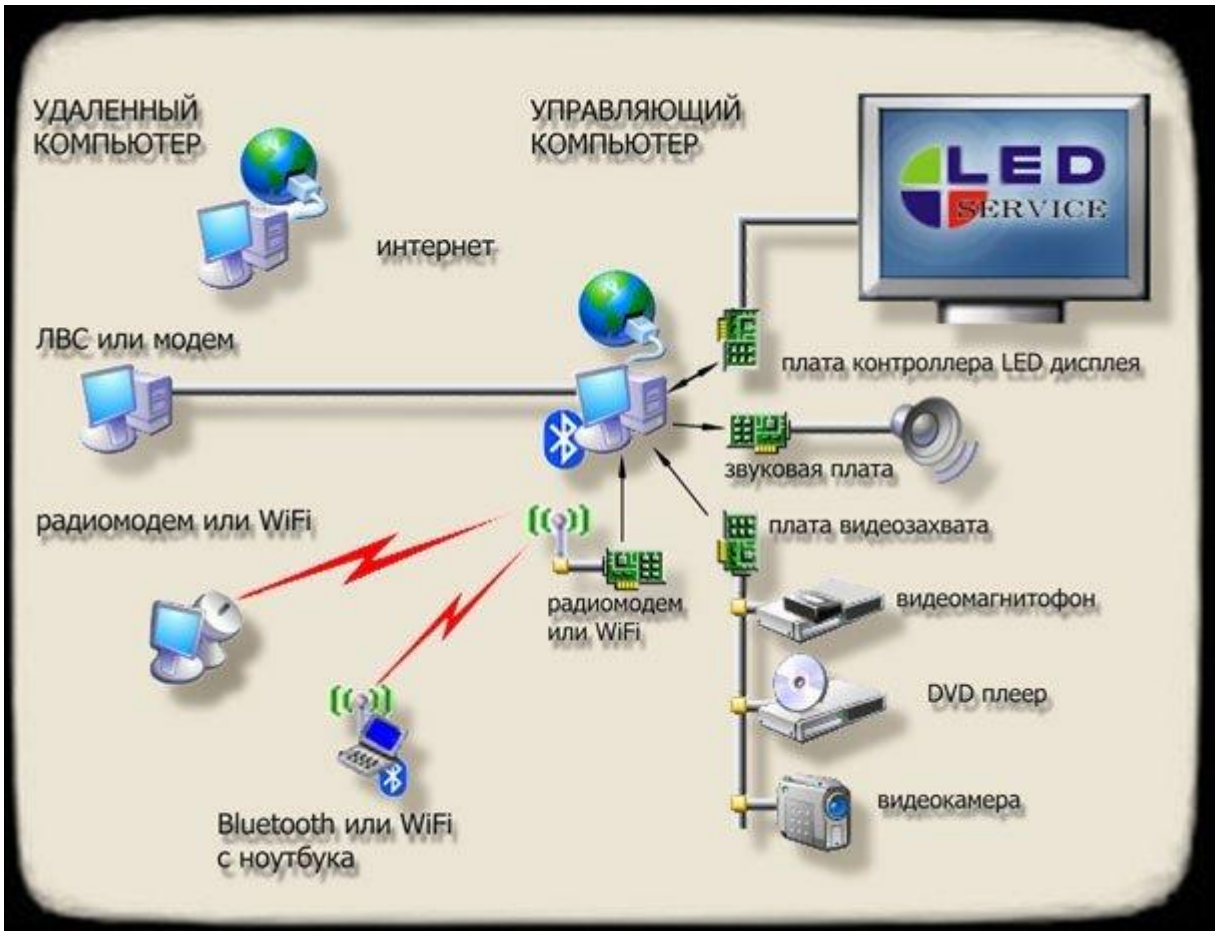
Первый вариант работы LED экрана – это когда у него нет доступа по внешнюю сеть Интернет, и информация поступает с помощью носителей (флешки). В таком варианте большинство уязвимостей исключаются и остаются те, которые касаются физического прямого воздействия на устройство. И угрозы не обязательно должны касаться прямого взлома устройства. Даже простое выведение из строя устройства с помощью отключения электропитания является критическим.

Основными рекомендациями к такому варианту по защите могут быть:

- Реализовать физическую + организационную защиту с помощью видеонаблюдения, сигнализации, защитного шкафа;
- Ответственный субъект (администратор), который следил бы за работой устройства.

Данный вариант крайне не удобен для администратора, так как нельзя следить за устройством удаленно.

Второй вариант подразумевает подключение устройства к серверу управления через беспроводные технологии (3g, wi-fi и тд). В таком случае мы имеем целый ряд угроз, характерных для сетевых технологий. Начиная от угроз отказа служб на устройстве, заканчивая перехватом управления устройства. При удаленном подключении билборда LED экраны имеют такие же уязвимости, как и домашние ПК или сервера. Имеются случаи о взломах таких экранов, где вместо рекламы транслировался видео поток 18+ и т.д.



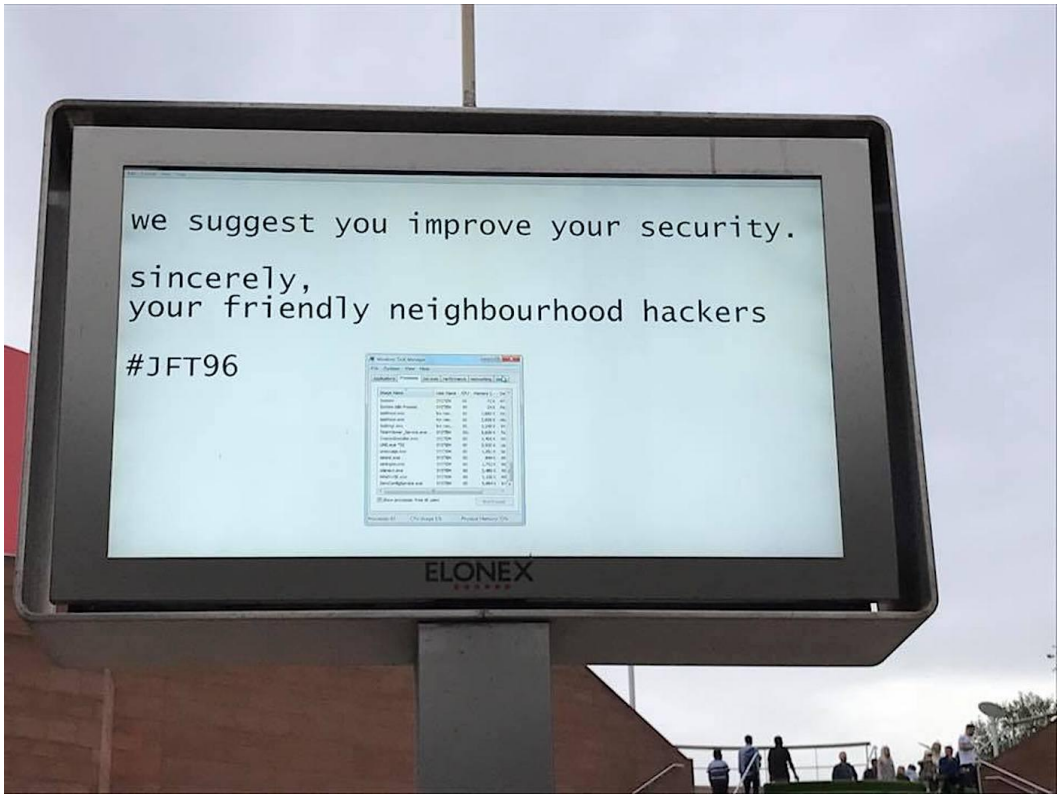
12.3. Известные атаки

Март 2008. Хакерский взлом в Лос-Анджелесе 10 городских экранов. На всех городских светодиодных экранах компании Clear Channel в паузы между коммерческими роликами внедрили изображение черепа. Комментаторы данного события в СМИ писали, что, как только появляется что-то цифровое, то возникает желание это взломать.

Март 2009. Хакеры в Нью-Йорке взломали электронные дорожные знаки. Неизвестные шутники взломали и перепрограммировали ряд электронных дорожных знаков в центре Нью-Йорка. Вместо нормальных предупреждений водителям их табло теперь показывают фразы “Нью-Йорк гибнет”.

Май 2017. Хакерам удалось взять под свой контроль рекламный щит за пределами торгового центра в Ливерпуле.

И они воспользовались возможностью, чтобы оставить замечательно вежливое сообщение: «Рекомендуем вам усилить вашу безопасность. Искренне ваши, Дружелюбные хакеры по соседству #JFT96».



«JFT96 - Justice for the 96». Это фраза стала девизом против несправедливости после происшествий на стадионе Хиллсборо в 1989 году. Тогда случилась давка, в результате которой погибли 96 человек, но правительство это объявило как "толпа пьяниц устроила беспорядки, в результате которой сами погибли". С тех пор, до прошлого года, ежегодно, 15 апреля проходили церемонии в честь погибших 96 на том злосчастном матче Ливерпуля против Ноттингем Форест.

Разработчик под ником «BITcrash44» опубликовал видео на YouTube, на котором он перехватывает видеосигнал с билбордов в Нью-Йорке, заменяя его изображением со своего iPhone. Для этого он использовал самодельный видео-репитер и передатчик, подключенный к стандартному аудиовыходу iPhone 4.

Разработчик пишет:

«Система работает крайне просто: подключаем передатчик в гнездо наушников iPhone 4 и включаем любой видеоролик из медиатеки iPod или фототеки. Передатчик транслирует видеосигнал на видеорепитер, а репитер, в свою очередь, передает его на любой экран, расположенный поблизости. Не имеет значение какого размера будет принимающий экран, потому что видео сохраняет пропорции, оставляя по краям черные полосы.»

«Для своей демонстрации я выбрал Таймс-сквер, потому что здесь расположено большое количество видеоэкранов. В то же время это одна из самых защищенных площадей Нью-Йорка, что несколько подогревает мой интерес. На ролике вы можете видеть, что репитер достаточно мощный, хотя сигнал остается не совсем стабильным. Я работаю над этим. Позже я опубликую еще один ролик с объяснением того, как я смог сделать подобную штуку.»

Ну и также нельзя, не взять во внимание статью о «хакере» Максе Корнелиусе :)

Надпись на таблоиде: Макс король :)

Необычный рекламный трюк придумала голландская ИТ компания Infosupport. С целью привлечения молодых, талантливых ИТ специалистов и стажеров, в 2008-2009 году был снят ряд видеороликов о великом хакере Максе Корнелиусе (Max Cornelisse), которые были размещены на Youtube канале Bas Welling. Макс управлял разводным мостом с помощью PDA, менял расписание на вокзале, менял информацию на дорожных информационных табло и , подключившись к телесуфлеру в телестудии, изменил текст, сообщаемый журналистами в прямой эфир (журналисты объявили Макса нобелевским лауреатом :)), и много других потрясающих вещей.

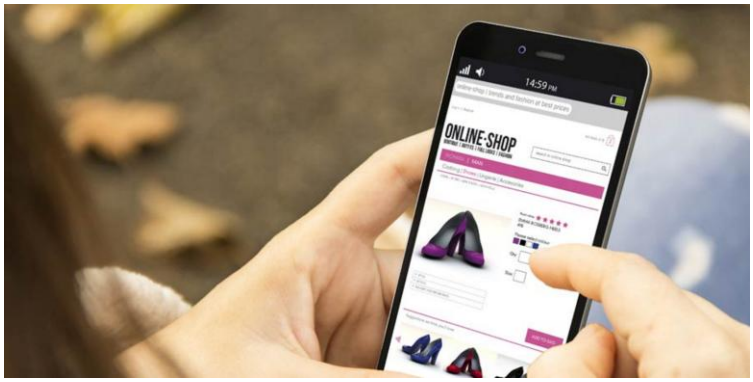
Для хакера он был слишком неосторожен, показывая свое лицо и имя в своих видеороликах. На самом деле это просто потрясающая вирусная реклама.

12.4. Уязвимости Постамата

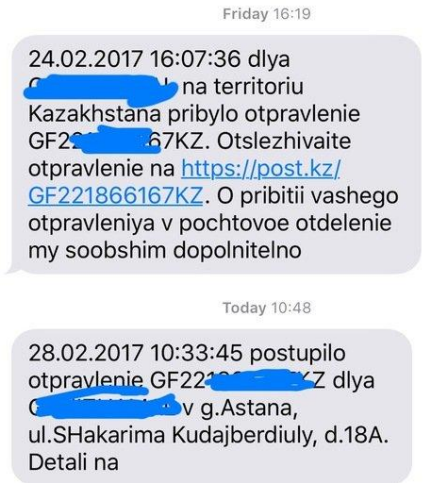
Постаматы (почтоматы) – терминалы с почтовыми ячейками, почтовые автоматы, являющиеся пунктами выдачи товаров из интернет-магазинов.

Как происходит оплата и доставка товара посредством постаматов?

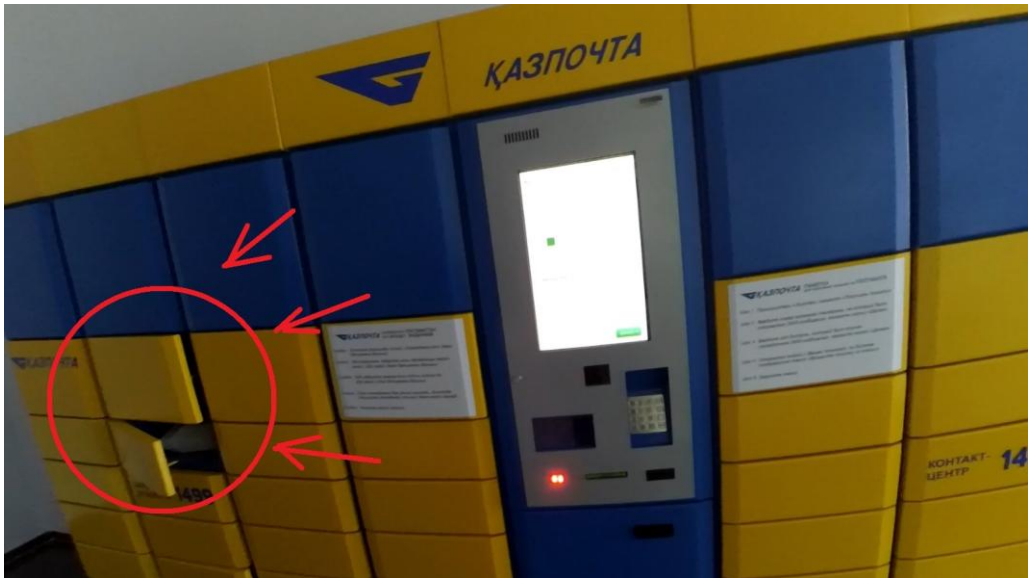
1. Покупатель оплачивает заказ или выбирает пост-оплату заказа.



2. В момент доставки заказа в постамат покупателю приходит СМС с кодом получения заказа.



Покупатель в удобное ему время приходит к выбранному терминалу, вводит код, вносит деньги (при постоплате) и забирает свой товар из ячейки. Сдача поступает на мобильный телефон, в личный кабинет (QIWI) или на электронный кошелек.



Получив извещение о том, что заказ ждет вас в Постамате, вы можете быть уверены, что он дождется вас в целости и сохранности:

- ПОСТАМАТ ЗАЩИЩЕН ОТ ВЗЛОМА. Он представляет собой крепчайший металлический шкаф. Каждая ячейка снабжена надежным электронным замком, а сам терминал оборудован видеокамерами. Кроме того, в отличие от европейских коллег, принципиально против размещения терминалов на улице. Постаматы стоят в торговых центрах, супермаркетах, где, как правило, есть служба охраны. Таким образом, максимально обезопасили Постаматы и от взлома, и от вандализма.
- ПОСТАМАТ ЗАЩИЩЕН ОТ «ЧЕЛОВЕЧЕСКОГО ФАКТОРА». Система устроена так, что получение вашей покупки посторонним лицом исключено. Все коды индивидуальны. Они обозначают ячейку именно с вашим товаром. Курьер при закладке заказов также не может перепутать, что куда поместить: он подносит коробку с уникальной маркировкой к считывающему устройству и в ответ автоматически открывается нужная ячейка.

Таким образом на данный момент (пока) в действующей системе постомата нету уязвимостей, если не брать во внимание перехват sms-сообщений пользователя (SS7 Attacks: Intercepting SMS).