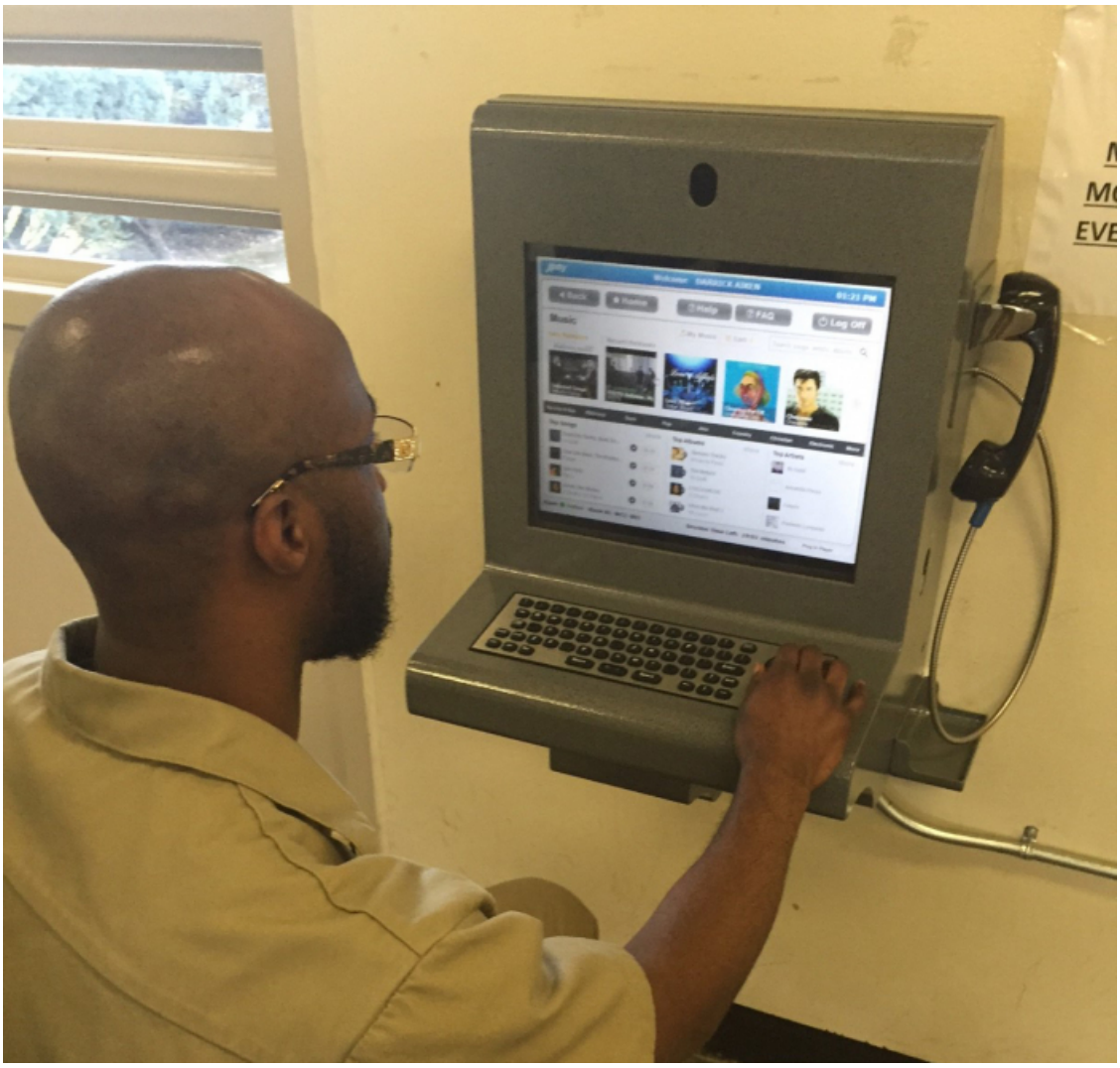
Тюремный хакинг

Технологии дали преступникам еще одно бескрайнее поле для "творчества", благодаря которому стены тюрем уже не преграда для совершения новых преступлений. И если в России преступники из мест заключения могут позволить себе лишь банальные телефонные мошенничества, то в США злодеи ушли далеко вперед. Осваивая технологии по полной, они умудряются взламывать базы данных и даже строить в тюрьмах подпольные телекоммуникационные сети.

Минувшим летом издание Associated Press поведало миру диковинную историю о том, как 364 заключенных в штате Айдахо обнаружили некий баг в планшетах компании JPay и с помощью этой уязвимости набрали кредитов. Как такое стало возможным, спросите вы? Дело в том, что в тюрьмах США подход к использованию современных средств связи среди заключенных несколько иной, нежели в российской пенитенциарной системе. Во многих американских тюрьмах заключенным доступны видеоигры, а также использование онлайн-сервисов для денежных переводов или видеосвиданий.

И с некоторых пор компания JPay, с разрешения Департамента исправительных учреждений США, начала устанавливать в тюрьмах специальные киоски и раздавать заключенным планшеты, которые могут синхронизироваться с этими киосками и даже работать с Wi-Fi.



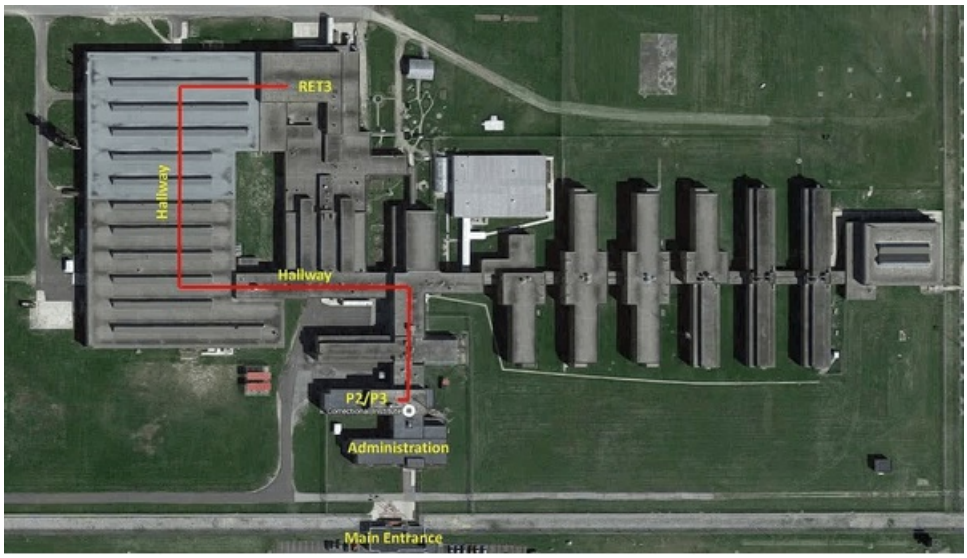
Для того чтобы закачивать различный контент на планшеты, заключенному нужно было иметь определенную сумму на специальном электронном счету. Для этого используются специальные медиа-аккаунты или JPay Credits, и простая, по своей сути, кредитная система. Спустя некоторое время, заключенные сумели найти лазейку, благодаря которой кредитовали сами себя, украв, таким образом, порядка 225 тысяч долларов.

Смешно, но эта история еще "цветочки" по сравнению с произошедшим в тюрьме Мэрион штата Огайо. 3 июля 2015 года IT-отдел тюрьмы получил сообщение от новой системы компьютерной безопасности, в котором утверждалось, что компьютер под логином canterburyrl, принадлежавший Рэнди Кентербери из компании RET3 (некоммерческая организация, занимающаяся утилизацией мусора на территории тюрьмы), существенно превысил лимит интернет-трафика. Этот звоночек оказался не последним и уже 6 июля IT-служба Мэрион получила семь оповещений о хакерских

атаках все того же canterburyrl и 59 оповещений об обходе блокировки с помощью "прокси". Выяснилось, что пользователь часами "бродил" по запрещенным ресурсам.

Несмотря на то, что логин пользователя был известен и принадлежал сотруднику некоммерческой организации, работающей на территории тюрьмы, вычислить нарушителя не представлялось возможным, хотя бы потому, что в дни, когда была зафиксирована подозрительная активность, владелец аккаунта Рэнди Кентербери находился дома, поскольку у него был "выходной".

Спустя несколько дней кропотливой работы, IT-служба Мэрион все же сумела "взять след": специалисты обнаружили имя компьютера, с которого и совершались несанкционированные подключения. Оно содержало в себе сочетание lab9 – так обозначались устройства из компьютерного класса для персонала тюрьмы. Но загвоздка был в том, что там располагалось лишь шесть компьютеров, а не девять.



Так тюрьма Мэрион выглядит с воздуха

Долгое время сотрудники IT-отдела не могли установить точное местоположение компьютера. Однако вскоре удалось обнаружить коммутатор и порт, куда он был подключен.

Сетевой хаб тюрьмы представлял собой классику кабельного ужаса. Из него разноцветные провода уходят в разные стороны в совершенно хаотичном порядке.



В итоге разбирательств выяснилось, что один из проводов проходил по потолку в учебном зале. За потолочными панелями и обнаружилось несколько подключенных, но неучтённых системных блоков.



Тот самый системный блок Dell


Место, где были обнаружены компьютеры

Следующие несколько дней сотрудники тюрьмы размышляли над тем, как действовать дальше. Метки на обнаруженных под потолком компьютерах говорили о том, что один из них принадлежал местной районной школе, а второй – компании, расположенной неподалеку.

Спустя несколько недель в тюрьму прибыла команда следователей, и работы по установлению преступников закипела. Из тюремных компьютеров было изъято более сотни жестких дисков. Следователи опрашивали всех: от заключенных до руководства тюрьмы. Ключевыми оставались вопросы: "Откуда могли взяться компьютеры?" и "Кто мог спрятать их под потолком?".

В одном из "нелегальных" компьютеров нашли целый список инструментов начинающего хакера: от браузера Tor до приложений для шифрования и отправки спама. Однако настоящей находкой для следователей стала программа для обмена текстовыми сообщениями, с помощью которой и удалось выйти на преступников. Ими оказались Адам Джонсон и Скотт Сприггс, отбывающие наказания за тяжкие преступления.



Адам Джонсон крайний справа

В тюрьме Джонсон, и Сприггс приобрели технический опыт. Сприггс проходил курсы по программированию на C и C++, изучал создание баз данных. Со временем Сприггс стал системным администратором тюремной системы обучения и помогал устанавливать новые компьютеры, что позволило ему стать специалистом еще и по оборудованию. Джонсон же изучал Visual Basic – несложный язык программирования.

Примечательно, что, несмотря на доказанный следствием факт сообщничества, Джонсон взял всю вину на себя и не выдал товарища следствию. С его слов, он украл у RET3 несколько компьютеров, которые Сприггс собрал для нужд тюрьмы, и спрятал их под потолком. В дальнейшем, он использовал украденный пароль одного из сотрудников RET3 – того самого Рэнди Кентербери.

Как удалось выяснить следствию, Джонсон и Сприггс не просто гуляли по сети, но также перехватывали тюремный трафик и взламывали аккаунты сотрудников исправительного учреждения. В интернете их интересовали материалы об изготовлении наркотиков и взрывчатки в домашних условиях, а также схемы мошенничества с банковским картами и возвратом налогов. Им даже удалось выпустить несколько кредитных карт на имена других заключенных.

Кроме этого, Джонсон и Сприггс благодаря своим возможностям организовали на территории тюрьмы что-то вроде черного рынка порнографии и видеофильмов. Они скачивали контент с интернета на SD-карты, а затем продавали заключенным, которые могли просматривать его на Nintendo Wii

Теперь два друга сидят в разных тюрьмах и видимо до конца своих дней проведут за стенами исправительных учреждений, возможно даже, что без какого-либо доступа к информационным технологиям.