Хакеры **отелей**

pandasecurity.com

panda

Хакеры отелей

После долгих лет работы в сфере компьютерной безопасности, есть одна вещь, которую мы знем точно: основная мотивация кибер-преступников - это деньги.

Именно поэтому хакеры используют трояны для получения конфиденциальных данных: специальные программы заражают наши компьютеры и устройства для кражи данных.

Одним из примеров является **CryptoLocker - популярная атака, которая использует "шифровальщик" для шифрования важной информации**, после чего жертва вынуждена платить выкуп за расшифровку данных.

Мы были свидетелями "классических" вредоносных программ и новых атак, разработанных специально под каждую отдельно взятую жертву, и мы видели, что делали компании в рамках этих атак.

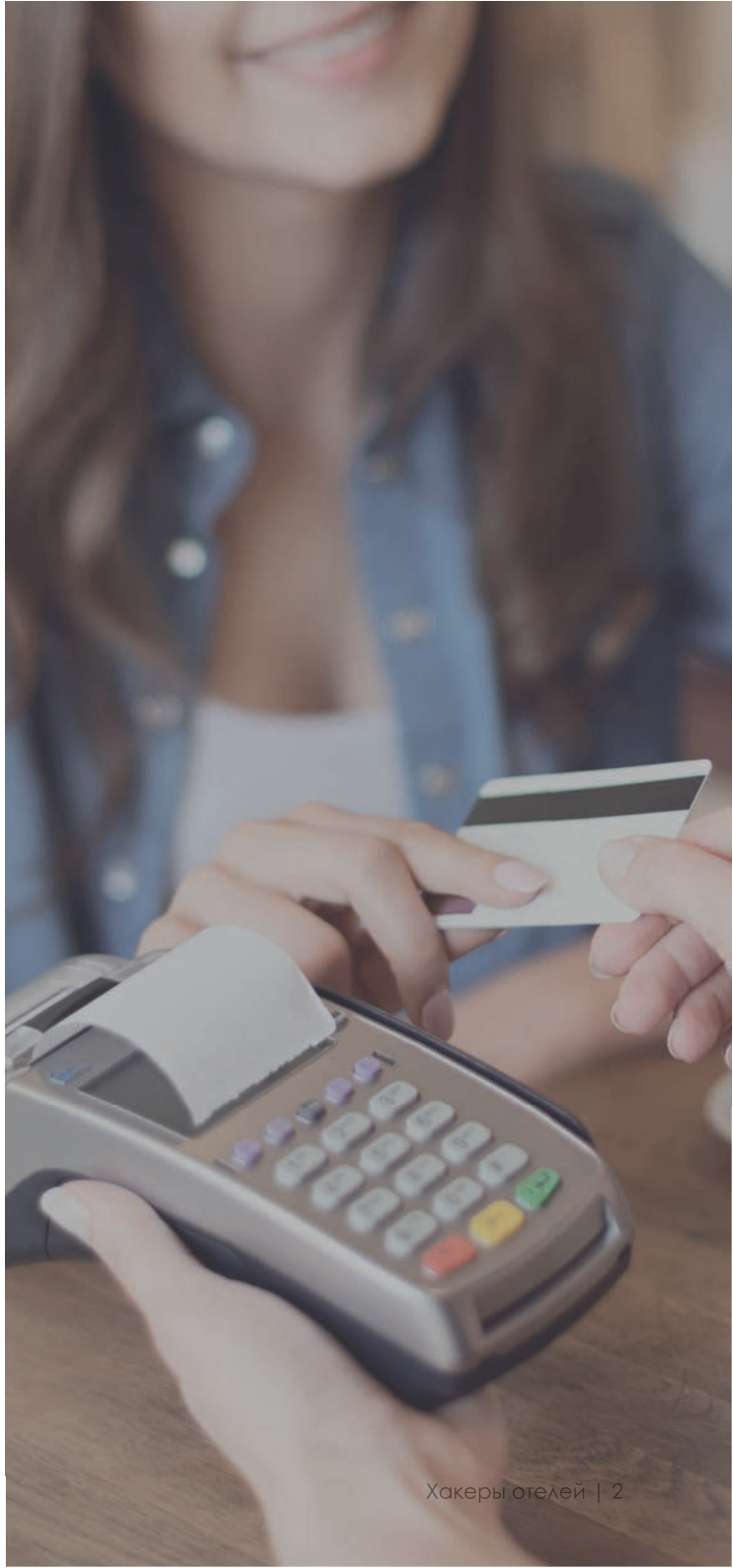
Совсем недавно эти кибер-преступники прошлись по гостиничным сетям.

Почему отели?

Хакеры видят: отели - прибыльный бизнес.

Когда хакер рассматривает отель в качестве следующей жертвы, он думает над там, что сможет "взломать" миллионы гостиничных номеров, в которых проживают миллионы людей, тратя миллионы долларов.

Начиная от бронирования номера и заканчивая платежами в рестаранах и гостиничных магазинчиках, гостиницы имеют сложные сети, которые хранят огромное количество критически важных и персональных данных, и хакеры только и желают их взломать. Если Вы недавно останавливались в отеле, то, возможно, есть смысл еще раз проверить операции по Вашей кредитной карте…



Обещанная история

2015 год установил новую веху в этой сфере деятельности.

К 2015 году **большинство отелей вне зависимости от их размеров стали жертвами кибер-преступлений**.

Кибер-преступники также "положили" глаз на те компании, которые оказывают услуги для отелей.

White Lodging

White Lodging управляет рядом известных гостиниц, таких как Hilton, Marriott, Hyatt, Sheraton и Westin. Хотя они представляют собой больше компанию по управлению отелями, нежели сеть гостиниц, они также стали жертвами крупной кибер-атаки, о которой стало известно в 2014 году.
В 2013 году **в четырнадцати их гостиницах была скомпрометирована информация о кредитных и дебетовых картах клиентов**.

Спустя два года они столкнулись с еще одной атакой на десять своих отелей (некоторые из них были жертвой предыдущей атаки). Хакеры нанесли еще больший урон, украв данные по кредитным картам клиентов: имена держателей карт, номера, коды безопасности и сроки действия. По данным White Lodging, эта атака отличалась от той, что была в 2013 году.

Пострадало 24 отеля

Mandarin Oriental

Роскошный Mandarin Oriental был атакован в марте 2015 года. **Вредоносная программа заразила POS-терминалы** в некоторых отелях группы, расположенные в Европе и Америке.

Вредоносная программа была специально разработана и направлена на такие типы машинных систем, позволяя осуществлять кражу информации о кредитных картах.

Скопрометированы тысячи кредитных карт

Trump Hotels

В период с мая 2014 до июня 2015 было атаковано семь заведений.

Как они сами признались, **были украдены данные кредитных карт клиентов через зараженные POS-терминалы и ПК**, расположенные в их ресторанах, магазинах с сувенирами и т.д.

Преступникам хватило одного года, чтобы получить огромный объем персональной конфиденциальной информации.

Десятки зараженных ПК и POS-терминалов

Hard Rock Las Vegas

В результате атаки было заражено несколько POS-терминалов в их ресторанах, барах и магазинах. Но устройства в отеле или казино не пострадали.

В течение семи месяцев (с сентября 2014 до апреля 2015) Hard Rock Las Vegas столкнулся с **атаками, которые привели к краже данных 173 000 банковских карт** из их ресторанов, баров и магазинов.

Но они были не единственным пострадавшим отелем/казино. FireKeepers Casino Hotel в Battle Creek также пострадал в 2015 году.

Украдено 173 000 банковских карт

Hilton Worldwide

В ноябре 2015 года Hilton Worldwide распространил пресс-релиз, в котором компания призналась, что стала жертвой кибер-атаки.

Они не сообщили подробной информации о том, что же произошло, но известно, что **была скомпрометирована вся информация о кредитных картах клиентов**.

К счастью, PIN-коды и другая персональная информация не пострадали.

Доступ к конфиденциальной информации

Starwood

Примерно в то же самое время, когда была атака на Hilton, Starwood сообщил о том, что они стали жертвой аналогичной кибер-атаки.

Было атаковано 105 отелей в сети Starwood (Sheraton, St. Regis, Westin, W и т.д.), что сделало эту атаку **крупнейшей атакой на отели подобного рода на тот момент**.

Они опубликовали список отелей, где были заражены их POS-терминалы.

Пострадало 105 отелей

Hyatt

Рекорд Starwood продержался недолго. Потом произошло то, что мы знаем как крупнейшая в истории кибер-атака на отели.

Сеть отелей Hyatt в своем пресс-релизе подтвердила, что были **заражены POS-терминалы в их 249 отелях, расположенных в 54 странах мира**.

С июля по сентябрь 2015 года были заражены их POS-терминалы (опять же!), после чего были украдены данные кредитных карт всех их клиентов.

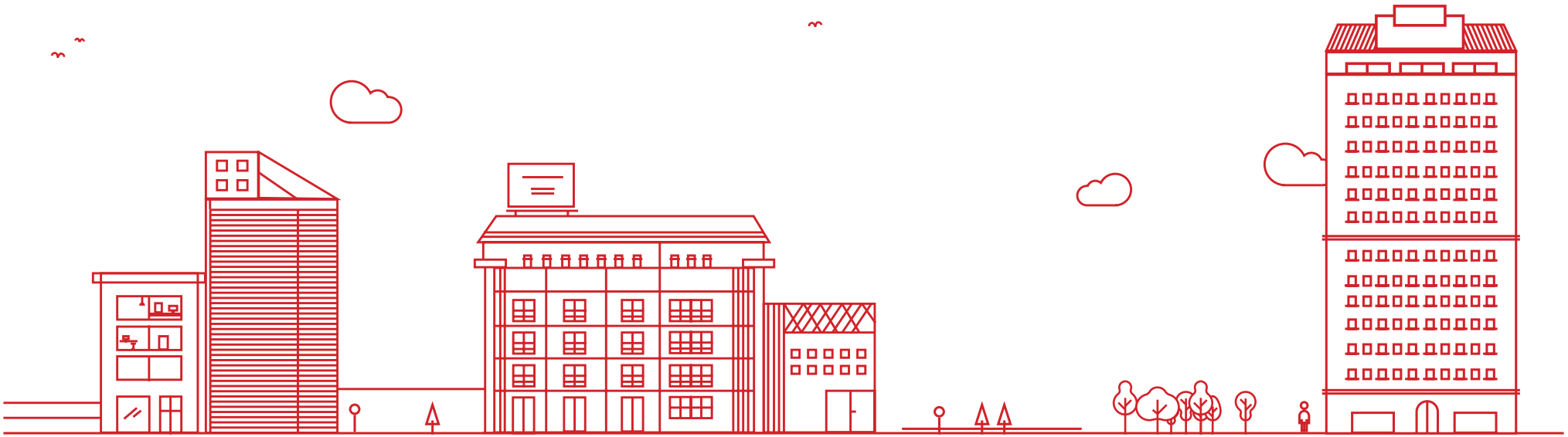
Пострадало 249 отелей

Rosen Hotels & Resorts

Самыми последними жертвами стали Rosen Hotels & Resorts. Пока они не предоставили подробностей кражи, но они подтвердили, что их **POS-терминалы были заражены вредоносными программами с сентября 2014 до февраля 2016**.

Заразив их POS-системы, неизвестные лица получили доступ к данным кредитных карт клиентов учреждений Rosen за последние полтора года.

1,5 года они были заражены и не знали об этом



Это не прихоть

За всеми этими атаками стоит реальный экономический интерес. **Гостиничный бизнес стал одной из основных целей для кибер-преступников**.

Помимо мотивации, стоит отметить и наличие вредоносных программ, специально разработанных для сбора важной информации о кредитных картах через POS-системы. Очевидно, что эти хакеры не собираются уходить на покой в ближайшее время.

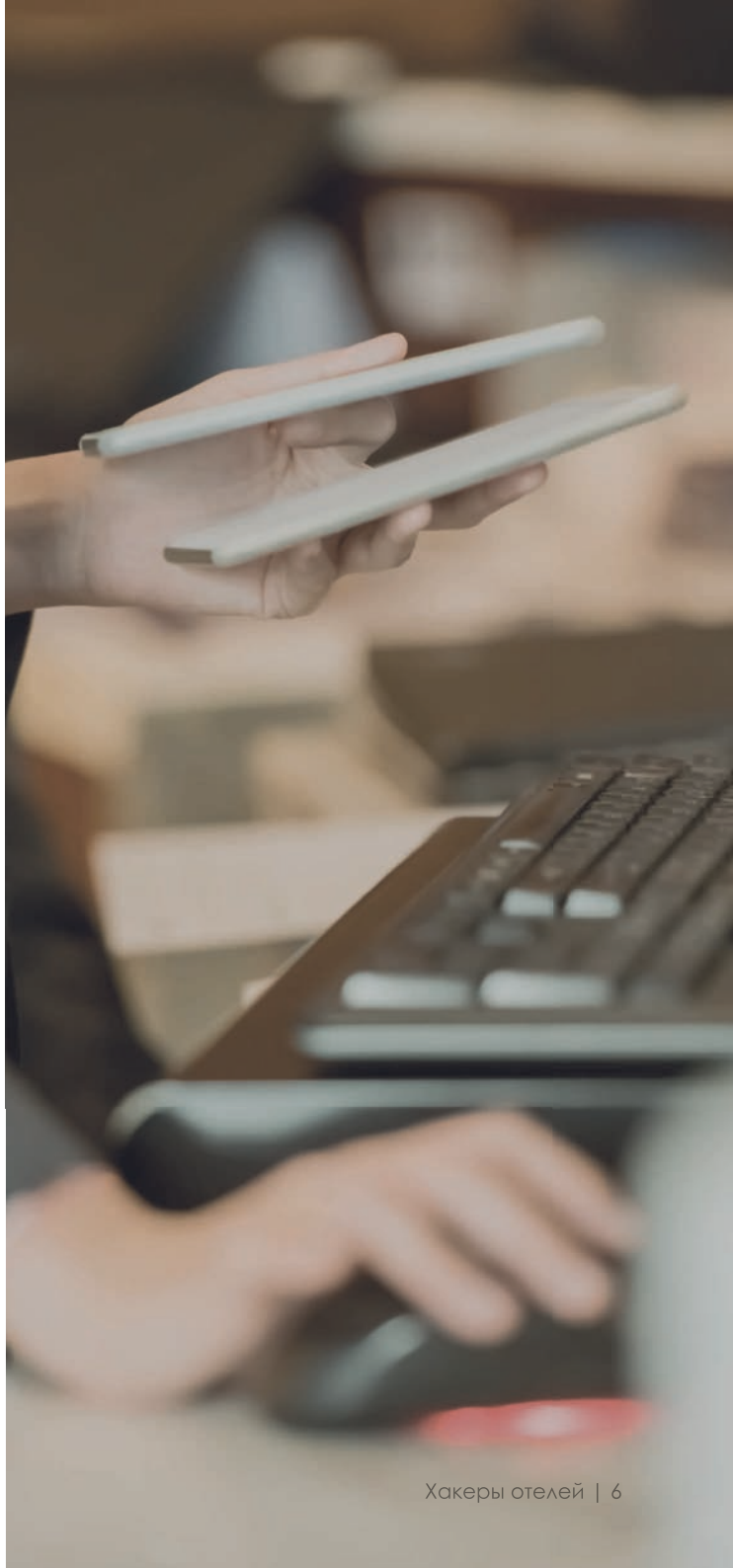
Эта тревожная ситуация влияет на гостиничный бизнес не только с экономической точки зрения, но также подрывает его репутацию, вызывает панику среди клиентов и дестабилизирует бизнес.

Мы должны быть начеку

Вредоносные программы, которые заражают POS-терминалы для кражи данных по кредитным картам, а также целенаправленные атаки на ИТ-системы отелей для кражи конфиденциальной информации - это два примера того, что может случиться в результате кибер-атаки. Подобные атаки имеют негативное влияние на финансовое состояние отелей и их репутацию.

Отелям необходимо усилить меры безопасности в своих сетях, на устройствах и в системах, а также знать, как выбрать наиболее подходящее решение для защиты их ИТ-систем.

Не любая система защиты подходит для гостиничных сетей, потому что каждая из них предлагает разные уровни безопасности, и не каждая способна защитить их в любой цифровой экосистеме или окружении.



Решение

Для защиты от современных угроз и целенаправленных атак мы должны иметь систему, которая обеспечивает конфиденциальность информации, защиту данных, деловой репутации и ИТ-активов.

Adaptive Defense 360 **- это первый и единственный сервис информационной безопасности, который сочетает в себе один из самых эффективных традиционных антивирусов с самой современной защитой и возможности классификации всех исполняемых процессов**.

Adaptive Defensive 360 способен обнаруживать вредоносные программы и странное поведение, которые не обнаруживаются другими сервисами защиты, за счет классификации всех запущенных и исполняемых процессов.

Благодаря этому решение способно обеспечивать защиту от известных вредоносных программ, а также от атак "нулевого дня", постоянных угроз повышенной сложности (Advanced Persistent Threats, APT) и целенаправленных атак.

С помощью Adaptive Defense 360 Вы всегда будете знать, что происходит с каждым Вашим файлом и процессом.

Подробные графики показывают все, что происходит в сети: хронология угроз, поток информации, как ведут себя активные процессы, как вредоносные программы проникают в систему, где это происходит, с кем, как угрозы получают доступ к информации и т.д.

Adaptive Defense 360 позволяет легко обнаруживать и закрывать уязвимости, а также предотвращать нежелательные элементы (навигационные тулбары, рекламное ПО, дополнительные компоненты и пр.).

Adaptive Defense 360: неограниченная видимость, полный контроль.

Подробнее:
pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Неограниченная видимость, полный контроль

pandasecurity.com

panda