Тренды киберпреступлений

Ущерб от киберпреступников ежегодно исчисляется сотнями миллионов долларов. Но какие сферы их деятельности наиболее прибыльны и показывают стабильный рост?

В бизнесе есть такой инструмент как BCG-матрица (название идет от названия компании, которая ее разработала — Boston Consulting Group). Это специальная диаграмма с двумя параметрами: «Доля на рынке» и «Рост», на которой располагаются различные продукты компании. Это позволяет владельцам бизнеса проанализировать, на какие сферы деятельности необходимо делать ставки, а от каких, возможно, стоит избавиться. Как это относится ко взлому? Аналитики из компании CISCO ежегодно составляют такую матрицу для рынка IT-преступлений, наглядно изображая наиболее актуальные с точки зрения прибыльности, а также скорости и масштабности распространения методы, которые используют злоумышленники. Это любопытно.

«Дойные коровы». В эту категорию попали давно известные виды нелегального бизнеса. Преступники успешно продолжают использовать scareware (фейковые антивирусы), кликфрод (автоматическое скликивание рекламы), спам с рекламой таблеток и так далее. Эта деятельность приносит много денег, но для нее не характерен активный рост.

«Звезды». это тоже очень прибыльные сферы деятельности преступников, но в отличие от «Дойных коров» они показывают еще и нешуточный рост. Сюда попали разработка/продажа веб-сплойтов, инструменты для кражи конфиденциальных данных, а также сервисы по выводу средств, позволяющие легализовать деньги, полученные незаконным путем.

«Собаки». Категория включает сферы бизнеса с низкой рентабельностью и низкими темпами роста. Денег приносят мало и не растут. Сюда попали: рассылка спама через социальные сети, старый добрый фишинг и, что может показаться удивительным после нескольких недавних прецедентов, DDoS-атаки. Но в то, что кто-то откажется от этого бизнеса, верится с трудом.

«Темные лошадки». В разделе находятся направления черного бизнеса, которые пока не получили широкого распространения, но в перспективе могут либо выстрелить (стать «звездами»), либо не выстрелить (перейти в категорию «собак»). Специалисты CISCO относят сюда атаки на VoIP и, конечно же, угрозы, связанные с мобильными устройствами.

НИКИТА КИСЛИЦИН
Главный редактор журнала «Хакер»

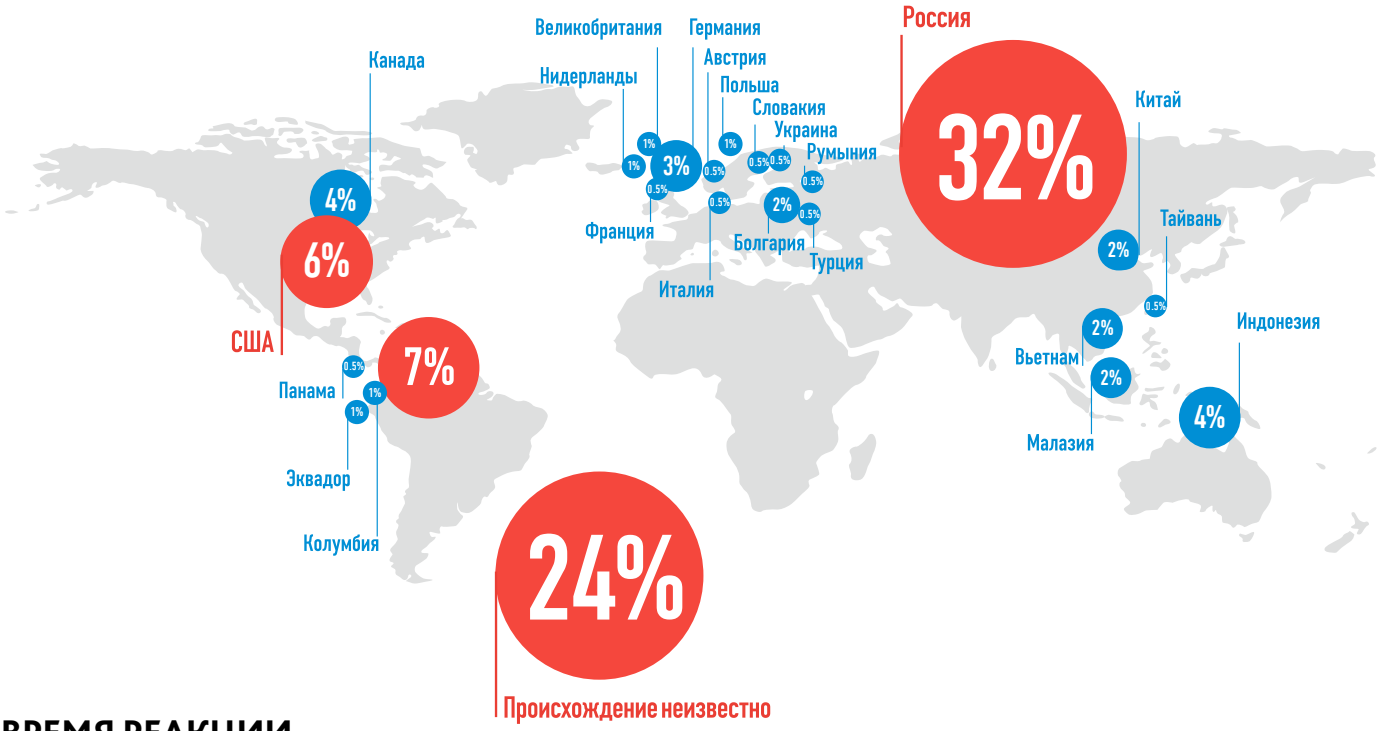
Материал предоставлен редакцией журнала «Хакер»

Безопасность платежей

Мировой рынок электронных платежей составляет больше десяти триллионов долларов в год, и эти деньги притягивают к себе огромное количество киберпреступников. Что насчет статистики по типам и источникам угроз? Каждая крупная компания, занимающаяся безопасностью электронных платежей, публикует отчеты о своей деятельности. Среди разнообразных цифр и графиков попадаются весьма занимательные данные.

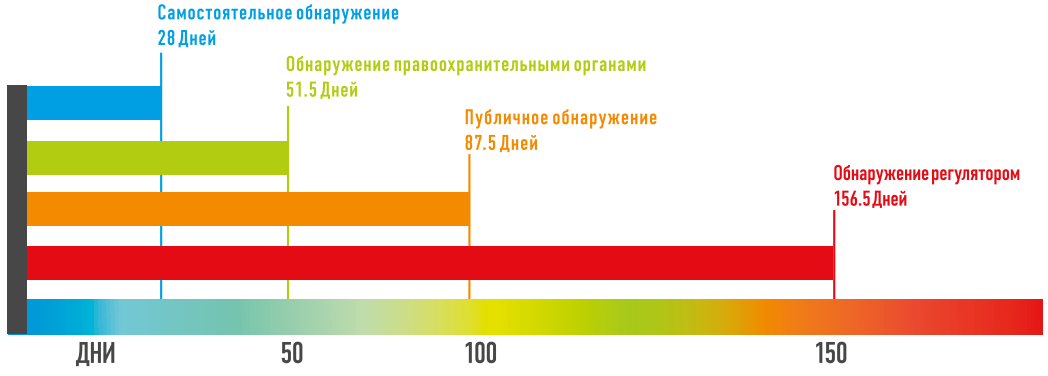
ПРОИСХОЖДЕНИЕ АТАК

Согласно отчету компании Trustwave, 32% атак на платежные системы осуществляются из России. Впрочем, сюда можно смело плюсовать и 24% атак, происхождение которых аналитикам установить не удалось: видимо, VPN + socks chain сделали свое дело, и часть российских хакеров сумела скрыть свое происхождение. В отчете компании Verisign эту проблему решили просто: 65% случаев атак они классифицировали как происходящие из «Восточной Европы».



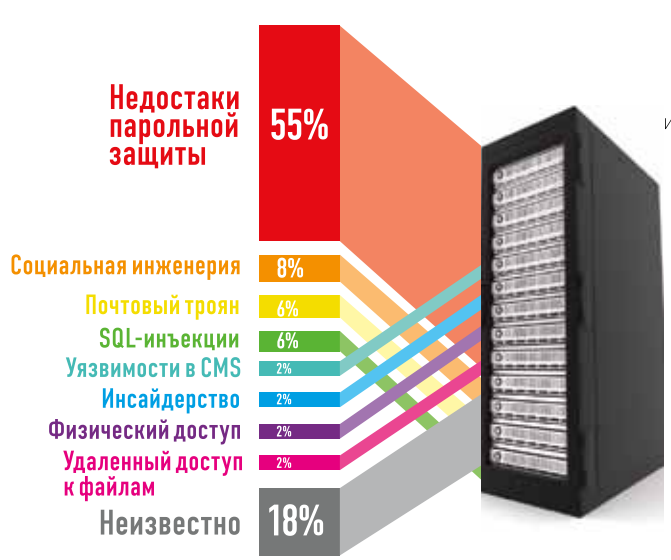
ВРЕМЯ РЕАКЦИИ

Изучая такой важный параметр как время обнаружения индидента, аналитики Trustwave пришли к неутешительным результатам. Даже компании, которые серьезно занимаются собственной безопасностью, замечают утечку в среднем лишь через месяц после того, как она произошла. Остальные компании порой не укладываются и в полгода.



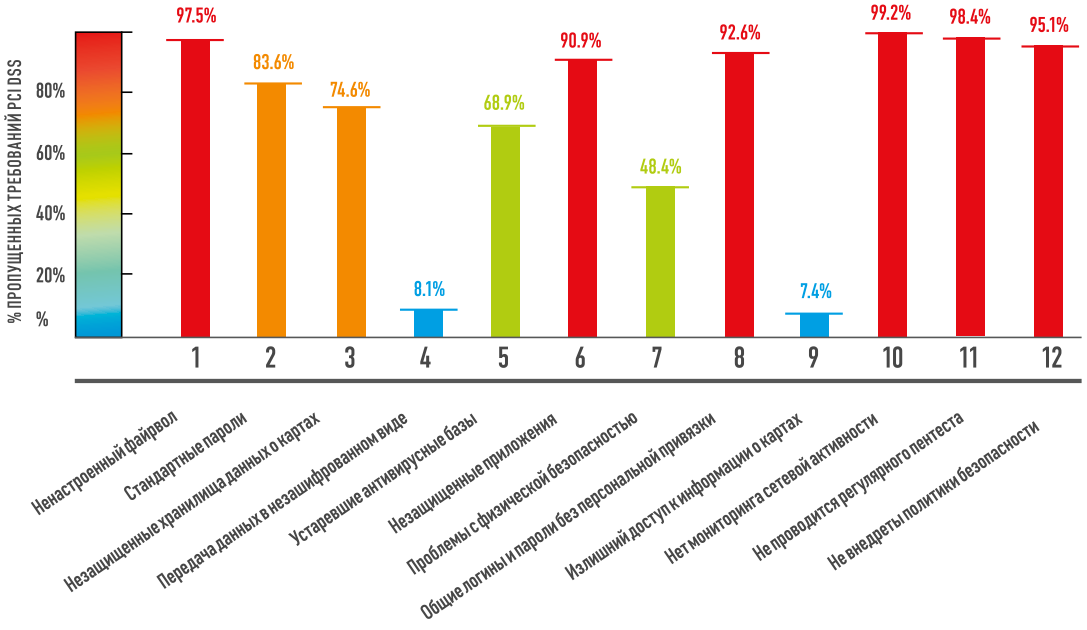
ТИПЫ УГРОЗ

Любопытно, что больше половины случаев утечек данных, по мнению Trustwave, происходят из-за удаленного доступа к приложениям, когда злоумышленникам известны логины и пароли. Verisign смотрит на классификацию угроз несколько более детально: изучив более 800 случаев утечек данных из финансовых систем, специалисты пришли к выводу, что 90% утекших записей утекли из-за разнообразных форм удаленного взлома, и только 10% записей пострадали из-за инсайдерства и физической кражи информации.



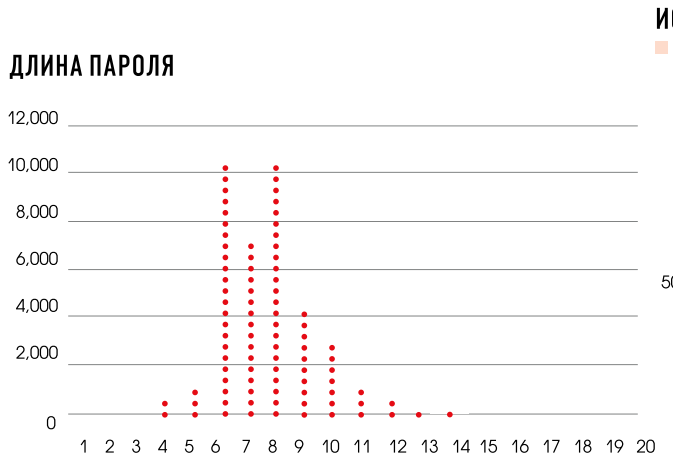
НАРУШЕНИЯ PCI DSS

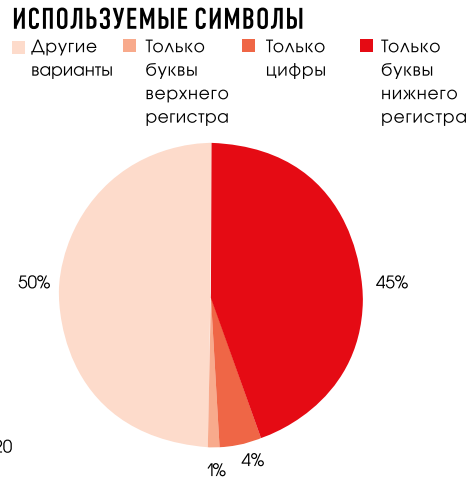
Как известно, существует специальный стандарт для обеспечения безопасности данных в платежной индустрии. Однако то обстоятельство, что любая финансовая организация проходит обязательную сертификацию по PCI DSS, никак не влияет на количество украденных денег. Аналитики утверждают, что дело не в том, что стандарт какой-то не такой, а в том, что многие компании его саботируют.



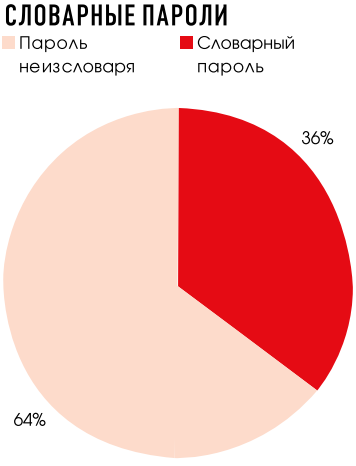
QWERTY, 12345, GFHJKM

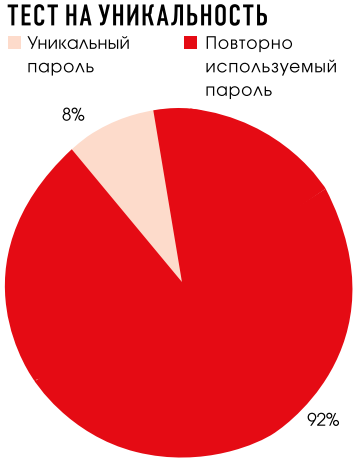
Наделавшие много шума хакерские группы Anonymous и Lulzsec своими выходками подкидывают высококачественный материал для различных исследований. Так, через torrent'ы без труда можно скачать базу пользователей Sony Pictures, из которой в открытом виде извлекается почти 40 тысяч паролей пользователей. На основе этой вполне репрезентативной выборки программист Трой Хант (www.troyhunt.com) сделал интересный анализ паролей.





Чем длиннее пароль, тем он надежнее. У 93% аккаунтов длина пароля варьируется от 6 до 10 символов (видимо, по минимальной длине действует требование сервиса), но при этом у 50% пользователей он менее 8 символов. Здравствуй, брутфорс и радужные таблицы. Сложность пароля непременно определятся символами, которые в него входят. Однако половина пассов состоит из символов одного типа, то есть либо только нижнего реестра, либо только из букв верхнего регистра, либо только из чисел.





Что может быть хуже, чем словарный пароль? Исследователь взял словарь на 1,7 миллиона слов (dazzlepod.com/site_media/txt/passwords.txt) и посмотрел, сколько паролей в него «попало». Оказалось, больше трети используемых пассов — словарные! Хороший вопрос: «Используют ли пользователи уникальные пароли для разных сервисов?». Поскольку в базу Sony Pictures включены пароли для различных сервисов, мы можем посмотреть пересечение пассов для одного и того же пользователя. Оказалось, что 92% юзеров используют один и тот же пароль. В случае с Sony Pictures все пароли хранились в открытом виде (хотя такое сложно даже представить!), но даже если бы они были захешированы, то 82% хешей непременно бы сдались под напором радужных таблиц (project-rainbowcrack.com). Это пароли из букв и цифр меньше 9 символов длиной.