Страны Персидского залива как товар на рынке преступных киберуслуг (анализ 2022–2023 годов)

Positive Technologies

ptsecurity.com

Содержание

Введение

Современный бизнес активно использует корпоративные сайты, интернет-магазины и веб-сервисы. Клиенты, регистрируясь на этих платформах, оставляют свои персональные данные, совершают покупки, а также платят банковскими картами. Кроме того, они могут хранить и передавать конфиденциальную информацию через предоставленные ресурсы.

Однако с ростом объема данных, доступных на этих платформах, возрастает и интерес со стороны киберпреступников. Злоумышленники стремятся получить доступ к ценной информации, хранимой на информационных системах компаний. Поэтому мы постоянно следим за активностью на теневых форумах и в мессенджерах, чтобы оценить потенциальную нацеленность злоумышленников на те или иные системы, а также оценить их интерес в сфере киберпреступных услуг. Это позволяет нам принимать соответствующие меры и защищать наших клиентов.

В этом исследовании мы оценим интерес хакеров на теневых площадках к странам Персидского залива, выделим наиболее популярные темы обсуждений и отрасли, а также проанализируем стоимость представленных товаров и услуг.

Резюме

- Среди исследованных сообщений больше всех выделяются сообщения, связанные с ОАЭ (46%) и Саудовской Аравией (23%).
- Из-за активности хактивистов и вымогателей самые атакуемые отрасли — госсектор и финансы.
- Данные (33%) и доступы (22%) — самые обсуждаемые темы на форумах. Треть всех данных распространяется бесплатно, что дает возможность всем пользователям теневых ресурсов использовать их для атаки.
- Стоимость большинства доступов ниже средней (от 100 $ до 1000 $), при этом почти все связаны с правами администратора.

Методика исследования

В ходе исследования мы проанализировали 252 телеграм-канала и форума в дарквебе с общим количеством пользователей 8 884 023 и общим числом сообщений 91 484 658. В выборку попали крупнейшие разноязычные площадки с разной тематической направленностью.

Для исследования рассматривался период с января 2022 года по конец июня 2023 года.

Изучались сообщения, связанные со странами Персидского залива: ОАЭ, Саудовской Аравией, Бахрейном, Оманом, Катаром, Кувейтом.

Анализировались сообщения по следующим категориям:

- Данные — персональные данные, логины и пароли для интернет-сервисов и конфиденциальная документация компаний.
- Доступы — данные для несанкционированного доступа к удаленному устройству в инфраструктуре компании.
- Спам-рассылки — инструменты и данные для массовой рассылки СМС-сообщений, электронных писем и для телефонных звонков.
- Обналичивание средств — предоставление услуг по обналичиванию средств.
- Кардинг — информация о банковских картах.
- DDoS — инструментарий для DDoS-атак, призывы к выполнению DDoS-атак.
- Документы — услуги по изготовлению фальшивых документов.
- Мошенничество — поиск людей и схем для мошенничества.
- Перенаправление трафика — переход на фишинговые сайты и скачивание вредоносных файлов.
- Фишинг — разработка, покупка или продажа сайтов для получения доступ к конфиденциальным данным пользователя.

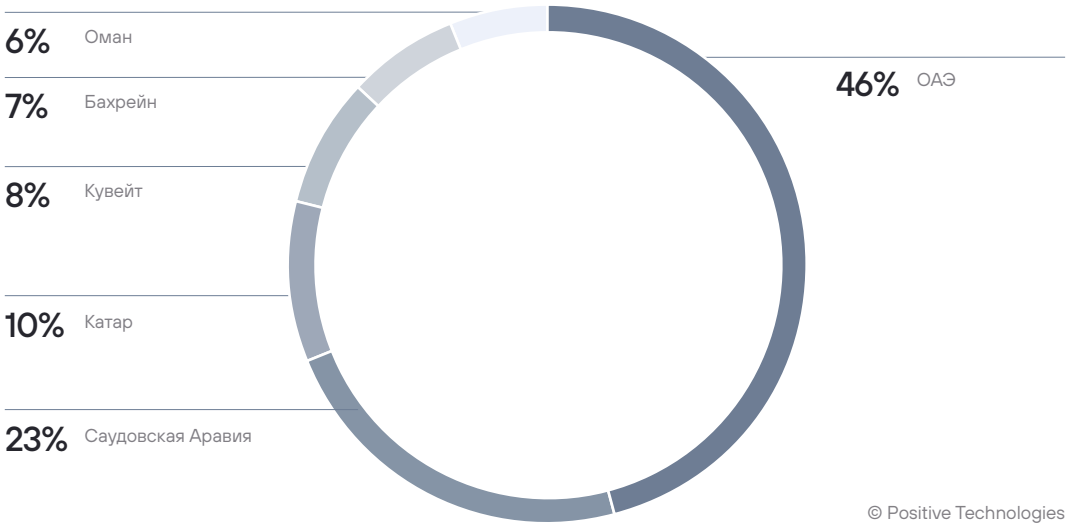
Далее в исследовании информация без уточнения конкретной страны относится к данным по региону Персидского залива.

На что нацелены покупатели в дарквебе: курс на Ближний Восток

Наибольшей популярностью в публикуемых сообщениях и объявлениях пользуются ОАЭ и Саудовская Аравия. Эти страны ассоциируются с нефтедобывающей промышленностью и финансовым достатком, что и привлекает злоумышленников из разных сфер.

Рисунок 1. Продажа доступа к компании, связанной с нефтегазовой промышленностью

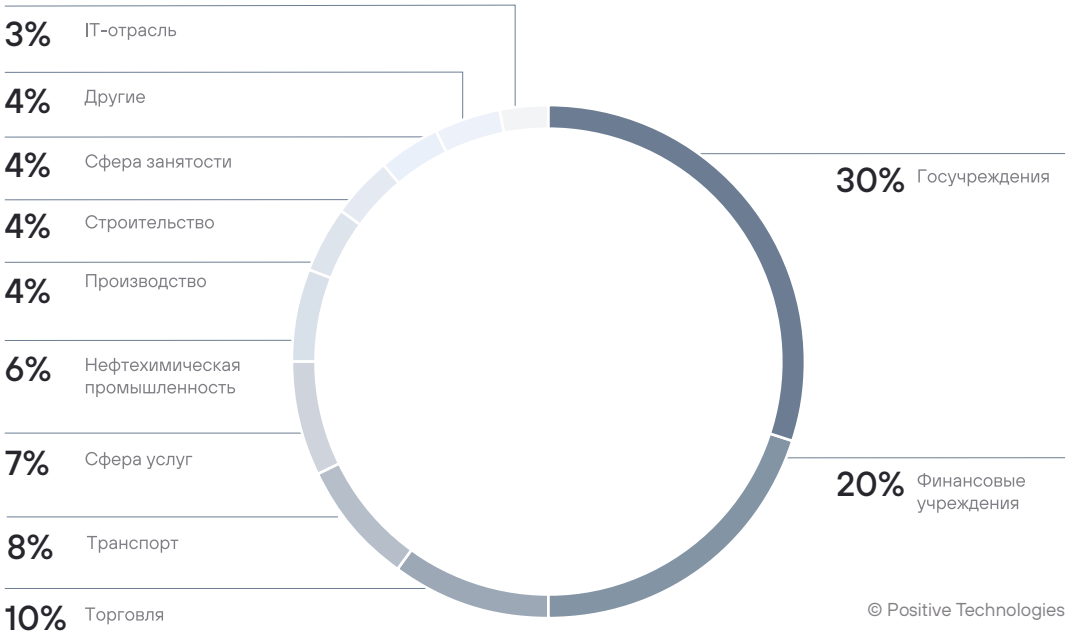
Рисунок 2. Доля сообщений на форумах по странам



Наиболее распространенные сообщения в дарквебе, связанные с исследуемым регионом, относятся к государственным и финансовым учреждениям. Хактивисты атакуют госучреждения по политическим мотивам. Разного рода злоумышленники, в том числе группы вымогателей, атакуют финансовые учреждения. По нашим данным, каждая вторая атака на организации в мире проходит с использованием шифровальщиков.

Рисунок 3. Объявление о покупке базы данных или доступа к банку

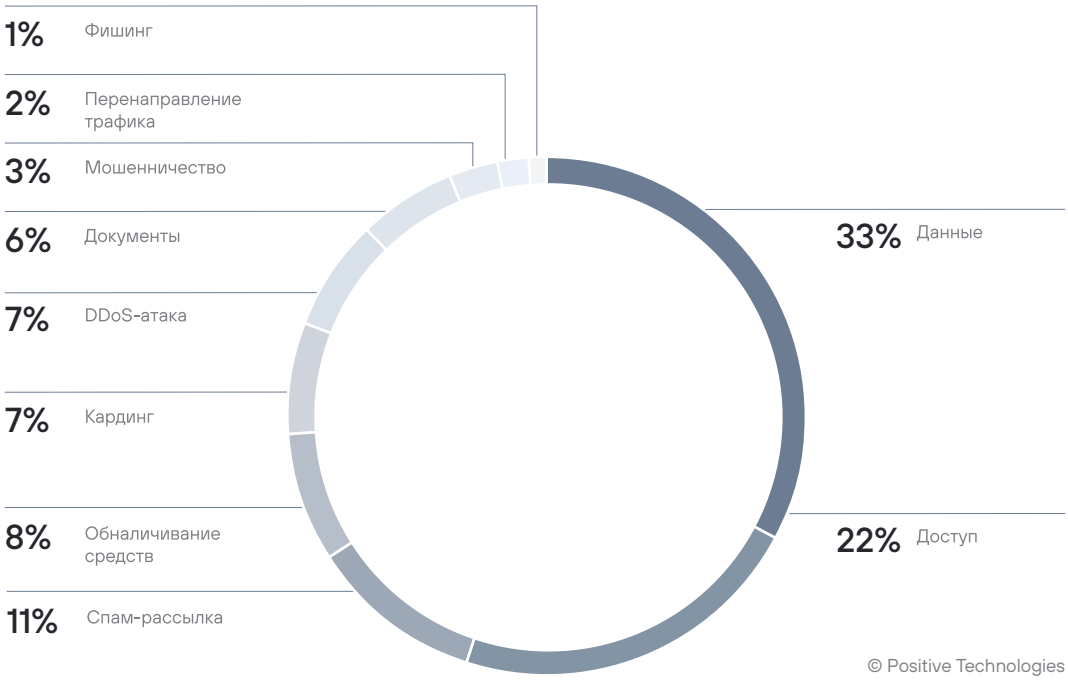
Рисунок 4. Доля сообщений на форумах по отраслям



Прослеживается значительное преобладание интереса к таким категориям, как данные и доступы.

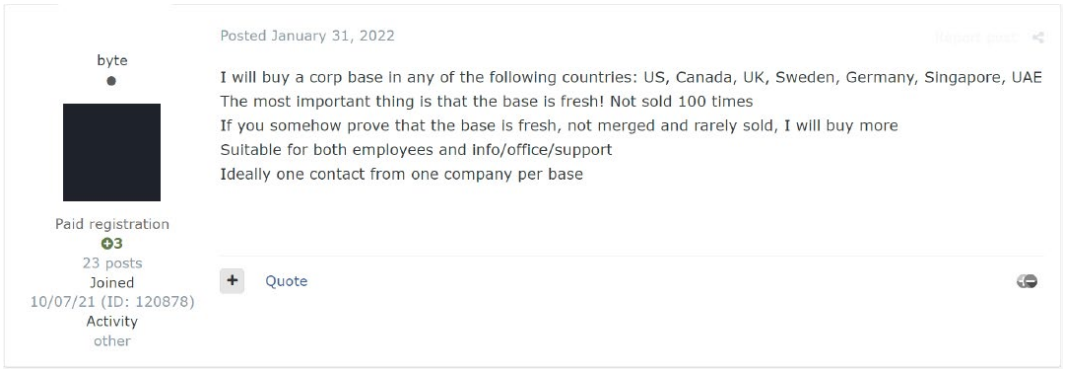
При анализе сообщений по категориям в целом (рисунок 5) и для каждой страны (приложение 2) видно, что данные и доступы всегда входят в топ-3 списков.

Рисунок 5. Доля сообщений по категориям



Треть всех объявлений занимают данные: базы данных организаций, данные аккаунтов, в том числе банковских. В результате атак на веб-ресурсы компаний хакеры получают информацию, которая может содержать персональные и учетные данные сотрудников и клиентов. Они могут быть использованы в дальнейшем другими злоумышленниками для атак на организации (например, для фишинга). Согласно исследованию, в 2022 году социальная инженерия применялась в 43% случаях успешных атак в мире.

Рисунок 6. Объявление о покупке базы данных сотрудников



Из-за деятельности хактивистов и вымогателей 31% всех данных распространяется бесплатно, так как цель хактивистов не связана с финансовой выгодой, а вымогатели могут опубликовать данные бесплатно в случае отказа жертвы платить выкуп. Это повышает вероятность использования таких данных другими злоумышленниками для атак на компанию или ее клиентов.

Рисунок 7. Сообщение о бесплатной раздаче базы данных компании из ОАЭ

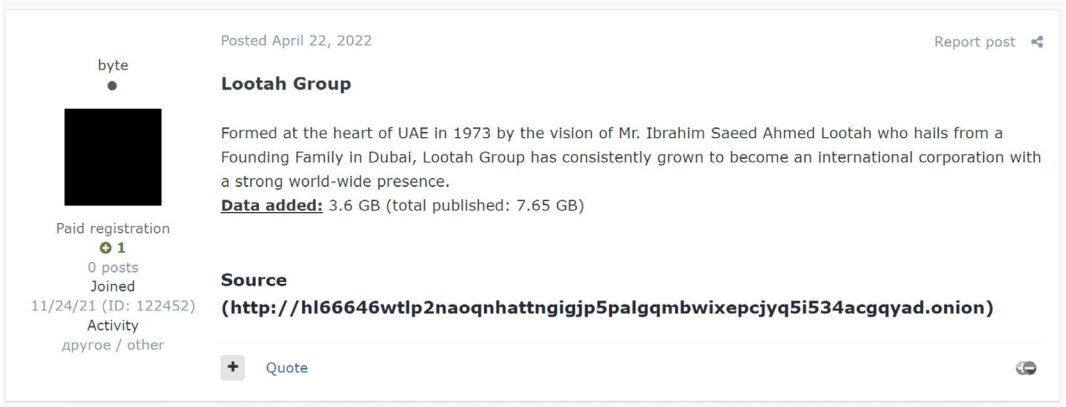
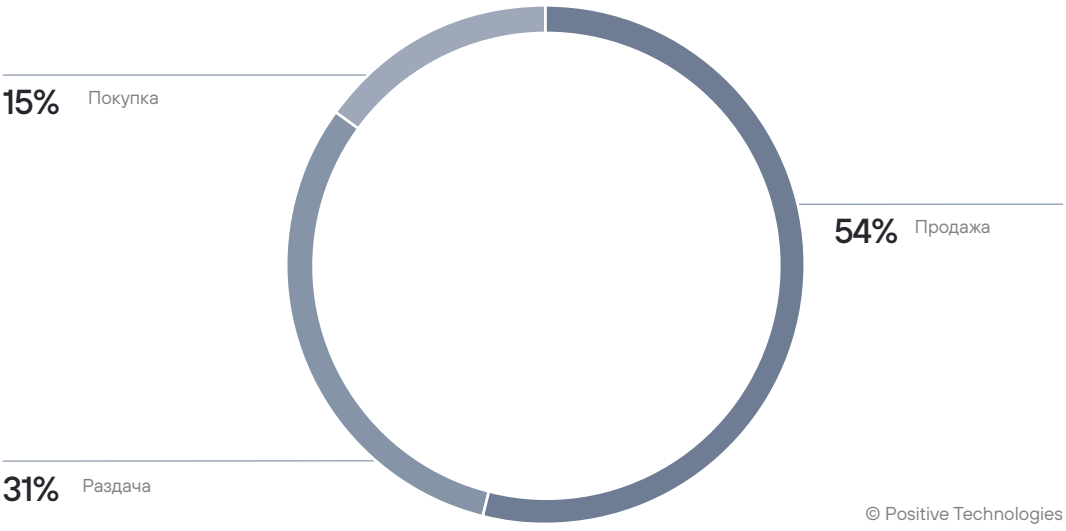
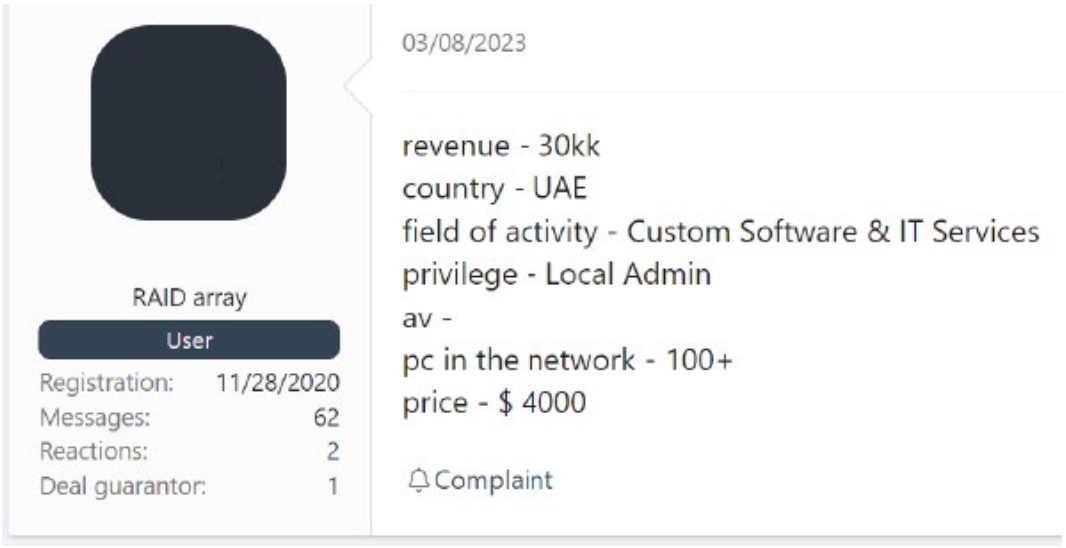


Рисунок 8. Доля сообщений по типу для категории «Данные»



Продажа доступов (рисунок 5) к инфраструктуре организаций из разных сфер составляет 22% от всех объявлений. Доступы и данные связаны между собой. Злоумышленники используют приобретенный на форумах доступ для внедрения в инфраструктуру компании и дальнейшего развития атаки внутри сети организации. В результате атаки злоумышленники могут получить данные, которые затем продаются на форумах или распространяются бесплатно.

Рисунок 9. Объявление о продаже доступа



В каждом третьем объявлении о продаже доступов предоставлялась возможность подключения к сети компании при помощи VPN или RDP. Продавцы могут их получить, используя стилеры. Согласно нашему исследованию число фишинговых писем с вредоносными вложениями — стилерами, похищающими учетные данные, растет.

Рисунок 10. Объявление о продаже доступа

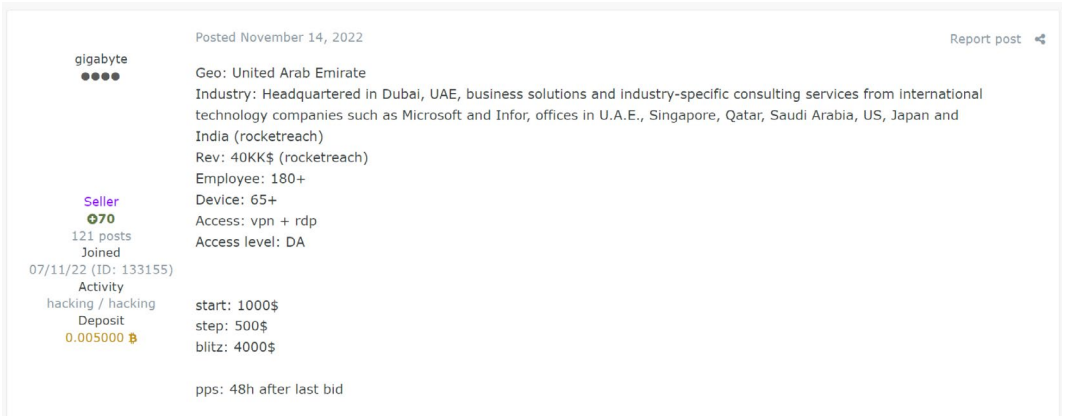
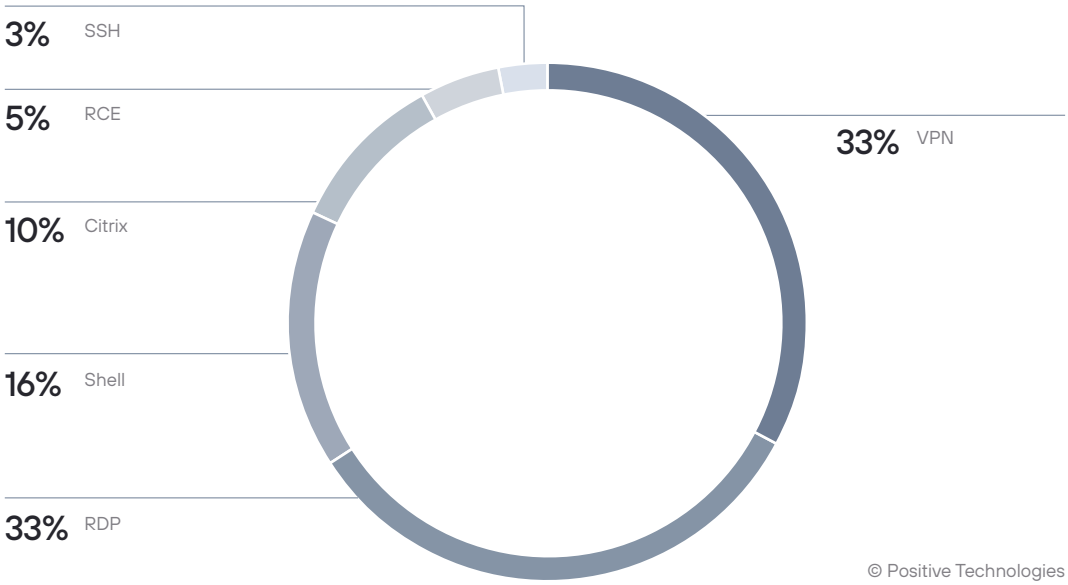


Рисунок 11. Доля сообщений по типу доступа

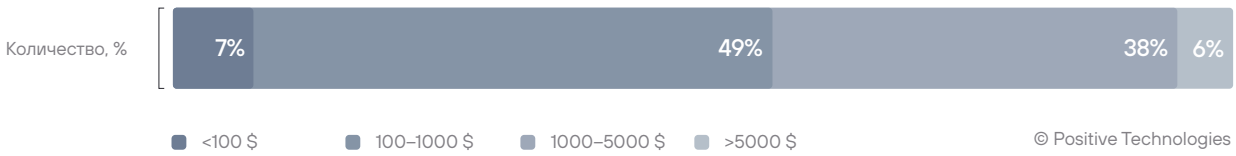


© Positive Technologies

В 16% сообщений, связанных с категорией «Доступы», обсуждалось использование подключения при помощи Shell — загруженного вредоносного ПО, — через которое в дальнейшем выполняется подключение к ресурсам компании. Подключение через Citrix (ПО, используемое как удаленный рабочий стол, с помощью которого злоумышленник получает прямой доступ к ресурсам) — в 10% сообщений. В единичных случаях упоминали протокол SSH (Secure Shell) для подключения к внутренним ресурсам компании, а также продажу доступов к удаленному выполнению кода (RCE) в сети компании.

Стоимость доступов — от 35 $ до 40 000 $. При этом цена на большую часть доступов (49%) находится в пределах от 100 $ до 1000 $, что является ниже среднего.

Рисунок 12. Распределение стоимости доступов



© Positive Technologies

Отметим, что 90% всех доступов связаны с правами администратора. Учитывая этот фактор, а также стоимость доступа, даже неопытные злоумышленники с небольшим бюджетом могут произвести успешную атаку на компанию. Однако есть и дорогостоящие доступы к крупным компаниям с большим оборотом. Такие доступы могут использоваться хакерами с более высоким уровнем подготовки для проведения сложных атак.

Рисунок 13. Объявление о продаже доступа

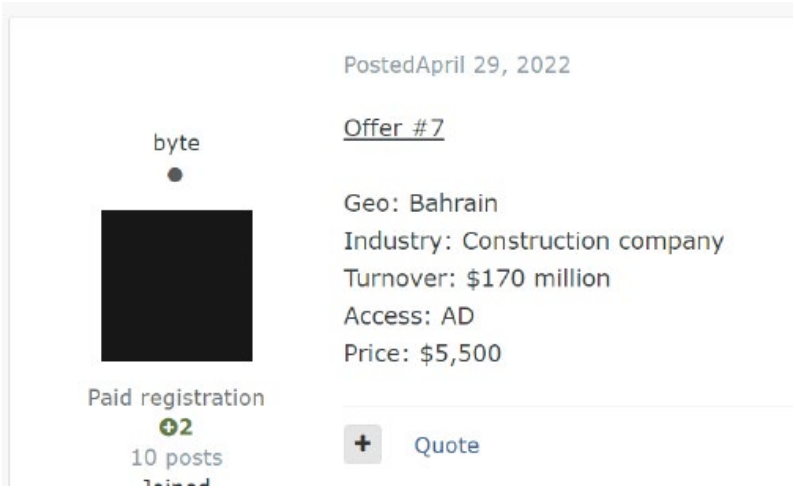
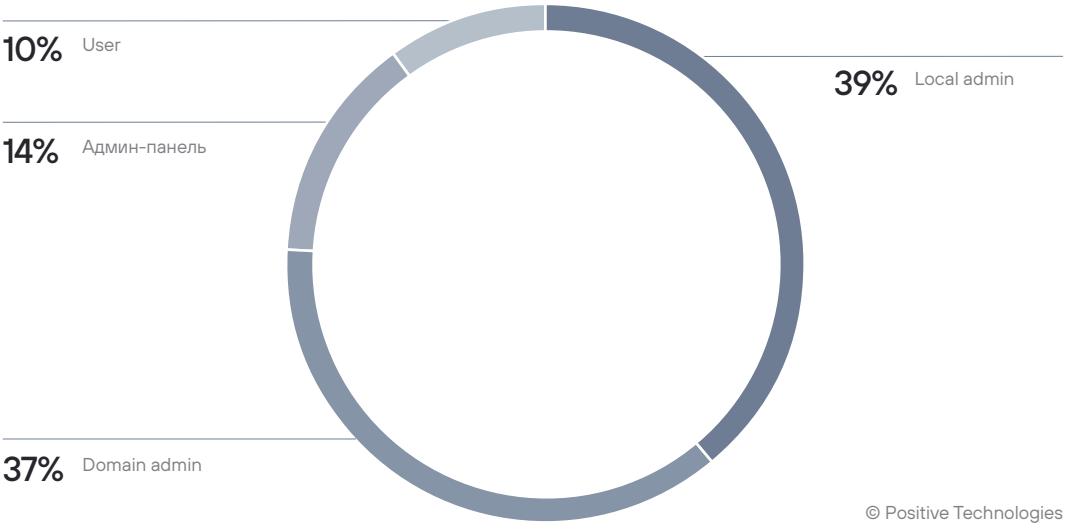


Рисунок 14.Привилегии доступов, представленных в дарквебе



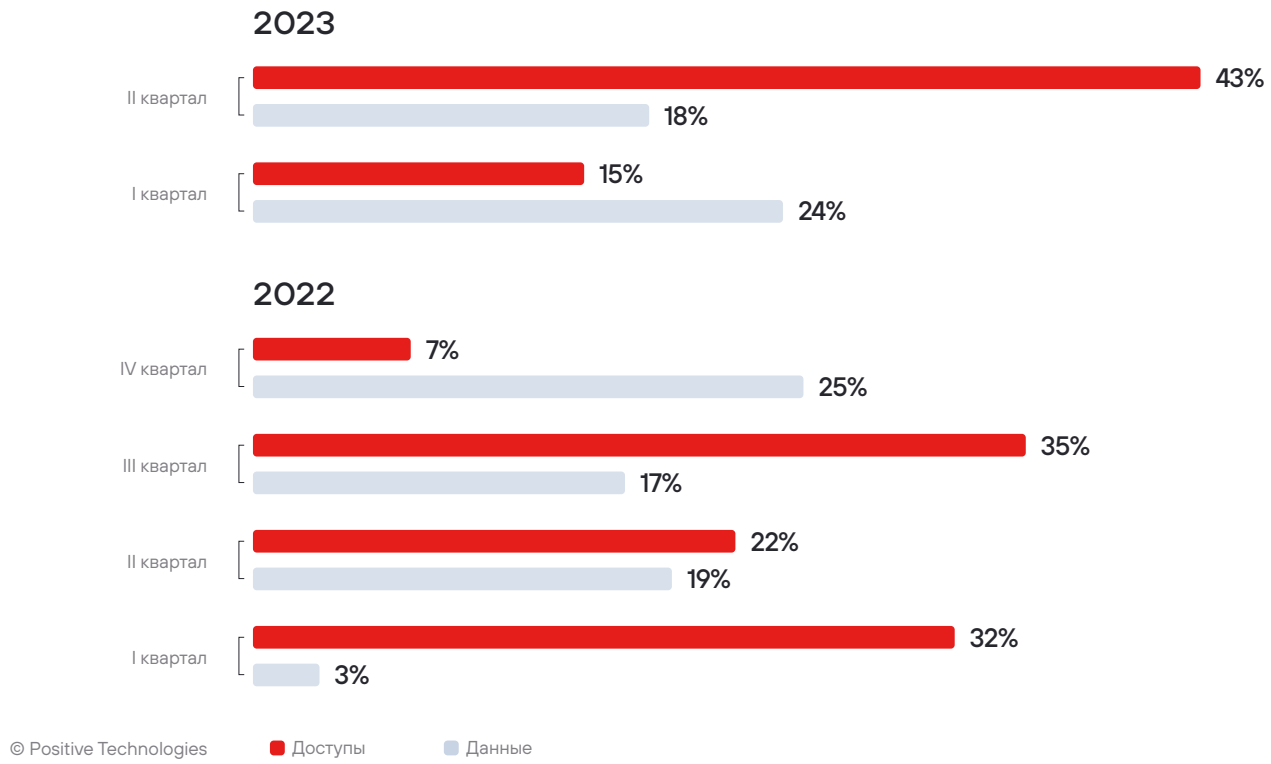
На рисунке 14 видно, что доступы с пользовательскими правами упоминались лишь в 10% сообщений. Как правило, такой вид доступа может заинтересовать продвинутого злоумышленника, способного самостоятельно доработать его для атаки. В остальных случаях сообщения относились к привилегированным видам доступа — локального администратора, администратора домена и админ-панели[1].

[1] Администратор домена имеет неограниченный доступ к домену — к компьютерам, серверам, которые входят в домен. Панель администратора, или админ-панель — это набор функций для выполнения определенных задач на сайте (например, для создания и редактирования контента, добавления настраиваемых полей к контенту, управления пользователями).

В конце 2022 года — начале 2023 года количество сообщений в категории «Доступы» достигло своего максимума.

В категории «Данные» в конце 2022 года было мало сообщений, но в начале 2023 года их количество значительно возросло, что может говорить о получении данных в результате атак с помощью продаваемых доступов. На первом этапе злоумышленники активно скупали доступы, после чего приступили к атакам, в результате которых были получены данные, представленные в дарквебе.

Рисунок 15. Количество сообщений для данных и доступов в 2022 и 2023 годах



Выводы

Наличие большого количества сообщений, связанных с данными и доступами, а также их низкая стоимость, облегчают для злоумышленников процесс получения первичного доступа к компании. Для новичков, не имеющих достаточных навыков для преодоления периметра или больших финансовых средств, это шанс провести успешную атаку. Опытные же хакеры могут не тратить время на поиск уязвимостей на периметре компании, а приобрести готовый доступ и развивать атаку внутри организации. Все это влечет за собой рост числа успешных атак на компании, поэтому стоит выстраивать защиту от кибератак с учетом всех возможных угроз и сценариев развития атаки злоумышленниками, применяя при этом современные средства защиты, такие как:

- Системы класса SIEM (security information and event management) — для сбора и анализа информации о событиях безопасности из различных источников. Совместное использование систем SIEM и XDR обеспечивает централизованное обнаружение угроз и реагирование на них.
- Решения класса NTA (network traffic analysis) — для анализа сетевого трафика, использование которых позволяет повысить эффективность защиты путем обнаружения атаки на ранних стадиях.
- Средства класса WAF (web application firewall) — для минимизации риска утечки информации путем блокировки атак на веб-приложения.

Приложение 1.

Распределение отраслей по странам

Рисунок 1. Доля сообщений по отраслям в ОАЭ

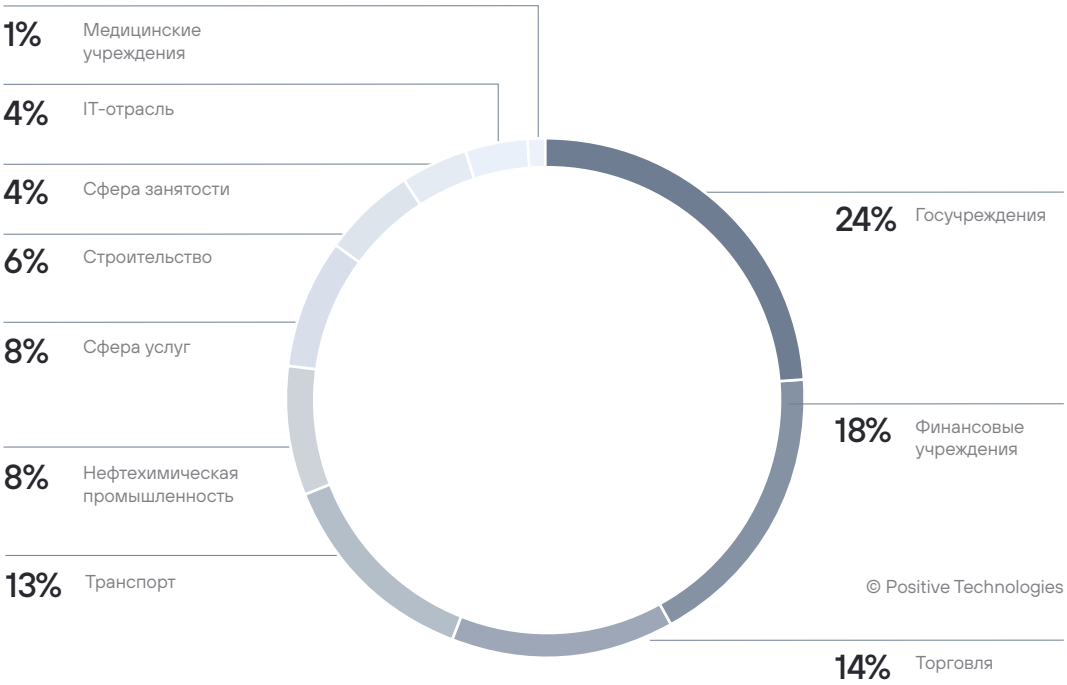


Рисунок 2. Доля сообщений по отраслям в Саудовской Аравии

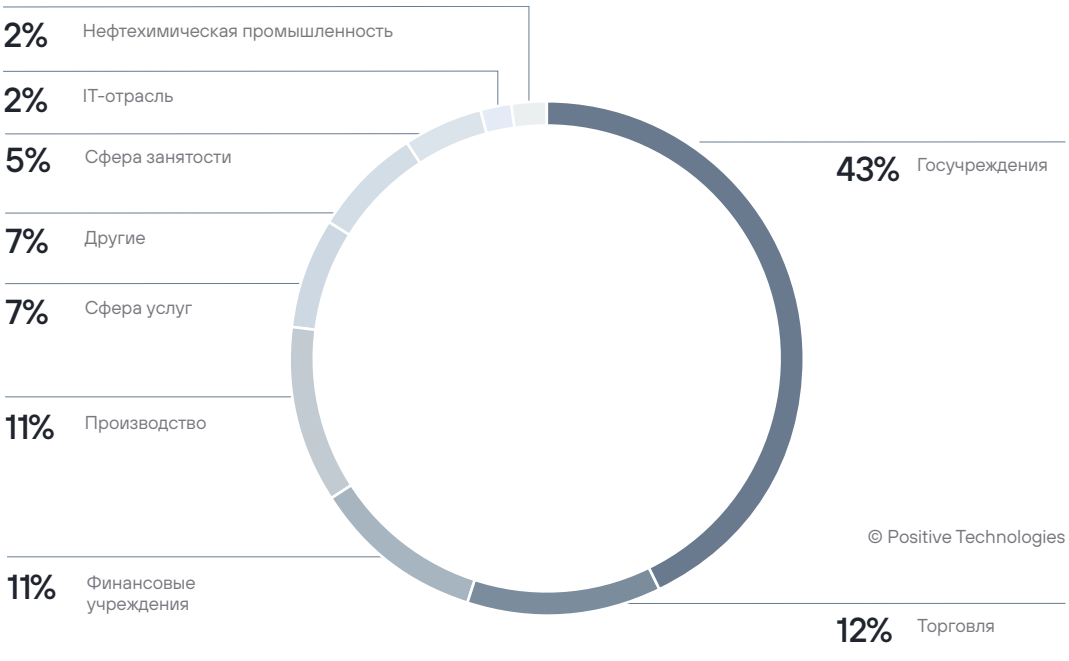


Рисунок 3. Доля сообщений по отраслям в Катаре

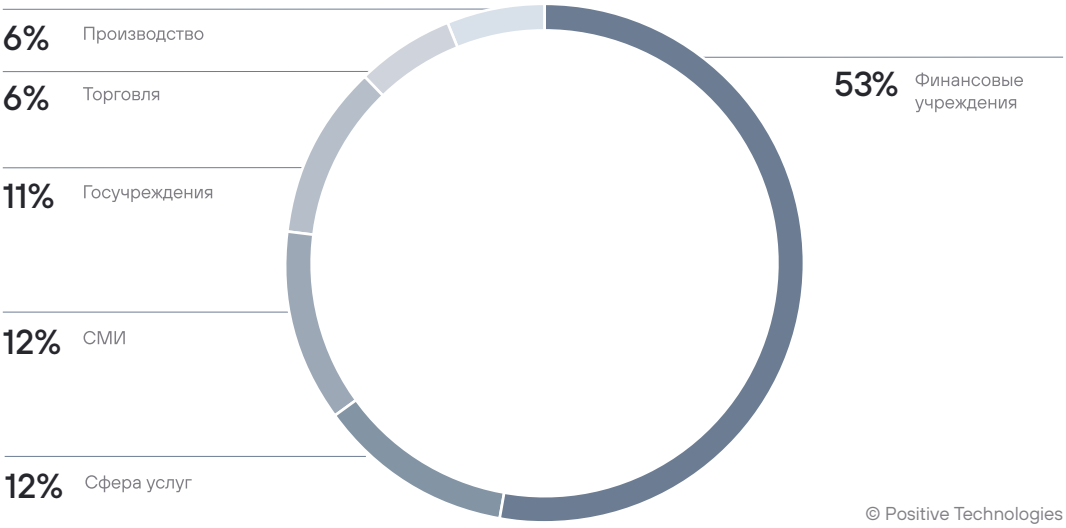


Рисунок 4. Доля сообщений по отраслям в Кувейте

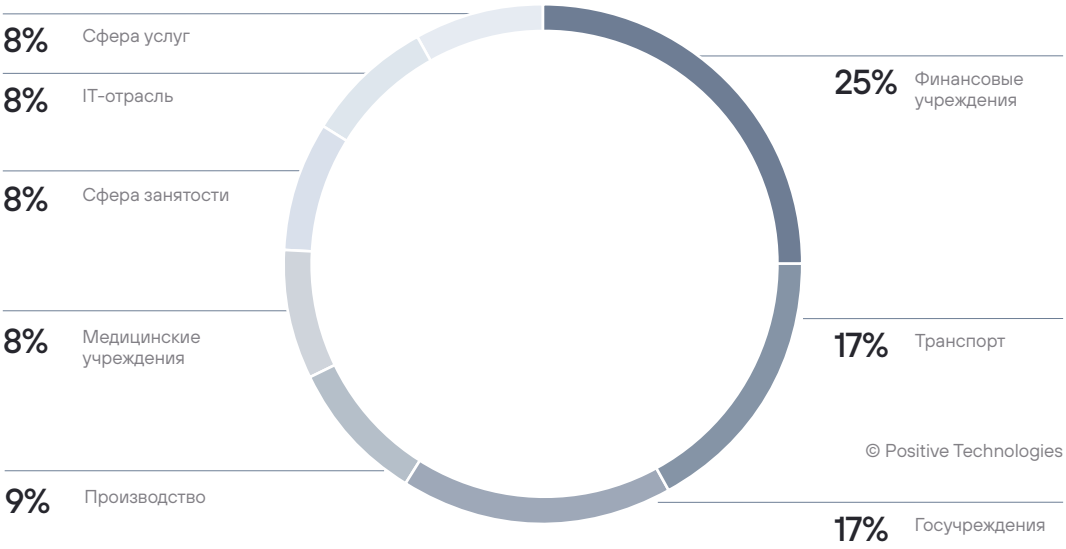


Рисунок 5. Доля сообщений по отраслям в Бахрейне

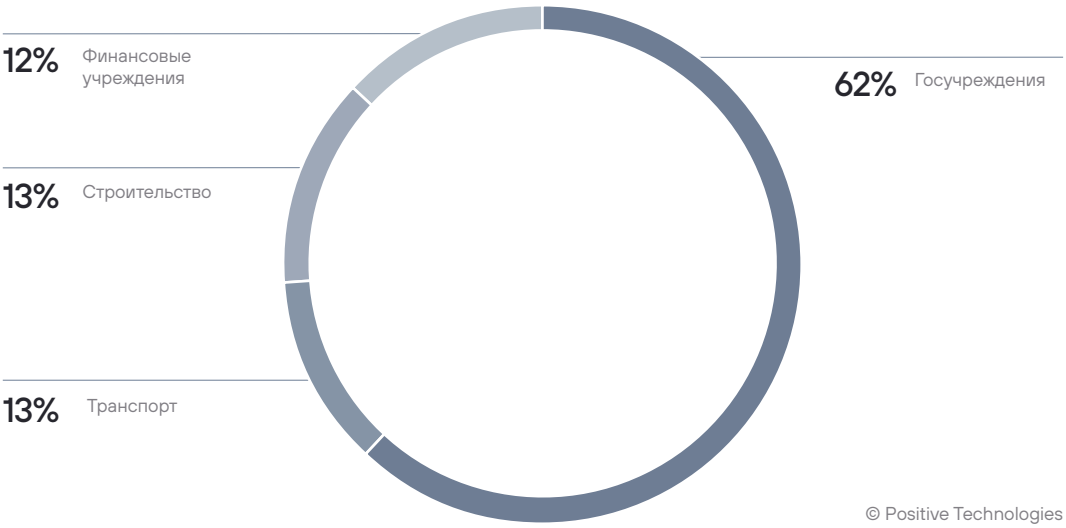
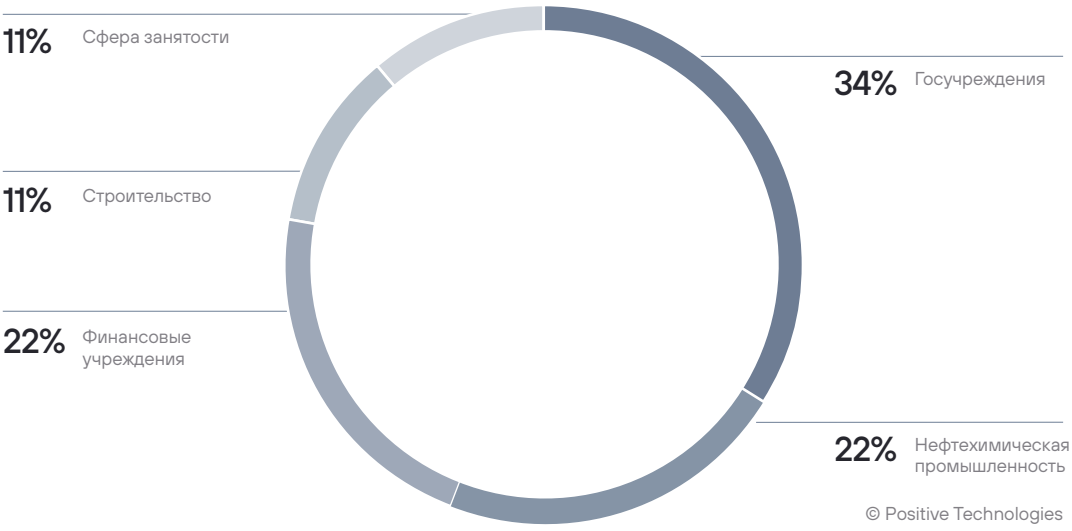


Рисунок 6. Доля сообщений по отраслям в Омане



Приложение 2.

Распределение категорий (тем) по странам

Рисунок 1. Доля сообщений по категориям для ОАЭ

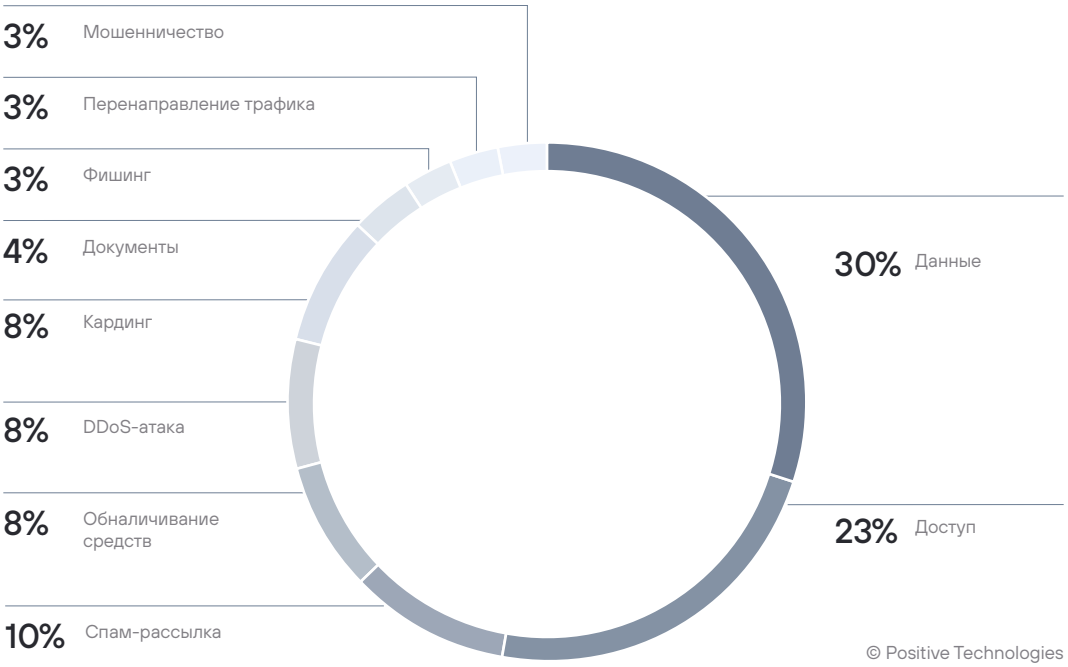


Рисунок 2. Доля сообщений по категориям для Саудовской Аравии

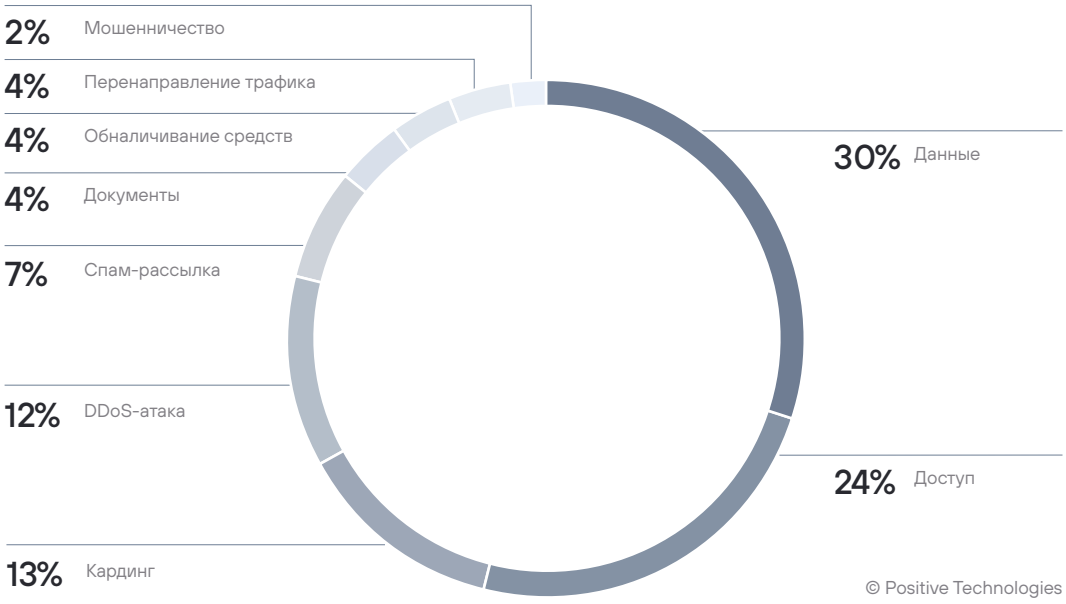


Рисунок 3. Доля сообщений по категориям для Катара

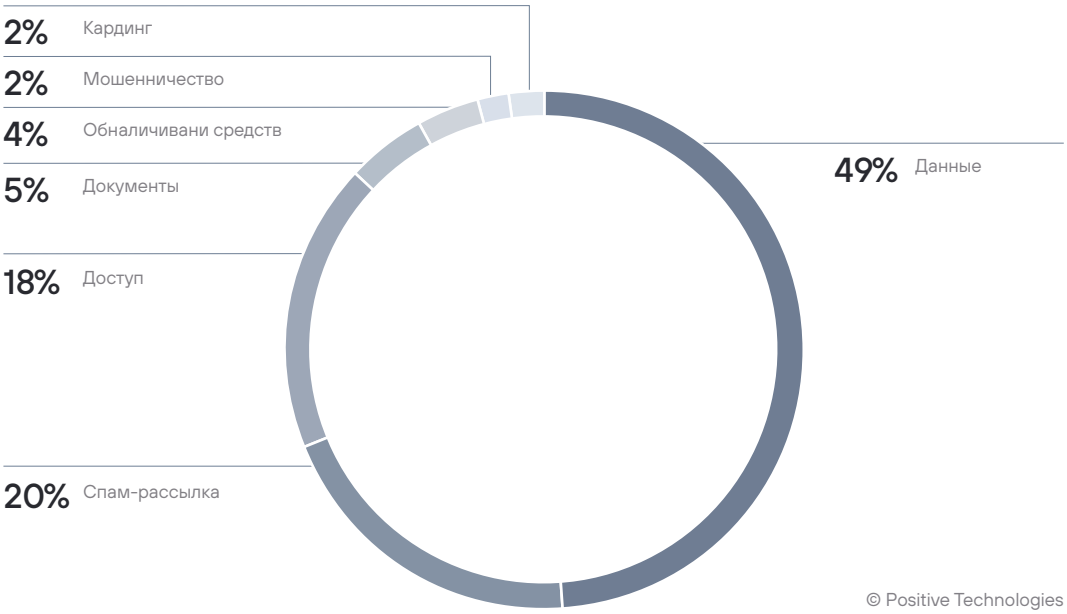


Рисунок 4. Доля сообщений по категориям для Кувейта

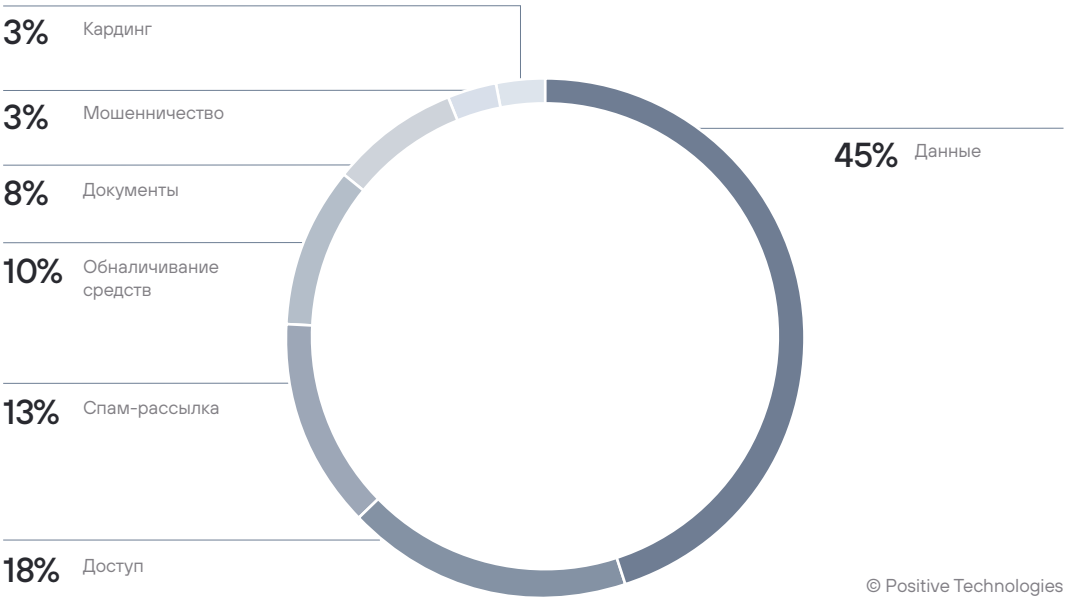


Рисунок 5. Доля сообщений по категориям для Бахрейна

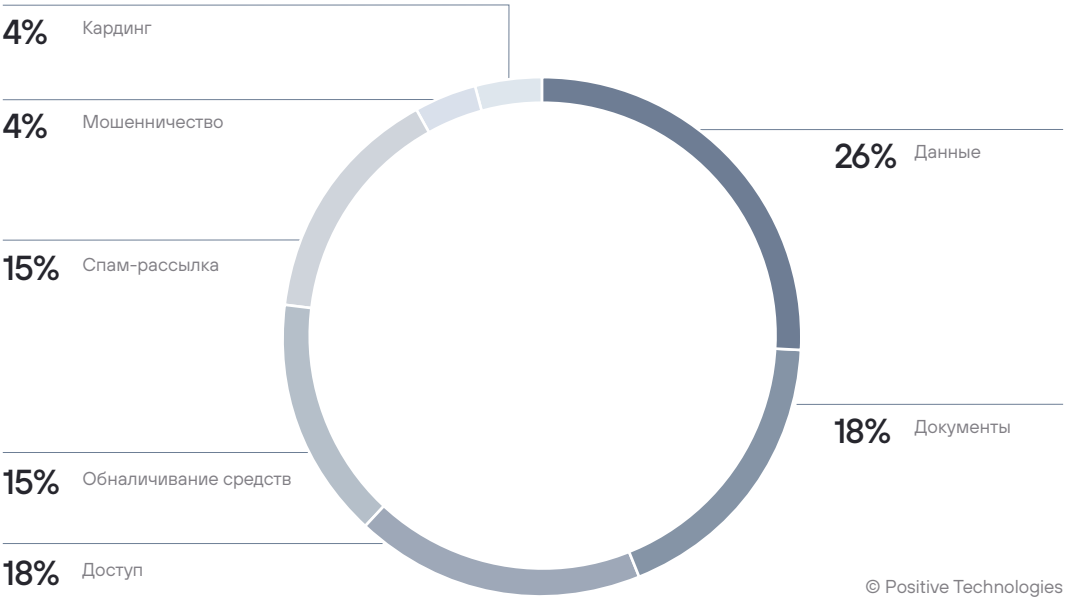
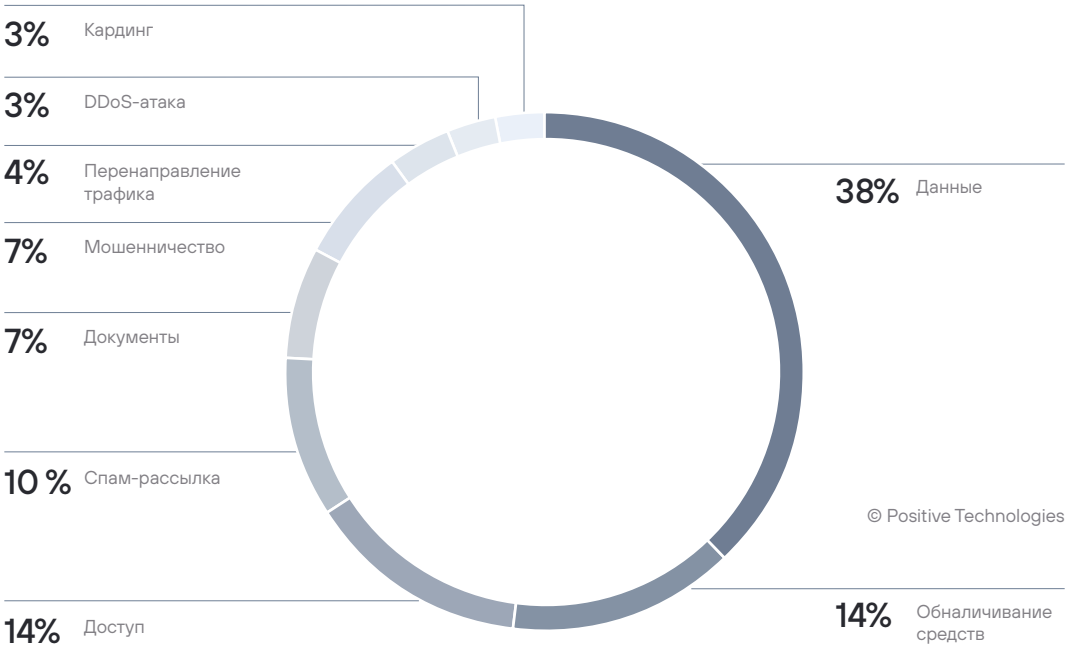


Рисунок 6. Доля сообщений по категориям для Омана



ptsecurity.com
pr@ptsecurity.com