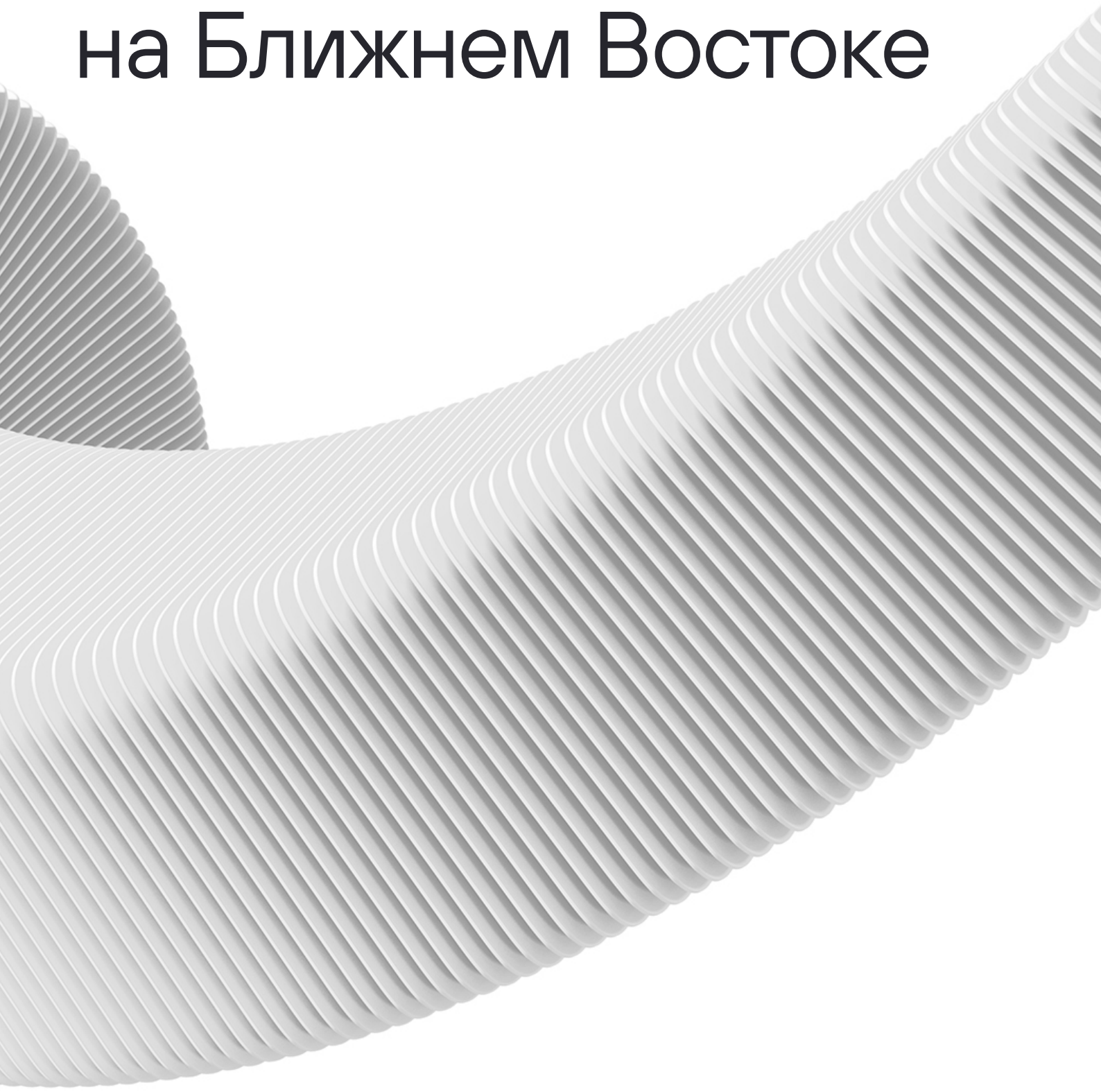
Как атакуют частных лиц на Ближнем Востоке



Positive Technologies

ptsecurity.com

Содержание

Введение

Киберпространство Ближнего Востока отличается интенсивностью и разнообразием атак злоумышленников, в фокус внимания которых попадают не только компании, но и обычные люди. В исследовании мы изучили наиболее распространенные методы атак, направленных на частных лиц стран Ближневосточного региона. Как киберпреступники наживаются на событиях масштаба чемпионата мира по футболу? Как не попасть на удочку мошенников, выбирая VPN-решение? «Котята» и «шакалы», «ксеноморфы» и «пешки» — кого еще лучше не встречать среди кибербарханов Ближнего Востока? В этой статье мы расскажем об актуальных для региона угрозах.

Уникальный киберландшафт Ближнего Востока формируют несколько факторов. В первую очередь отметим колоссальную роль стран Персидского залива во всемирной экономике: к примеру, только через Ормузский пролив проходит пятая часть всех морских поставок нефти. В последние годы в регионе наблюдается стремительный технологический рост. Уже к 2020 году ОАЭ, Катар, Бахрейн и Кувейт возглавили рейтинг стран по наибольшему проценту интернет-пользователей. Свой отпечаток накладывает и геополитическая обстановка. Кроме того, разнообразие в методах атак обусловлено и географическим положением: на Ближнем Востоке действуют не только местные злоумышленники, но и европейские и азиатские киберпреступники. В таких условиях атакам злоумышленников подвергаются и объекты критически значимой инфраструктуры, и различные организации, и обычные пользователи.

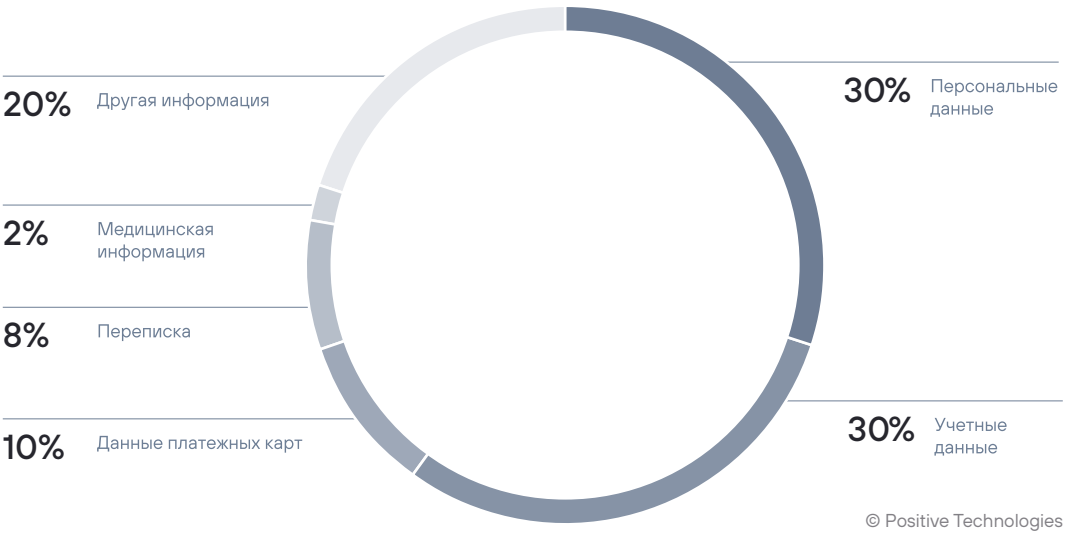
Кто и зачем атакует частных лиц на Ближнем Востоке

Согласно исследованию актуальных киберугроз, в период с начала 2022 года по конец I квартала 2023 года 20% успешных кибератак, которые привели к негативным последствиям, на Ближнем Востоке было направлено на частных лиц. Злоумышленники стремились похитить у пользователей денежные средства и конфиденциальные данные для перепродажи на теневых ресурсах, шантажа и последующих атак.

На активности киберпреступников отразились и общественно-политический ландшафт. В 39% успешных атак на частных лиц злоумышленники преследовали идеологические цели. Основной мотив хактивистов не получить финансовую выгоду, а достичь политических целей, сделать громкое заявление на социальную или религиозную тему. Такие злоумышленники активно ведут аккаунты в социальных сетях, через которые распространяют украденные конфиденциальные данные, включая личные.

По нашим данным, в Ближневосточном регионе с утечкой конфиденциальной информации частные лица столкнулись в 63% успешных атак. Большую часть украденной информации составили персональные (30%) и учетные данные (30%). Также интерес киберпреступников вызывали данные платежных карт (10%), переписка пользователей (8%).

Рисунок 1. Типы украденных данных в атаках на частных лиц



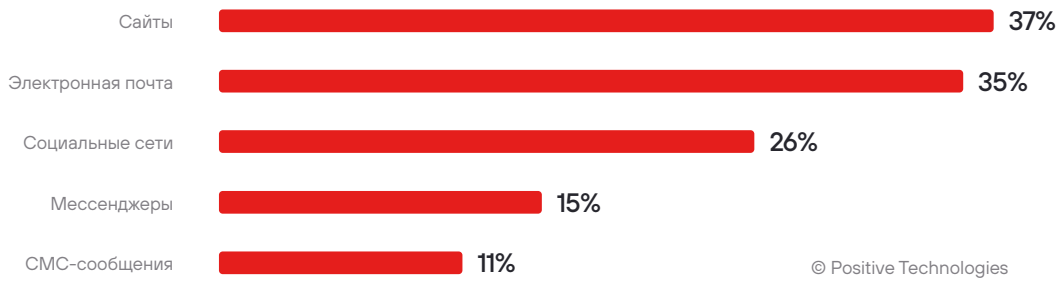
Социальная инженерия: способы обмана пользователей

В подавляющем большинстве (96%) успешных атак на частных лиц в странах Ближнего Востока использовались приемы социальной инженерии; чаще всего атаки были массовыми: злоумышленники пытались охватить максимальное число жертв. Как правило, мошенники обещали некую выгоду и провоцировали жертву на необдуманную установку вредоносного приложения, переход по вредоносной ссылке или перевод средств на счет злоумышленников.

Чаще всего в успешных атаках злоумышленники использовали поддельные сайты и электронные письма, фальшивые аккаунты в социальных сетях.

В каждой пятой (20%) фишинговой кампании применялся комплексный подход: злоумышленники эксплуатировали сразу несколько каналов социальной инженерии в одной атаке. Преступники вели жертву по цепочке из нескольких шагов до заражения устройства и потери данных. Например, пользователей могли завлекать с помощью аккаунтов в социальных сетях, содержащих ссылку на канал в мессенджере, из которого жертва устанавливала вредоносное приложение.

Рисунок 2. Используемые злоумышленниками каналы социальной инженерии



При массовой атаке киберпреступники стремятся охватить как можно больше пользователей. Для этого активно используют заметные инфоповоды, новости о громких мировых и региональных событиях. Злоумышленники часто использовали на фишинговых сайтах защищенный протокол HTTPS с действительными SSL-сертификатами для лучшей маскировки мошеннической схемы.

Рассмотрим несколько тем, которые киберпреступники активно эксплуатировали в успешных атаках на пользователей из стран Ближнего Востока.

Службы доставки

В ОАЭ с 2020 года и по нынешнее время злоумышленники маскируют сообщения под уведомления от известных служб доставки. В период пандемии COVID-19 онлайн-шоппинг обрел огромную популярность, увеличивая и рынок доставки заказанных товаров до покупателя. Злоумышленники пользуются этим и проводят массовые фишинговые кампании: создают поддельные сайты-однодневки, а также рассылают СМС-сообщения с требованиями срочно оплатить доставку посылок. У попавшихся в ловушку жертв преступники похищали денежные средства и данные банковских карт. Стоит отметить, что в своих атаках киберпреступники использовали фишинговые комплекты — наборы скриптов, которые позволяют быстро создать сайт, имитирующий известный бренд доставки.

Мы советуем всегда сохранять бдительность в сети. Требование срочно оплатить услугу или товар — это, скорее всего, ловушка. Для отслеживания своих посылок используйте официальные сайты компаний. Если не уверены в надежности отправителя, не стоит переходить по ссылке из сообщения: проверьте информацию на официальном ресурсе самостоятельно. Будьте внимательны с сокращенными URL-ссылками, поскольку злоумышленники часто используют их для маскировки фишингового сайта. Не совершайте поспешных эмоциональных действий, возьмите паузу на несколько минут: за это время вы успеете вспомнить, что неоплаченных доставок у вас нет.

Масштабные события

Киберпреступники находят способы заработка в период проведения крупных мероприятий. Во время чемпионата мира по футболу в Катаре в 2022 году мошенники создавали фишинговые сайты, приложения и аккаунты в социальных сетях, маскирующиеся под официальные ресурсы, которые предлагали приобрести билеты на матчи и атрибутику для болельщиков. Наиболее активно злоумышленники действовали на Ближнем Востоке, пользуясь географической близостью к проводящей чемпионат стране. Они создавали фальшивые аккаунты в соцсетях и рассылали вакансии, предлагающие работу на стадионах. От пользователя требовалось заполнить подробную форму с якобы необходимыми для трудоустройства персональными данными, которые тут же становились известны злоумышленникам.

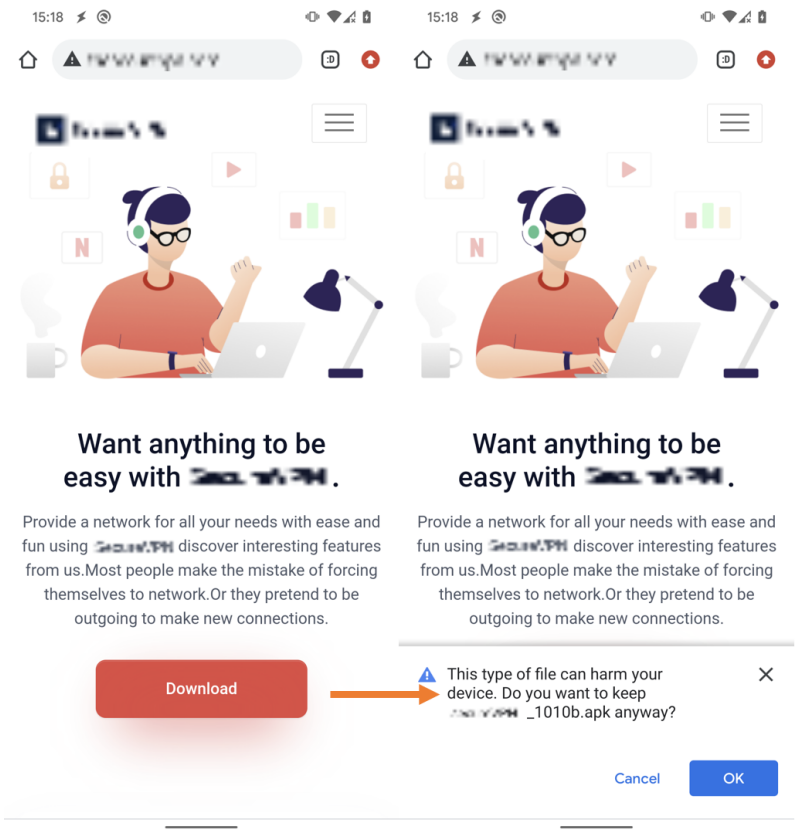
При покупке товаров и услуг, например билетов на мероприятия, старайтесь уточнить, действительно ли сайт является официальным. Во время крупных событий перед покупкой атрибутики и билетов проверяйте, входит ли продавец в списки партнеров организации, ответственной за проведение мероприятия. Помните, что большая скидка на востребованный товар — одна из излюбленных ловушек мошенников. То же касается и выгодных вакансий: слишком хорошее предложение о работе — веская причина насторожиться.

VPN

В 2022 году страны Персидского залива заняли верхние строчки мирового рейтинга по использующей VPN-сервисы доле населения. Рынок находящихся с точки зрения закона в серой зоне приложений и сервисов привлекает и злоумышленников, которые распространяют вредоносные версии ПО, а также активно используют рекламу виртуальных частных сетей в фишинге, завлекая пользователей выгодными предложениями и обещаниями анонимности.

Например, в рамках одной из кампаний злоумышленники создавали фишинговые сайты, предлагающие скачать якобы официальные VPN-решения. Однако в результате на устройство жертвы под видом оригинального приложения устанавливалось шпионское ПО.

Рисунок 3. Фишинговый сайт поддельного VPN-решения



Мы подготовили несколько простых рекомендаций о том, как не попасться на уловки мошенников при установке приложений:

- Отдавайте предпочтение давно загруженным в магазин приложений решениям с высоким рейтингом и «живыми» комментариями (написанными не ботами). Бессмысленные никнеймы, повторяющиеся фразы отзывов и общие формулировки без деталей и комментариев о работе приложения могут свидетельствовать о накрутке оценки.
- Скачивайте установочные файлы только с официальных ресурсов.
- Увидев рекламу выгодного предложения, самостоятельно откройте официальный сайт компании. Если акция не фишинговая, вы получите эти же условия без риска заразить свое устройство.

Темная сторона: как киберпреступники готовятся к атакам

Одна из причин успеха социальной инженерии — многочисленные утечки данных из различных организаций. На теневых ресурсах злоумышленники активно продают информацию о пользователях, а также раздают украденные архивы данных бесплатно.

Рисунок 4. Сообщение о продаже украденных данных

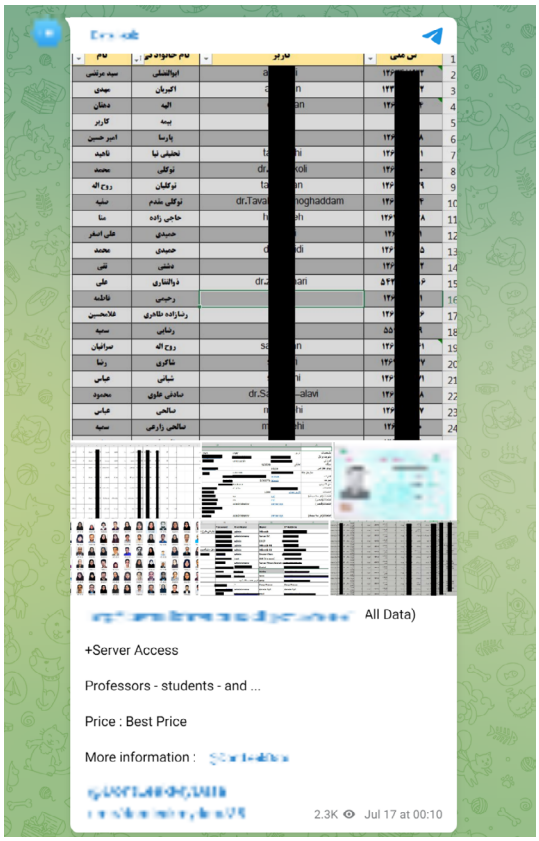
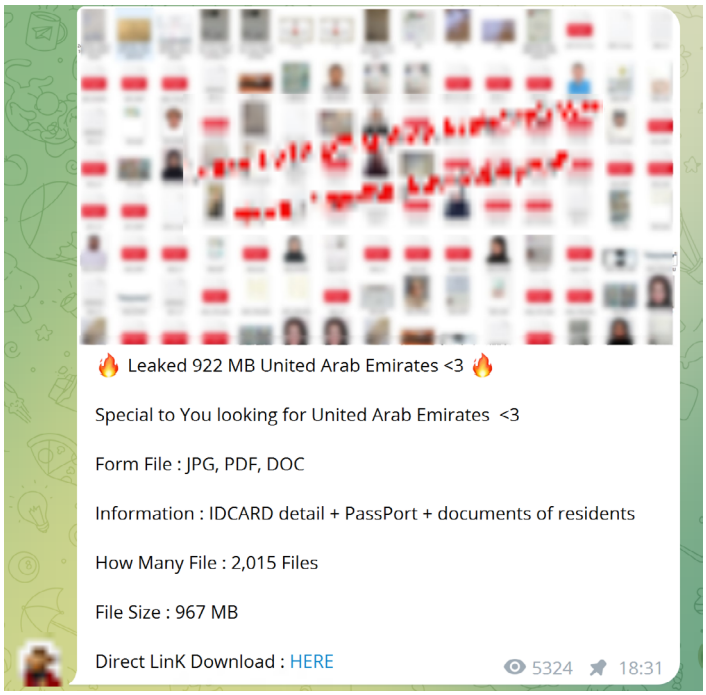
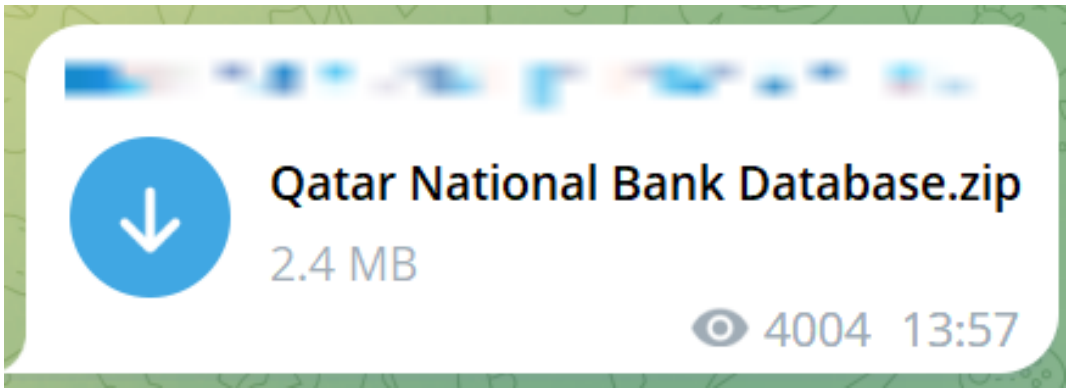


Рисунок 5. Сообщение о раздаче украденных данных



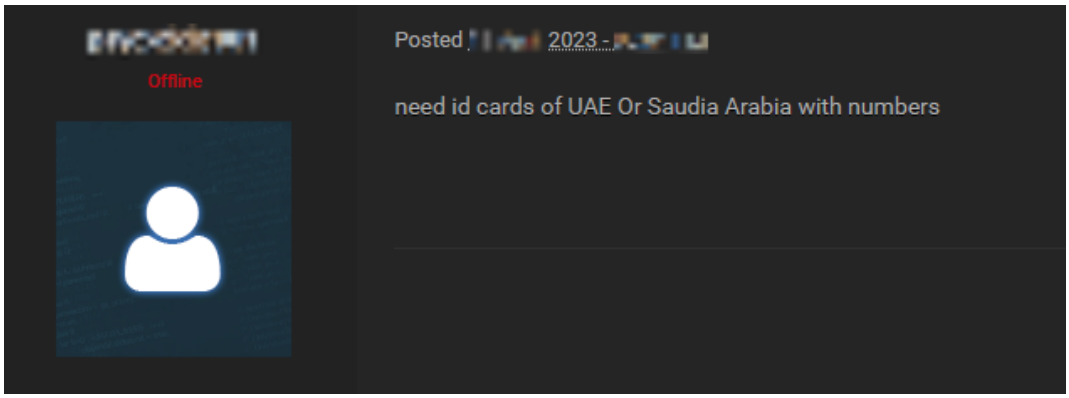
Скомпрометированную информацию преступники используют в последующих атаках на пользователей. Так, результатом успешной атаки на банк могут стать мошеннические действия в адрес его клиентов.

Рисунок 6. Сообщение о раздаче данных, украденных из катарского банка



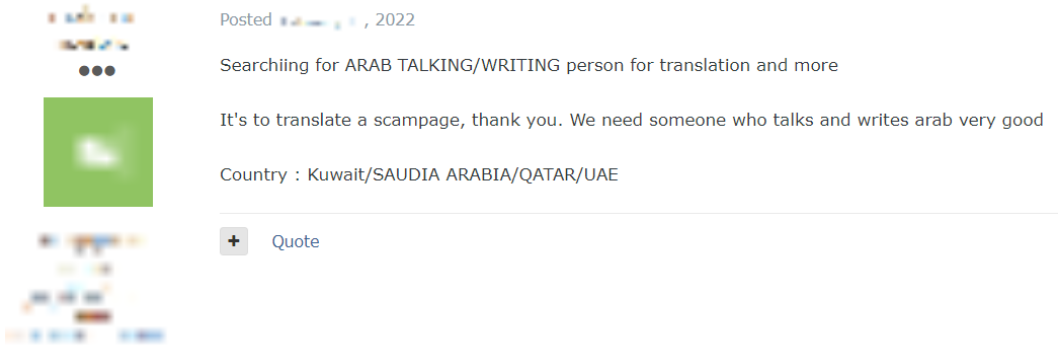
На форумах в дарквебе мы отмечаем также спрос на покупку данных. В одном из объявлений пользователь теневого ресурса искал данные идентификационных карт граждан ОАЭ и Саудовской Аравии. Такая информация может позволить злоумышленнику провести целевые атаки, направленные на конкретных частных лиц.

Рисунок 7. Сообщение о покупке данных идентификационных карт граждан ОАЭ и Саудовской Аравии



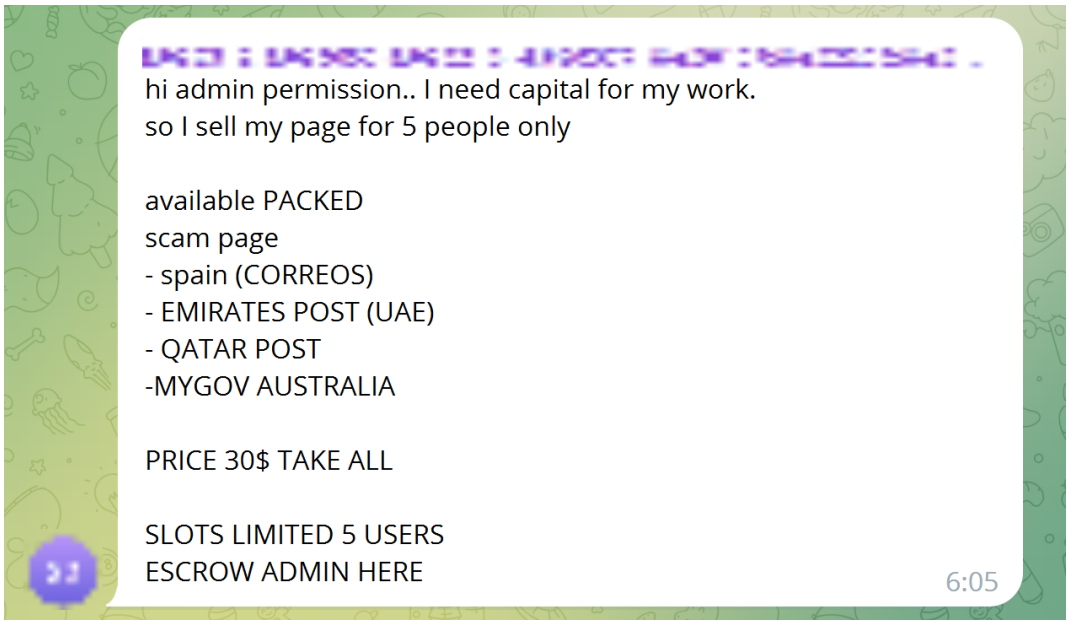
Кроме того, часть объявлений содержали запросы о сотрудничестве.
Например, одному злоумышленнику требовался носитель арабского языка, чтобы перевести фишинговую страницу для атак на пользователей стран Ближневосточного региона.

Рисунок 8. Сообщение о сотрудничестве



В некоторых объявлениях злоумышленники предлагали на продажу уже готовые решения для фишинговых атак, в том числе мошеннические сайты, маскирующиеся под официальные ресурсы служб доставки, таких как Emirates Post и Qatar Post. Покупка готовых решений может позволить провести успешную атаку даже неопытному злоумышленнику.

Рисунок 9. Сообщение о сотрудничестве



Социальная инженерия во всем мире опирается, как правило, на понятные всем человеческие чувства, будь то страх, раздражение, жадность, надежда. Злоумышленник эксплуатирует их, заставляя жертву совершать поспешные и необдуманные действия. Напоминаем вам, что лучший способ борьбы с социальной инженерией — сохранять бдительность.

Шпионское ПО: что похищает и как защититься

Согласно нашим данным, киберпреступники использовали вредоносное ПО в 7 из 10 успешных атак на частных лиц в Ближневосточном регионе. Чаще всего злоумышленники заражали устройства пользователей шпионским ПО (60% атак с использованием ВПО). Этот вид вредоносного ПО собирает информацию с зараженного устройства, после чего передает ее злоумышленнику. В зависимости от задачи шпионское ПО может похищать персональные, банковские и учетные данные пользователя, файлы из памяти устройства.

К примеру, обнаруженная в 2023 году (в том числе и на Ближнем Востоке) шпионская программа KingsPawn может не только отслеживать местоположение жертвы, записывать телефонные разговоры и манипулировать файлами в памяти смартфона, но и включать запись с микрофона зараженного устройства, делать снимки с фронтальной и задней камер. После программа подчищает следы вредоносной активности. Кроме того, KingsPawn ориентирована на устройства с iOS и даже может осуществлять генерацию одноразовых кодов для iCloud (time-based one-time password, TOTP) на произвольные даты. Это позволяет проводить постоянную эксфильтрацию данных пользователя непосредственно из облачного хранилища.

Шпионское ПО разрабатывается так, чтобы его было сложно обнаружить и оно как можно дольше оставалось на устройстве жертвы. Часто программы-шпионы содержат в коде дополнительные функции, характерные для других типов вредоносов, например загрузчиков, инструментов для удаленного управления, стилеров или банковских троянов. Загрузчики используются для распространения ВПО, в том числе шпионского. Их основная задача — скомпрометировать устройство, после чего скачать и установить целевую вредоносную нагрузку. Как правило, загрузчики создаются таким образом, чтобы антивирусы не распознали в них угрозу. ВПО для удаленного управления позволяет злоумышленнику получить удаленный доступ к скомпрометированному устройству и контролировать зараженную систему. Модули удаленного управления помогают скрыть работу вредоносного ПО от пользователя и систем безопасности.

Один из типичных сценариев заражения шпионским ПО:

1. С помощью социальной инженерии пользователя обманом заставляют скачать загрузчик шпионской программы. Киберпреступники распространяют свои продукты через фишинговые сайты и письма, мессенджеры и СМС-сообщения. Загрузчик может быть скрыт в безобидном на первый взгляд документе или встроен в приложение. В каждой четвертой атаке с использованием шпионского ПО (28%) киберпреступники маскировали вредоносные инструменты под официальные приложения известных разработчиков. В некоторых случаях злоумышленникам удавалось даже представить свои инструменты в официальных магазинах приложений.

2. Получив требующиеся для незаконной активности права на устройстве и установив связь с подконтрольным злоумышленнику сервером, загрузчик скачивает и устанавливает вредоносные модули для шпионажа.

3. Установленный вредонос собирает информацию с зараженного устройства: записывает нажатия клавиш клавиатуры, делает снимки экрана, перехватывает учетные данные из браузеров, почтовых клиентов, мессенджеров и конфигурационных файлов, крадет платежные данные из приложений мобильных банков. Далее программа передает информацию злоумышленнику. Для этого используется канал связи с управляющим сервером, также могут использоваться установленные на устройстве легальные программы. Например, шпионское ПО CodeRAT, нацеленное на разработчиков, говорящих на фарси, использовало общедоступный API анонимной загрузки файлов на базе Telegram.

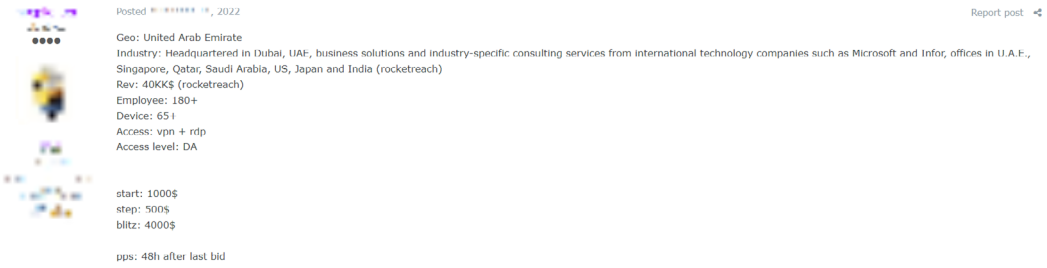
Применяемое киберпреступниками шпионское ПО можно условно разделить на две группы. Первое распространяется по модели malware as a service («ВПО как услуга») или в виде бесплатных исходников. Злоумышленники разрабатывают вредоносное ПО и передают его другим киберпреступникам, которые уже активно применяют его на практике. Часто именно такие вредоносы используются в массовых атаках. Например, в начале 2023 года клиенты банков в ОАЭ стали жертвами новой версии банковского трояна Xenomorph, который похищал не только платежные данные, но и сами денежные средства. Кроме того, исследователи обнаружили рекламный сайт, предназначенный для распространения этого ВПО по модели MaaS. Эксперты предполагают, что злоумышленники намерены начать таким образом крупномасштабное распространение вредоноса.

Ко второй группе относятся программы, используемые в целевых, тщательно спланированных многоэтапных атаках (advanced persistent threat). APT-группировки — это команды высококвалифицированных преступников с хорошим финансированием и техническим оснащением, они часто используют инструменты собственной разработки, в том числе и шпионское ПО. На Ближнем Востоке применяется целая плеяда таких программ: PlugX, семейство модулей Jackal, SandStrike, FurBall, LazaSpy.

Последствия для организаций

При помощи шпионского ПО злоумышленники могут скомпрометировать не только персональную и платежную информацию, данные аккаунтов социальных сетей, стриминговых сервисов и других ресурсов для личного пользования. Среди украденной информации могут оказаться корпоративные учетные данные, сведения о подключении к сети организации и другая чувствительная информация. Украденные данные злоумышленники выставляют на продажу на теневых форумах. В результате завладеть доступом к организации и провести успешную атаку сможет высококвалифицированный злоумышленник, что приведет к недопустимым для компании последствиям: нарушению технологических и бизнес-процессов, краже денежных средств, утечке конфиденциальной информации, атакам на клиентов и партнеров.

Рисунок 10. Объявление о продаже доступов к VPN и RDP



В октябре 2022 года исследователи ESET проанализировали развернутую группой POLONIUM кампанию кибершпионажа. Группировка была нацелена более чем на дюжину организаций в Израиле, включая маркетинговые и страховые компании, СМИ и социальные службы. Эксперты предполагают, что злоумышленники получили первоначальный доступ к целевым системам с помощью скомпрометированных учетных данных VPN, выставленных ранее в открытый доступ.

В начале года мы писали об увеличении доли использования шпионского ПО в атаках на частных лиц по всему миру. На это стоит обратить внимание и пользователям в странах Ближнего Востока, поскольку в исследуемом регионе доля использования шпионского ПО в период с начала 2022 по I квартал 2023 года была выше (60%), чем данные общемировой статистики 2022 года (43%).

Проще всего защититься от шпионских программ на этапе заражения. Чтобы сохранить свои данные в безопасности, следуйте простым и действенным советам:

- Не устанавливайте приложения из ненадежных источников. Хотя в некоторых случаях киберпреступникам удавалось размещать свои продукты и в официальных магазинах приложений, поэтому перед установкой мы советуем всегда проверять информацию о разработчике, дату загрузки в магазин, а также внимательно изучать отзывы других пользователей.
- Используйте антивирус. Это поможет уберечь ваше устройство от заражения в случае взаимодействия с вредоносным файлом.
- Следите за правами, которые запрашивает приложение при установке, и не разрешайте избыточных действий (тех, которые очевидно не нужны ему для выполнения основных функций).
- Следите за работой своего устройства. Если батарея внезапно стала быстрее разряжаться, резко вырос трафик мобильного интернета, самопроизвольно включается Wi-Fi или сервис геолокации, это может говорить о работе шпионских программ.
- В социальных сетях и мессенджерах не открывайте подозрительные вложения, особенно если вы недостаточно хорошо знакомы с отправителем. Архивы, файлы с провокационными названиями — как с незнакомыми расширениями, так и с привычными (.pdf, .xls, .doc), — могут содержать вредоносные скрипты или ссылки на фишинговые ресурсы.
- Если скачиваете программу из интернета, убедитесь в надежности ресурса. Внимательно проверьте адрес в строке браузера: адреса фишинговых сайтов часто похожи на официальные ресурсы, но с небольшими изменениями, незаметными при беглом взгляде, например с повтором лишней буквы или заменой буквы на другую похожую. Посмотрите содержание ресурса: киберпреступники могут пренебречь наполнением, создав лишь основную страницу, а такие разделы, как «Контакты» или «Политика конфиденциальности» оставить без внимания. Опечатки, изображения в низком расширении также можно отнести к признакам подделки. Обращайте внимание на способы оплаты. Если сайт принимает средства только банковским переводом — это повод насторожиться.

Целенаправленные атаки

В целенаправленных атаках злоумышленники действуют против определенной группы лиц или конкретного пользователя. В таких атаках меняется и подход киберпреступников: сначала жертву внимательно изучают и после этого ведут долгую и планомерную работу.

APT-группировки: продвинутые угрозы

В рассматриваемый период APT-группировки активно атаковали не только организации, но и частных лиц на Ближнем Востоке. Именно хакерские группы широко используют уязвимости — как известные, так и нулевого дня — и часто первыми применяют новые методы атак.

Например, в середине 2022 года хакерская группировка CharmingKitten применила метод Multi-Persona Impersonation в атаках на частных лиц. Вместо одного фишингового письма злоумышленники заводили продолжительный диалог из тщательно продуманных сообщений, используя несколько поддельных личностей журналистов и коллег из других стран. В конце такого диалога жертва получает зараженный документ под предлогом, например, проверки корректности ответов на вопросы интервью. При открытии файла на устройство загружается шпионское ПО.

Злоумышленники используют как общедоступные, так и собственные инструменты для успешной компрометации даже тех систем, которые считаются хорошо защищенными.

Все APT-группировки хорошо подготовлены и представляют серьезную угрозу в сети. Приведем несколько примеров APT-групп, атаковавших частных лиц на Ближнем Востоке:

- CharmingKitten — одна из самых известных и активных группировок региона. Применяет для атак на частных лиц продвинутые методы социальной инженерии и использует множество видов собственного вредоносного ПО.
- Bahamut — группировка активно применяет фишинговые сообщения и сайты, вредоносные поддельные приложения. Киберпреступники были замечены в атаках на широкий спектр различных целей. Эксперты считают, что злоумышленники работают в качестве наемников.
- GoldenJackal — группировка с 2019 года шпионит за чиновниками и дипломатами на Ближнем Востоке с помощью целого семейства собственных вредоносных модулей. Злоумышленники действуют скрытно, тщательно выбирая своих жертв и сводя количество атак к минимуму, чтобы снизить риск разоблачения.

Хактивисты

Часть целенаправленных атак совершалась хактивистами, в них преступники пытались нанести жертве максимальный материальный и репутационный ущерб. Киберпреступники иногда действовали точечно, применяя разнообразные средства против конкретной личности. Добившись успеха, хактивисты максимально распространяли украденные личные данные жертвы.

> Мы настоятельно рекомендуем частным лицам начинать переписку с проверки контактов собеседника. Преступники могут представиться журналистами, сотрудниками реальных организаций. Чтобы обнаружить обман, сверяйте данные о собеседнике с контактами, указанными на официальных ресурсах.

Выводы

Ближний Восток — регион, в котором активно применяются новейшие методики кибератак и действуют хорошо подготовленные злоумышленники.

Пользователи страдают от масштабных фишинговых кампаний, опирающихся на крупные события и популярные темы, а также становятся жертвами целевых атак, проводимых различными группировками и хактивистами. Злоумышленники встраивали сертификаты безопасности в фишинговые сайты, а в целевых рассылках притворялись реальными личностями, чтобы жертве было сложнее распознать обман.

Главной угрозой для устройств стало заражение шпионским ПО. Киберпреступники распространяли как приобретенные на теневых ресурсах, так и самописные шпионские программы с широким набором функций. Этот вид вредоносного ПО активно применялся в целевых атаках, зачастую мотивированных политическими причинами.

Сохраняющаяся геополитическая напряженность, внутренние политические события, религиозные конфликты создают плодородную почву для киберпреступников. Группы хактивистов постепенно становятся все более серьезной угрозой, их методы усложняются, позволяя атаковать все более значимые цели. Распространение же готовых комплектов и инструментов для проведения кибератак, использование которых не требует высокой квалификации, способствует появлению новых злоумышленников.

Многие страны Ближневосточного региона принимают меры по борьбе с киберпреступниками — как в техническом, так и в законодательном плане. Несмотря на это, частным лицам необходимо оставаться бдительными, помнить о собственной безопасности при общении в интернете, внимательно следить за работой своих устройств и своевременно устанавливать обновления безопасности.

Компаниям также необходимо заботиться о безопасности данных сотрудников и клиентов. Утечки данных наносят репутационный и финансовый ущерб, а также ставят под удар пользователей, чья информация была скомпрометирована. Чтобы действия киберпреступников не приводили к таким недопустимым для компании последствиям, как мошенничество в адрес пользователей, мы рекомендуем обратить внимание на устойчивость организаций к атакам злоумышленников. Для поддержания киберустойчивости необходимо регулярно проводить проверку эффективности принятых мер безопасности, и особое внимание мы рекомендуем уделять верификации недопустимых событий.

Об исследовании

Отчет содержит информацию об инцидентах информационной безопасности, затронувших частных лиц Ближневосточного региона, основанную на собственной экспертизе компании Positive Technologies, а также на данных авторитетных источников. В исследовании мы учитываем только успешные кибератаки (инциденты), которые привели к негативным последствиям для частного лица. В отчете были рассмотрены инциденты в таких странах, как Бахрейн, Египет, Израиль, Иордания, Ирак, Иран, Йемен, Катар, Кипр, Кувейт, Ливан, Объединенные Арабские Эмираты, Оман, Палестина, Саудовская Аравия, Сирия.

По нашей оценке, большинство кибератак не предается огласке из-за репутационных рисков. В связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий киберпреступных группировок. Наше исследование проводится с целью обратить внимание обычных граждан и компаний, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз на Ближнем Востоке.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы используем в исследовании, приведены в глоссарии на сайте Positive Technologies.

ptsecurity.com
pr@ptsecurity.com