Актуальные киберугрозы: Азиатский регион 2022–2023

Positive Technologies

ptsecurity.com

Содержание

Введение

В мире, где цифровые технологии проникают во все сферы жизни, кибербезопасность становится одной из ключевых проблем для государств, организаций и частных лиц. Азия со своим разнообразием культур, политических систем и экономических условий также ощущает этот глобальный тренд. В последние годы страны Азии стали глобальными лидерами в области внедрения технологических инноваций, опережая весь остальной мир, но с развитием цифровых технологий в странах этого региона возрастает и необходимость в разработке и реализации устойчивых стратегий кибербезопасности.

В этом отчете мы расскажем о состоянии кибербезопасности в странах Азии. Более подробно мы сосредоточимся на анализе шести крупных стран региона: Китае, Индии, Таиланде, Малайзии, Вьетнаме и Индонезии. Эти страны имеют значительное влияние в регионе, проходят различные стадии цифровой трансформации и сталкиваются с разнообразными проблемами в области кибербезопасности.

Цели отчета:

- Оценить существующий ландшафт кибербезопасности в регионе.
- Определить общие киберугрозы и уязвимости.
- Проанализировать проблемы законодательства и регулирования в сфере кибербезопасности.
- Предложить рекомендации по повышению киберустойчивости.

Ключевые выводы

- Азия — регион со стремительно развивающейся цифровой экономикой и технологиями. Но внедрение инноваций влечет за собой рост активности злоумышленников и, соответственно, необходимость укреплять кибербезопасность.
- Азиатско-Тихоокеанский регион стал самым атакуемым в 2022 году: на него пришелся 31% от общемирового числа атак.
- Рост числа кибератак ставит под угрозу важные для экономики стран Азии отрасли, которые становятся более уязвимыми по мере цифровой трансформации своих операций. Жертвами атак чаще всего становились госучреждения (22% от числа всех атак на организации), промышленные компании (9%), IT-компании (8%) и финансовые организации (7%).
- Кибершпионаж — одна из основных угроз для организаций и государств Азии. В 49% успешных атак на организации была скомпрометирована конфиденциальная информация. Злоумышленников интересуют как данные о пользователях, так и сведения, представляющие собой коммерческую тайну. Государства и организации инвестируют большие суммы в развитие науки и технологий, поэтому здесь так активны кибершпионские группировки: кража такой информации может дать конкурентам технологическое преимущество.

- В 27% успешных атак организации столкнулись с нарушением основной деятельности, в том числе приостановкой бизнес-процессов, отсутствием доступа к инфраструктуре или данным.
- Шифровальщики представляют серьезную угрозу для бизнеса в регионе. Главными жертвами шифровальщиков стали промышленные предприятия, на которые пришлось 34% успешных атак. Вымогатели также нацелены на медицинские учреждения, финансовые организации и IT-компании.
- На теневых форумах ведется торговля и обмен доступами к сетям организаций, скомпрометированными базами данных, услугами по взлому сервисов. В регионе наиболее часто встречаются объявления о продаже доступов к компаниям Китая, Таиланда и Индии. В основном это государственные организации, IT-компании и компании из сферы услуг. Стоимость доступа к сети варьируется от 100 долларов до нескольких тысяч, в зависимости от организации и уровня привилегий.
- Несмотря на быстрое развитие цифровой инфраструктуры и готовность инвестировать в кибербезопасность, законодательство в сфере кибербезопасности все еще требует совершенствования. Кроме того, заметен недостаток международного сотрудничества и единых региональных стандартов в области информационной безопасности.
- Рекомендации для государств по повышению уровня кибербезопасности включают актуализацию законодательства в сфере ИБ, совершенствование механизмов по взаимодействию организаций и национальных центров по реагированию на киберинциденты, поддержку образовательных программ в сфере кибербезопасности, развитие международного взаимодействия и обмена данными.
- Рекомендации для обеспечения киберустойчивости организаций включают определение недопустимых событий и защиту критически важных активов, мониторинг киберугроз и реагирование на них с помощью современных средств защиты, а также оценку эффективности принятых мер и обучение сотрудников.

Цифровое развитие Азии и новые угрозы

Азия — это не только уникальное место стечения культур и традиций, но и центр инноваций и технологий. Экономики региона — одни из самых динамичных и быстрорастущих в мире. Цифровая экономика развивается здесь стремительно, тут находятся представительства технологических гигантов, появляется множество платформ электронной коммерции. В Юго-Восточной Азии цифровая экономика показывает годовой рост в 17%, а в Китае — 13%, это больше, чем показатели США (7%) и Европы (10%). Прогнозируется, что к 2030 году интернет-экономика Юго-Восточной Азии достигнет 1 трлн долларов благодаря популярности электронной коммерции, цифровых платежей, онлайн-образования и удаленной работы. В сфере цифровых платежей к 2030 году объем транзакций предположительно будет составлять от 600 млрд до 1 трлн долларов.

Количество интернет-пользователей увеличивается быстрыми темпами. В целом в Азии доля населения, имеющего доступ к интернету, составляет 67%, а в странах Юго-Восточной Азии эта доля еще выше — 80%. Уровень использования смартфонов в наиболее развитых странах региона также высок, например в Малайзии он составляет 90%.

Кроме того, в технологически передовых странах все больше используются новые технологии, такие как интернет вещей, виртуальная реальность, искусственный интеллект, автономные транспортные средства, которые становятся ключевыми потребителями интернет-услуг.

Правительства стран поддерживают развитие инфраструктуры в рамках национальных стратегий по цифровой трансформации. Многочисленные государственные инициативы, такие как «Цифровая Индия», стратегия Сингапура «Умная нация» или MyDIGITAL в Малайзии, подтверждают стремление региона к цифровому лидерству. Масштабные инвестиции в цифровую инфраструктуру делают этот регион привлекательным для технологических стартапов и крупных игроков рынка.

Но где есть инновации, там появляются и угрозы: быстрое цифровое развитие не всегда сопровождалось укреплением кибербезопасности, а привлекательность региона для злоумышленников только росла. И сейчас увеличивающаяся зависимость от технологий делает кибербезопасность первоочередным вопросом для правительств, бизнеса и граждан.

47%

респондентов заявили об увеличении количества атак на их организации (согласно отчету 2023 Thales Data Threat Report)

По данным отчета IBM, самым атакуемым в 2022 году стал Азиатско-Тихоокеанский регион, на страны этого региона пришелся 31% от общемирового числа атак. Из отчета CheckPoint следует, что во втором квартале 2023 года среднее количество атак в неделю в Азиатско-Тихоокеанском регионе увеличилось на 22% по сравнению с 2022 годом. Более половины организаций Азиатско-Тихоокеанского региона (59%) сообщили, что столкнулись с кибератаками в 2022 году.

Исследование, проведенное Cloudflare в июле 2023 года среди более 4000 руководителей в области кибербезопасности из Австралии, Китая, Гонконга, Индии, Индонезии, Японии, Малайзии, Новой Зеландии, Филиппин, Сингапура, Южной Кореи, Тайваня, Таиланда и Вьетнама, показало, что 78% респондентов столкнулись по крайней мере с одним инцидентом информационной безопасности за последние 12 месяцев. Из них 80% сообщили о четырех или более инцидентах, 50% столкнулись с 10 или более инцидентами. Около 63% респондентов сообщили, что финансовые последствия инцидентов кибербезопасности для их организаций за последние 12 месяцев составили как минимум 1 млн долларов США, при этом у 14% убытки превысили 3 млн долларов США.

Правительства региона осознают наличие угрозы, поэтому придают все большее значение разработке национальных программ по кибербезопасности и инвестируют средства в их реализацию. Тем не менее в регионе недостаточно развито международное взаимодействие, нет единых стандартов в области кибербезопасности, за исключением отдельных инициатив стран ASEAN. В ряде стран законодательная база не успевает обновляться, чтобы соответствовать актуальным угрозам. Организации сталкиваются, с одной стороны, с неясными или нереалистичными требованиями от регуляторов, а с другой — со строгими санкциями за их невыполнение.

Несмотря на растущую частоту атак, только 38% респондентов Cloudflare считают свои организации хорошо подготовленными к угрозам, при этом те, кто работает в здравоохранении, образовании, государственном секторе и туризме, считают, что они, скорее всего, не готовы противостоять кибератакам.

Несмотря на большое количество киберинцидентов, более чем у трети организаций (36%) нет плана реагирования на инциденты, что делает их уязвимыми к атакам.

Хотя страны Азии вкладывают значительные ресурсы в развитие кибербезопасности, существует дефицит квалифицированных специалистов, способных противостоять продвинутым угрозам. Например, в Малайзии нехватка специалистов по кибербезопасности оценивается в 8 тысяч человек. Стратегия кибербезопасности Малайзии (MCSS) нацелена на решение этой проблемы путем обучения и сертификации 20 тысяч специалистов по кибербезопасности к 2025 году. Согласно результатам опроса по обеспечению информационной безопасности, проведенного VNISA среди 135 вьетнамских организаций, до 76% организаций не имеют достаточных кадровых ресурсов в области кибербезопасности, чтобы соответствовать текущим требованиям. В целом в Азиатско-Тихоокеанском регионе замечен наибольший рост числа специалистов по кибербезопасности (15,6% в 2022 году). Тем не менее, по данным ISC2, дефицит в этой сфере оценивается в 2,16 млн человек. Большая часть экспертов в регионе считает, что такой разрыв ставит их организации под угрозу кибератак.

Развитие технологий в Азии, увеличение количества интернет-пользователей будут и дальше поддерживать интерес к этому региону со стороны злоумышленников. Поэтому если не принять меры по решению существующих проблем, то страны Азии будут сталкиваться с ежегодным увеличением экономических потерь от кибератак.

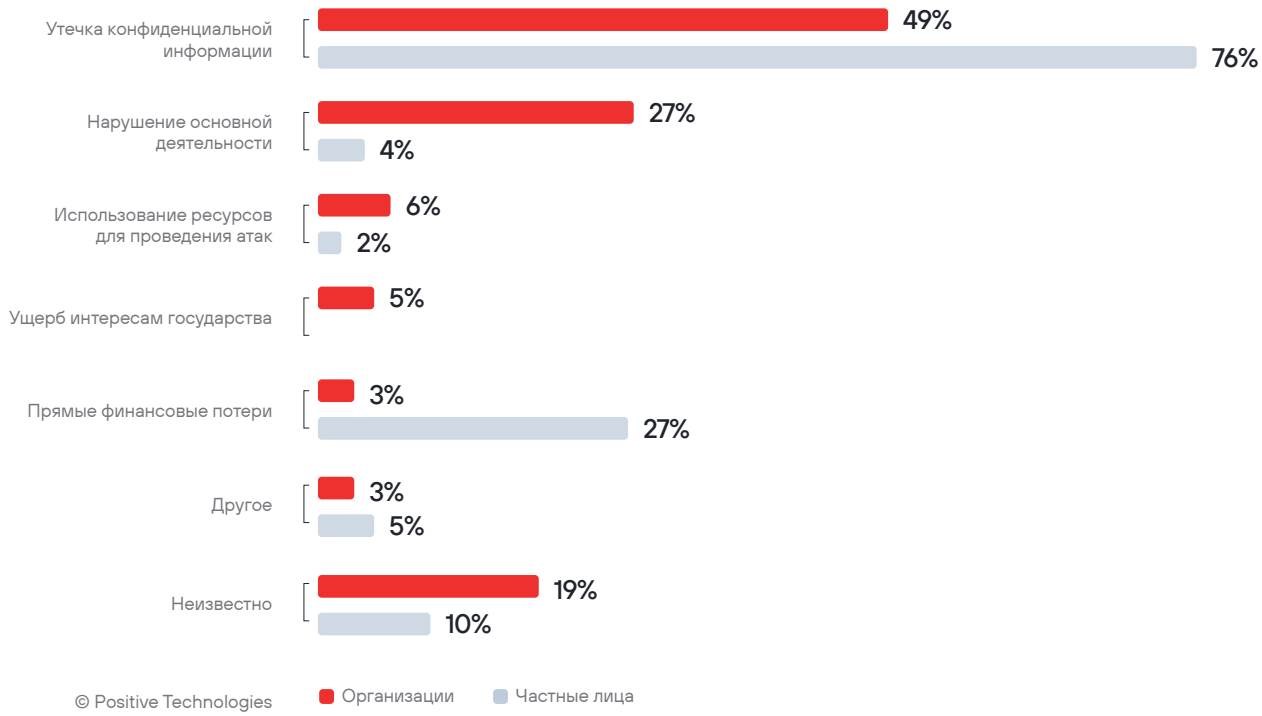
Цели злоумышленников

Кибератаки могут приводить к разным негативным последствиям, вплоть до недопустимых для организации событий, которые катастрофически скажутся на ее деятельности[1]. Почти в каждой второй успешной атаке на организации (49%) была скомпрометирована конфиденциальная информация, а в 27% успешных атак организации столкнулись с нарушением основной деятельности, в том числе приостановкой бизнес-процессов, отсутствием доступа к инфраструктуре или данным.

Относительно малое количество атак (3%) приводило к прямым финансовым потерям — вследствие уплаты выкупа вымогателям или непосредственной кражи денег со счетов компании. Однако общий ущерб от кибератаки складывается из дополнительных расходов, включая затраты на реагирование, расследование, восстановление инфраструктуры, и убытков, связанных с вынужденным простоем и оттоком клиентов. Например, по оценкам IBM, средняя стоимость одной утечки для компании в 2023 году в странах ASEAN составляет 3,05 млн долларов, а в Индии — 2,18 млн.

[1] Недопустимое событие — событие, возникающее в результате кибератаки и делающее невозможным достижение операционных и стратегических целей организации или приводящее к длительному нарушению ее основной деятельности.

Рисунок 1. Последствия атак



74%

атак носили целенаправленный характер, то есть были нацелены на конкретные организации, отрасли или людей.

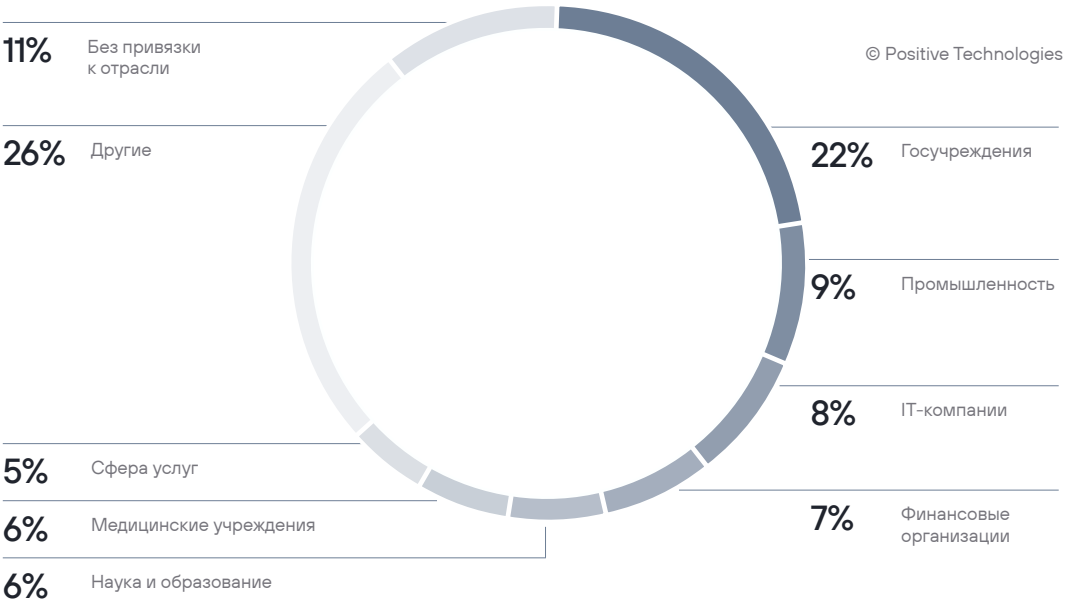
С утечкой конфиденциальной информации сталкивались и обычные пользователи, причем к таким последствиям приводили 76% успешных атак. В 27% случаев пользователи теряли деньги в результате действий злоумышленников.

В рассматриваемый период с начала 2022 года по первое полугодие 2023-го жертвами атак среди организаций чаще всего становились госучреждения (22% от числа всех атак), промышленные компании (9%), IT-компании (8%) и финансовые организации (7%).

24 %

успешных атак были направлены на частных лиц

Рисунок 2. Категории жертв среди организаций



Государственные учреждения

Государственные учреждения в регионе стали основной целью киберпреступников по нескольким причинам. В первую очередь в этих системах хранится большое количество ценной информации, включая личные данные граждан, статистику, сведения государственного значения. Злоумышленникам удавалось украсть данные в 44% успешных атак на государственные организации. В 2022 году было зафиксировано несколько крупных утечек данных из государственных учреждений азиатских стран. Например, осенью 2022 года в Индонезии злоумышленник похитил базу данных с информацией о 105 миллионах граждан, где содержались персональные данные, включая номера удостоверений личности. Предполагается, что данные были украдены из Всеобщей избирательной комиссии Индонезии. База была выставлена на продажу в дарквебе за 5000 долларов.

Многие страны региона проводят цифровую трансформацию и активно интегрируют новые технологии в свои государственные системы. Но при этом возникают новые уязвимости. Некоторые государственные учреждения не могут соответствовать высоким стандартам кибербезопасности из-за ограниченных ресурсов или недостаточной осведомленности о киберугрозах. В июле 2023 года стало известно об утечке данных более 300 миллионов жителей Индонезии, предположительно, из системы Dukcapil. Среди утекших данных — идентификационные номера граждан, контактные телефоны, электронные адреса, домашние адреса. Ответственность за обработку данных граждан и ведение реестров населения в Индонезии лежит на Dukcapil — департаменте при министерстве внутренних дел страны. Dukcapil занимается предоставлением государственных услуг населению, выдачей удостоверений личности, свидетельств о рождении и смерти, позволяет организациям, в том числе финансовым, идентифицировать пользователей для предотвращения мошенничества. Этот орган играет важную роль в системе учета населения Индонезии и активно работает над цифровой трансформацией и внедрением новых технологий.

Кроме того, Юго-Восточная Азия, Индия и Китай имеют большое политическое влияние. Кибератаки на госучреждения могут совершаться как хактивистами для выражения своих политических идей, так и высококвалифицированными APT-группировками с целью шпионажа или дестабилизации ситуации в регионе. Например, группировка хактивистов DragonForce в 2022 году атаковала веб-ресурсы более 70 правительственных и коммерческих организаций Индии.

Промышленность

Промышленность и производственные предприятия в регионе являются важными элементами глобальной цепочки поставок и играют ключевую роль в мировой экономике. Страны региона — мировые лидеры в области производства товаров. Например, на Китай приходится около 30% всего мирового производства. Поэтому они подвергаются атакам с целью кибершпионажа или экономического саботажа. Кроме того, с точки зрения вымогателей, у крупных производственных и промышленных компаний может быть большой потенциал для уплаты выкупа, чтобы восстановить свои операции и избежать простоя.

Производственные предприятия и промышленные компании часто обладают ценной интеллектуальной собственностью, такой как технологические патенты и коммерческая тайна, которые могут быть целью кибершпионажа. Азиатские производители инвестируют миллиарды долларов в исследования и разработки ежегодно. Например, Китай потратил более 3 триллионов юаней (около 456 миллиардов долларов) на научные исследования в 2022 году. Кража такой информации может дать конкурентам или иностранным государствам технологическое преимущество.

В 2023 году индийская компания Solar Industries Limited, производитель промышленных и оборонных взрывчатых веществ, стала жертвой атаки программы-вымогателя. Группировка BlackCat (ALPHV) украла 2 терабайта данных с серверов компании. Среди украденных данных были технические детали производимого оружия и взрывчатых веществ, чертежи, информация о поставках вооружения, контракты компании с заказчиками.

Парализация ключевых предприятий может нанести серьезный удар по экономике страны в целом. Атаки на такие заводы или производственные мощности могут создать сбои в глобальных цепочках поставок, вызывая экономические потери и дестабилизацию рынков. Suzuki Motorcycle India, производитель мотоциклов, в мае 2023 года столкнулся с кибератакой, которая привела к остановке его заводов на неделю. По оценкам компании, потеря в производстве в течение этого периода составила более 20 000 транспортных средств. Suzuki Motorcycle India — пятый по величине производитель двухколесных транспортных средств в Индии, с объемом производства, приближающимся к миллиону единиц.

IT-компании

IT-компании входят в тройку самых атакуемых отраслей по ряду причин. В первую очередь страны Юго-Восточной Азии, включая Индию и Китай, испытали бурный рост в области IT и стали центрами технологических инноваций, в этом регионе находятся ведущие IT-компании мира. Эти компании обладают большим объемом ценных данных, среди которых особый интерес представляют интеллектуальная собственность и пользовательская информация. Их взлом может принести киберпреступникам значительную выгоду, будь то продажа информации на теневом рынке или ее использование для конкурентного преимущества. Кроме того, ресурсы известных IT-компаний можно использовать для проведения атак на другие организации по всему миру.

В июне 2023 года Taiwan Semiconductor Manufacturing Company (TSMC), крупнейший в мире производитель микросхем, сообщил об утечке своих данных. Вымогатели LockBit требовали у компании выкуп в размере 70 миллионов долларов, угрожая опубликовать украденные данные. Утечка информации, «относящейся к первоначальной настройке и конфигурации сервера» (по словам представителя компании), произошла из-за инцидента безопасности у одного из IT-поставщиков TSMC, компании Kinmax Technology. Вымогатели угрожали, что опубликуют информацию о точках входа в сеть TSMC и учетные данные для доступа к ней.

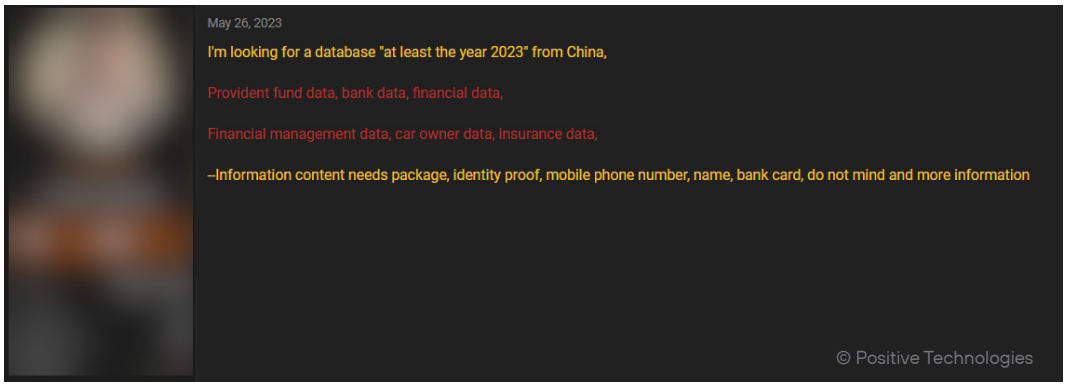
Хотя требования регуляторов по безопасности становятся строже, многие компании в этих регионах еще не полностью соответствуют международным стандартам безопасности. Это может делать их более уязвимыми для кибератак.

Финансовые организации

Организации в сфере финансов и страхования чаще находятся на более продвинутых этапах цифровой трансформации по сравнению с другими отраслями. В результате злоумышленникам требуется больше усилий, чтобы успешно провести атаку против этих организаций, и они, как правило, прибегают к методам социальной инженерии. Однако в рассматриваемом регионе мы видим два основных вектора атаки — электронные письма с вредоносными вложениями и эксплуатация уязвимостей. Это свидетельствует об относительно низком уровне защищенности финансовых организаций. В основном жертвами атак становились индийские банки. В половине случаев успешная атака приводила к краже данных о клиентах банка.

Примечательно, что объявления о покупке баз данных на теневых форумах преимущественно относятся именно к финансовым организациям. Такая информация может быть использована для проведения фишинговых атак. Например, в марте 2023 года появилась новость об утечке данных 600 тысяч клиентов индийского банка HDFC Bank. Среди скомпрометированных данных были имена, даты рождения, номера телефонов, электронные адреса, физические адреса, информация о трудоустройстве, кредитные рейтинги, информация о займах. После этого пользователи начали сообщать о взломе своих банковских аккаунтов и попытках фишинговых атак.

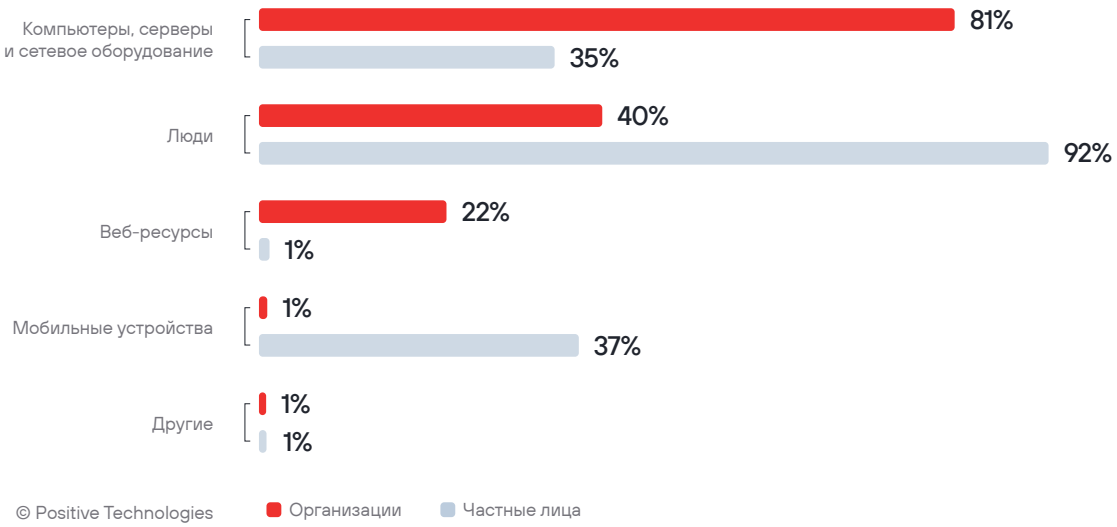
Рисунок 3. Объявление о покупке данных на теневом форуме



Основные киберугрозы

Большинство атак на организации (81%) направлены на компьютеры, серверы и сетевое оборудование. В 22% случаев злоумышленники успешно взламывали веб-ресурсы, чаще всего с использованием известных уязвимостей или компрометации учетных данных.

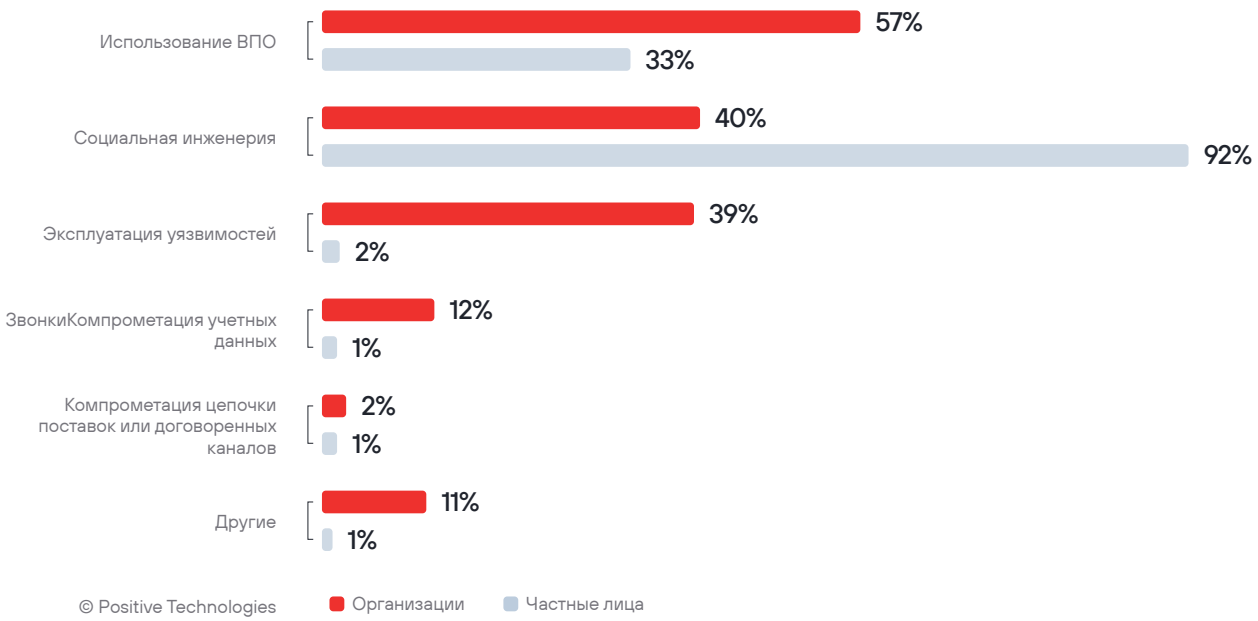
Рисунок 4. Объекты атак



В атаках на организации ВПО используется в 57% случаев. Почти в равной степени применяются как методы социальной инженерии (40% успешных атак), так и эксплуатация уязвимостей в ресурсах компаний (39%). Это свидетельствует о недостаточной защите публично доступных ресурсов компаний. Ресурсы менее защищенных стран могут также использоваться как плацдарм для отработки эксплойтов для уязвимостей.

В 12% случаев атаки проводились с использованием скомпрометированных учетных данных.

Рисунок 5. Методы атак



Частные лица в 92% атак становились жертвами социальной инженерии, а в каждой третьей успешной атаке на них использовалось вредоносное ПО.

Кибершпионаж и утечки данных

В атаках на организации злоумышленникам чаще всего удавалось похитить персональные данные (38% от общего объема украденной информации), учетные данные (14%) и сведения, составляющие коммерческую тайну (28%). Персональные данные утекали в основном из систем государственных учреждений, компаний сферы услуг и ритейла и финансовых организаций. А сведения, относящиеся к коммерческой тайне, интересовали преступников в первую очередь в атаках на промышленные организации и IT-компании.

В атаках на частных лиц злоумышленников интересовали главным образом учетные и персональные данные (35% и 28% соответственно), а также данные платежных карт (12%).

Рисунок 6. Типы украденных данных (в успешных атаках на организации)

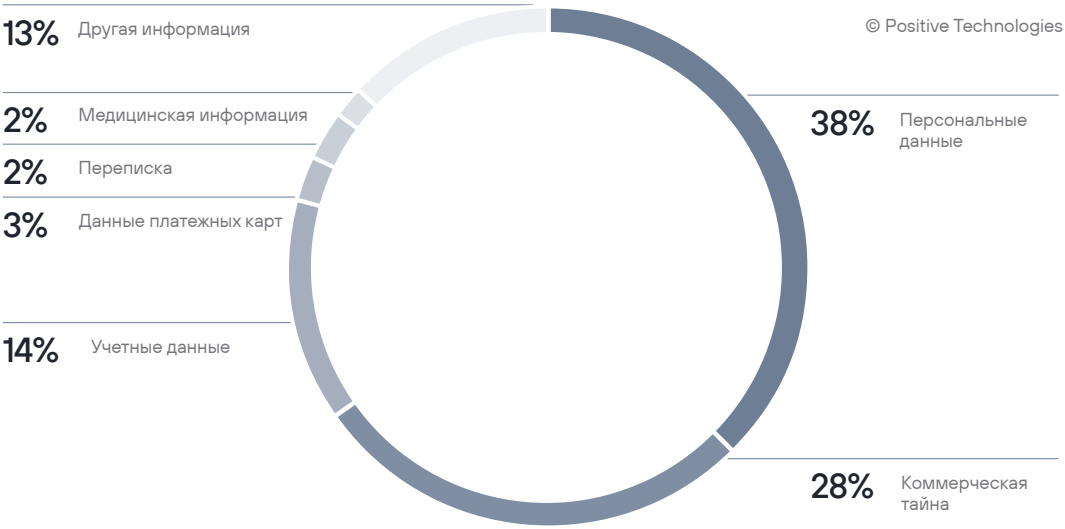
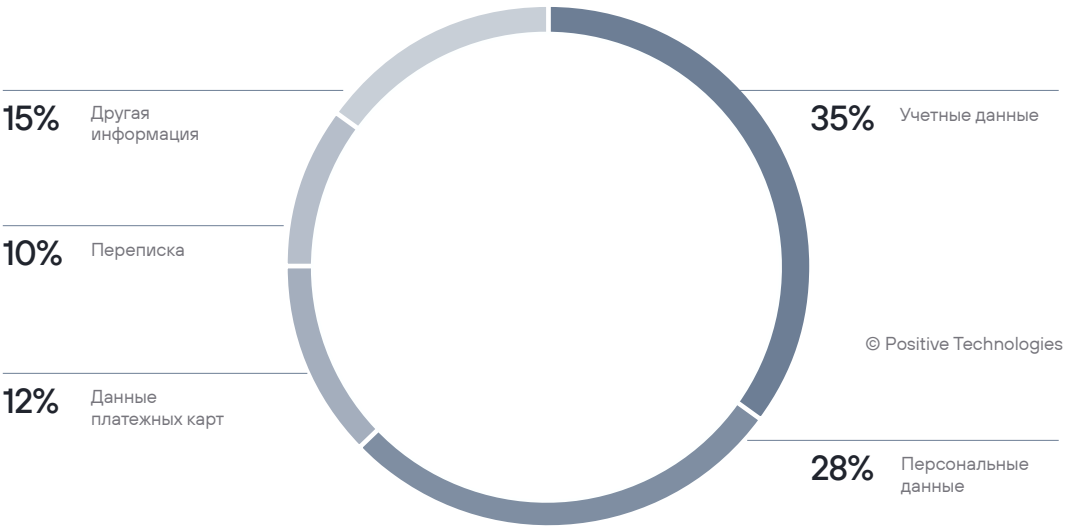


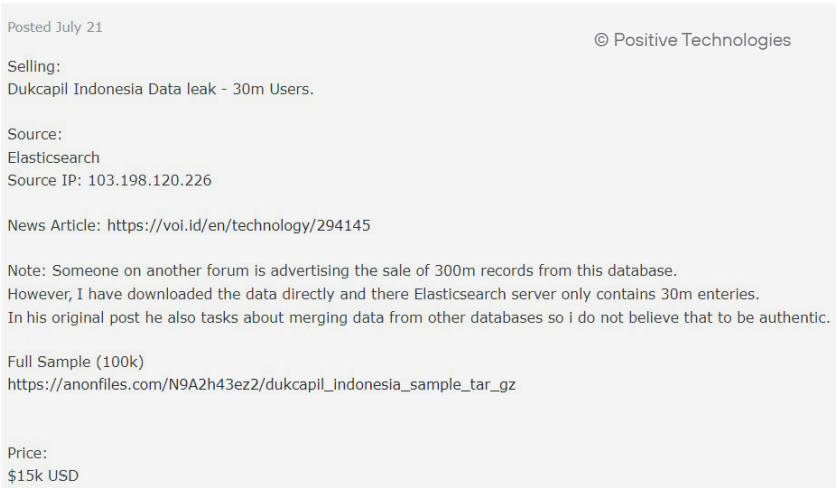
Рисунок 7. Типы украденных данных (в успешных атаках на частных лиц)



Украденные базы данных и другую информацию злоумышленники могут открыто публиковать или продавать в дарквебе. Например, в мае на продажу была выставлена база, содержащая 2,1 млрд уникальных записей о клиентах китайского сервиса экспресс-доставки с персональными данными и мобильными номерами. Стоимость базы составляла 40 тысяч долларов.

Рисунок 8. Объявление о продаже базы данных пользователей в дарквебе

Большую часть данных, которые выставлены на продажу или бесплатно раздаются в дарквебе, закономерно составляет информация, украденная у китайских (39% среди стран Азии) и индийских (22%) организаций и частных лиц. В основном продаются данные, похищенные из государственных и финансовых организаций. В июле 2023 года в дарквебе появилось объявление о продаже базы данных 30 млн пользователей индонезийского государственного сервиса Dukcapil за 15 тысяч долларов.



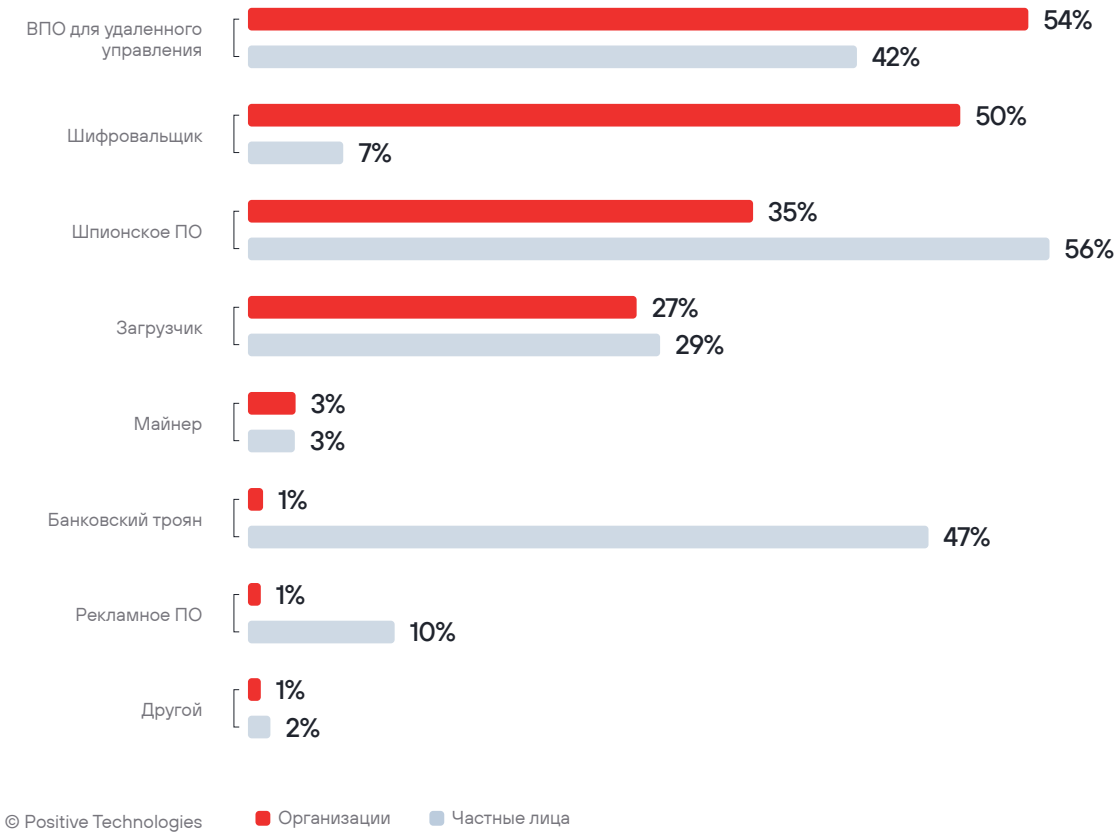
В странах Азии атаки проводят множество высококвалифицированных группировок (advanced persistent threat, APT). Такие группы хорошо организованы, обладают опытом и техническими навыками. Они могут проводить атаки как с целью кибершпионажа, так и с целью получения финансовой выгоды или нарушения деятельности предприятия. Перечислим несколько APT-группировок и финансово мотивированных групп, которые были активны в 2022 и 2023 годах и занимались кибершпионажем в регионе:

- **Mustang Panda.** Кибершпионскую группировку Mustang Panda (TA416, RedDelta, Bronze President) обнаружили в 2017 году. Под прицел преступников попадали государственные, религиозные и некоммерческие организации во Вьетнаме, Китае, Мьянме, Пакистане и Монголии. Mustang Panda действует не только в Азии, но и в Африке, Европе и США.
- **Sharp Panda** проводит кампании в Юго-Восточной Азии с 2021 года. Кибершпионы атакуют правительственные организации Вьетнама, Таиланда и Индонезии.
- **APT32** (OceanLotus, Canvas Cyclone, APT-C-00, Cobalt Kitty) активна как минимум с 2012 года. Группировка специализируется на кибершпионаже и атакует правительственные и корпоративные сети стран Восточной и Юго-Восточной Азии.
- **Dark Pink.** Группировка Dark Pink (Saaiwc Group) действует с 2021 года. Киберпреступники похищают документы военных, правительственных, некоммерческих и религиозных организаций Юго-Восточной и Тихоокеанской Азии. Действуют скрытно и тщательно выбирают цели.
- **BlueHornet** (AgainstTheWest, APT49) атакует не только государственные организации Китая, Северной Кореи, Ирана и России, но и действует против базирующихся в этих странах APT-группировок. Blue Hornet скомпрометировали и распространили данные Kryptonite Panda, Lazarus Group.
- **Transparent Tribe.** Пакистанская группировка Transparent Tribe (APT36, Copper Fieldstone, Mythic Leopard, ProjectM) с 2013 года атакует индийские государственные, военные и исследовательские организации, их работников и служащих. С 2022 года киберпреступники дополнительно нацелились на образовательные учреждения и студентов на Индийском субконтиненте.
- **Billbug.** Группировка Billbug (Lotus Blossom, Thrip) существует с 2009 года. Кибершпионы нацелены на правительственные и промышленные организации в Азии. В атаках преступники применяют как легальное ПО двойного назначения, так и специальные бэкдоры.
- **Charming Kitten.** Иранская группировка Charming Kitten (APT35, Phosphorus, TA453, Ajax Security Team) специализируется на кибершпионаже и краже данных организаций и частных лиц, связанных с геополитическими интересами Ирана. Киберпреступники атакуют жертв на Ближнем Востоке, в Азии, Европе и США.
- **Desorden.** Финансово мотивированная группа Desorden (chaoscc) с 2021 года атакует индийские и малайзийские компании в различных секторах экономики. Группа похищает данные высокодоходных предприятий, чтобы получить как можно больший выкуп. Летом 2022 года Desorden начала кампанию на региональном уровне, сосредоточившись на тайских организациях.

Вредоносное ПО

Наиболее распространенным типом вредоносного ПО в атаках на организации стали инструменты для удаленного управления (54% атак с использованием ВПО). Шифровальщики оказались на втором месте: они использовались в половине атак. Почти в каждой третьей атаке применялось шпионское ПО.

Рисунок 10. Типы вредоносного ПО (доля успешных атак с использованием ВПО)



Частные лица чаще всего сталкивались с заражением устройств вредоносами, предназначенными для кражи данных: шпионским ПО (56%), банковскими троянами (47%), а также ВПО для удаленного управления (42%).

Распространение ВПО в атаках на организации происходит прежде всего за счет компрометации компьютеров, серверов и сетевого оборудования (44%) и через рассылки по электронной почте (41%). На устройства обычных пользователей вредоносы чаще всего попадают через зараженные сайты (34%), электронную почту (16%), социальные сети (16%) и мессенджеры (11%).

Рисунок 11. Способы распространения вредоносного ПО в успешных атаках на организации

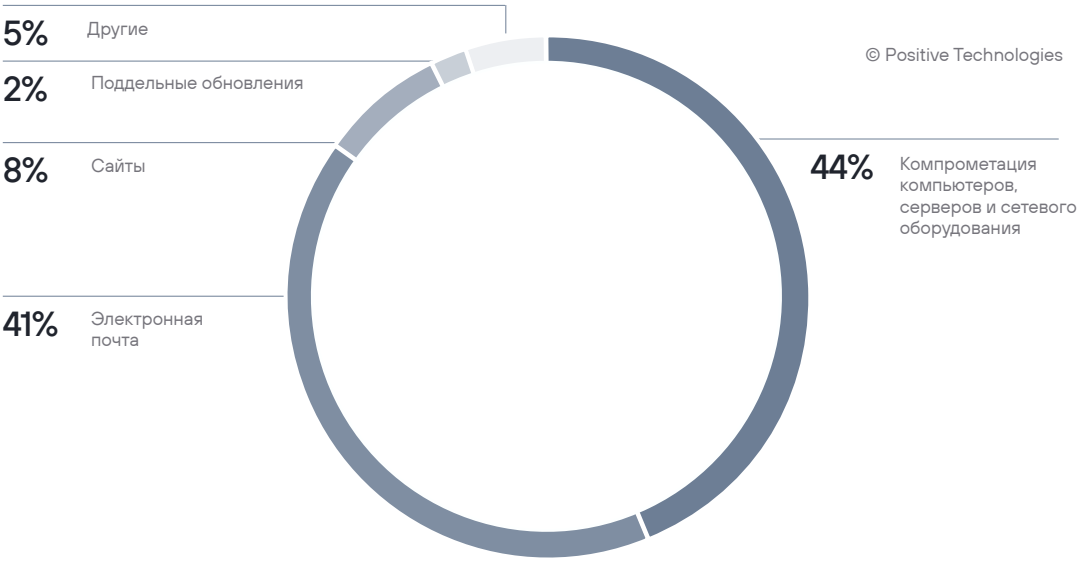
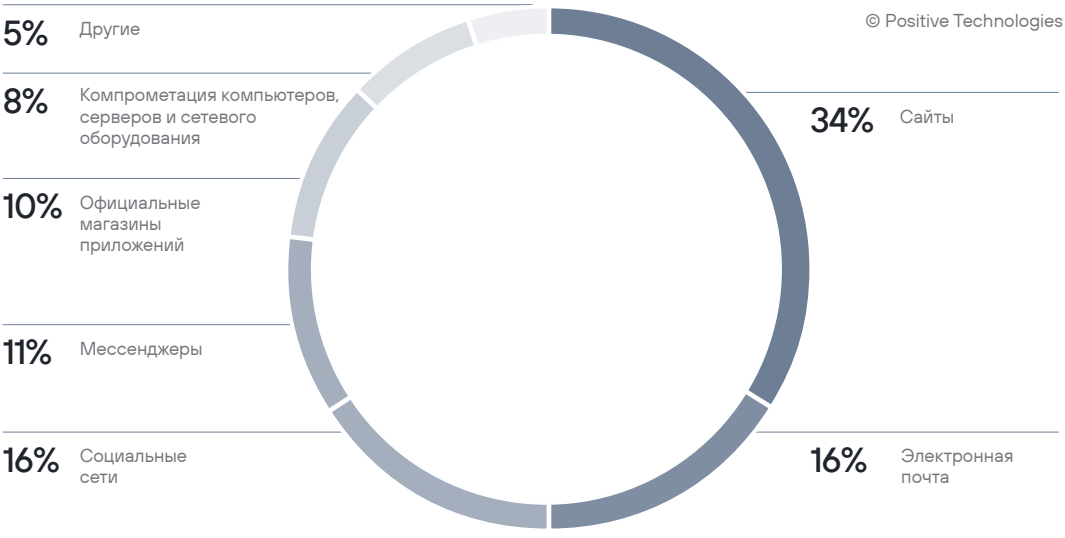


Рисунок 12. Способы распространения вредоносного ПО в успешных атаках на частных лиц

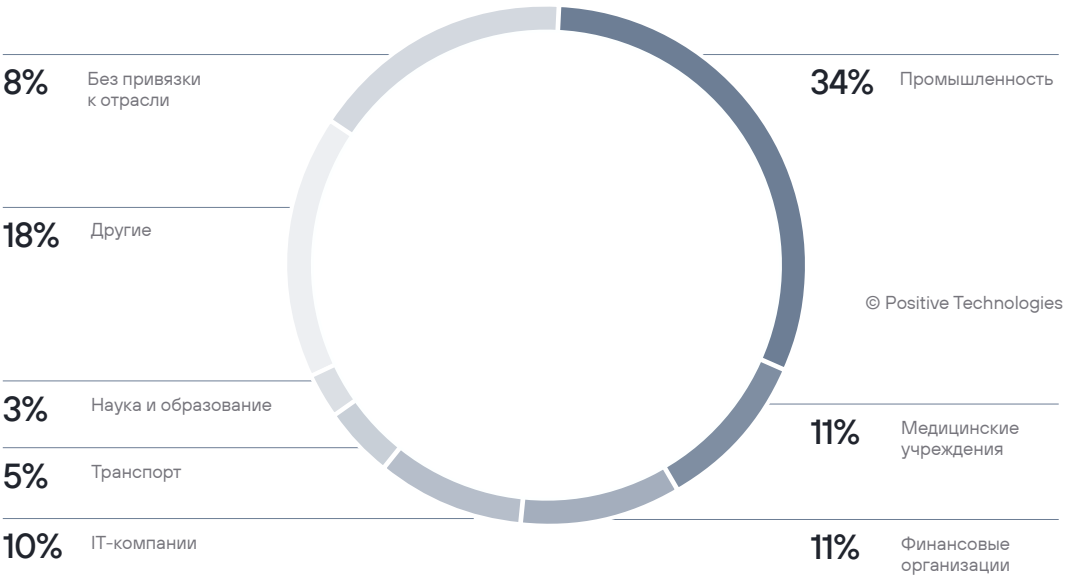


Шифровальщики и вымогатели

Как и во всем мире, в регионе наблюдается активность вымогательского ПО. Например, по данным индийского центра реагирования на киберинциденты CERT-In, количество атак вымогателей в Индии за 2022 год увеличилось на 53%. Особенность атак в последнее время состоит в том, что злоумышленники предпочитают не шифровать инфраструктуру, а требуют выкуп за нераспространение скомпрометированной информации, — это также глобальный тренд, о котором мы говорили в прогнозах на 2023 год. При этом средняя сумма запрашиваемого выкупа остается высокой и измеряется миллионами долларов. Например, в Индии в 2022 году средняя сумма выкупа за расшифровку данных и восстановление доступа к инфраструктуре составила 1,2 миллиона долларов. Далеко не все компании готовы к атакам шифровальщиков: по результатам опроса Corinium Intelligence в странах Юго-Восточной Азии, 45% респондентов предполагают, что в случае атаки шифровальщика ущерб для компании будет варьироваться от среднего до значительного, и только 55% респондентов уверены в надежности принятых мер по резервному копированию и восстановлению.

Главными жертвами шифровальщиков стали промышленные предприятия, на которые пришлось 34% успешных атак. Вымогатели также нацелены на медицинские учреждения, финансовые организации и IT-компании.

Рисунок 13. Распределение инцидентов с использованием шифровальщиков по отраслям



В ноябре 2022 года Всеиндийский институт медицинских наук (AIIMS) в Нью-Дели столкнулся с атакой программы-вымогателя, что привело к приостановке оказания медицинских услуг. Атака затронула различные цифровые сервисы больницы, включая выставление счетов, создание отчетов, проведение лабораторных тестов, сервисы скорой помощи и систему записи на прием. IT-системы, отвечающие за функционирование электронной больницы, пришлось отключить и перевести все операции в ручной режим. На восстановление работы IT-систем потребовалось около двух недель. Более того, злоумышленники похитили данные о пациентах, включая медицинскую информацию, данные о донорах, записи о госпитализациях, вакцинациях и т. д. Руководство больницы отказалось платить выкуп, и вымогатели опубликовали эти данные в дарквебе. Больнице удалось предотвратить еще одну атаку в июне 2023 года, которая не повлияла на оказание услуг пациентам.

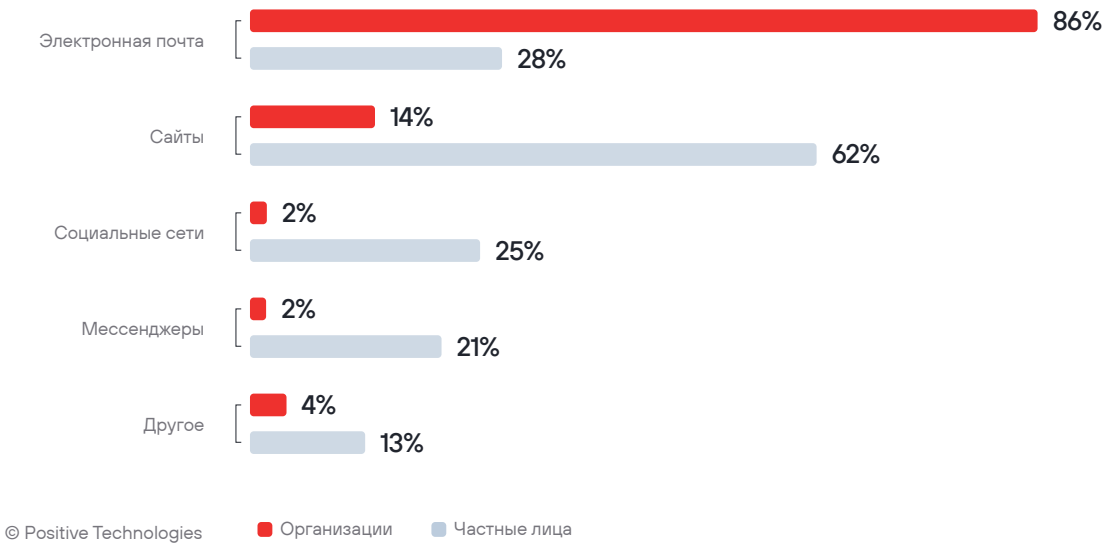
В начале апреля 2023 года Fullerton India, крупное кредитное учреждение Индии, стало жертвой атаки программы-вымогателя LockBit 3.0. В результате атаки было скомпрометировано более 600 ГБ данных, включая персональные данные клиентов Fullerton India, финансовую информацию, номера банковских счетов, детали кредитных договоров и др. Вымогатели потребовали выкуп в размере 240 млн рупий (около 3 миллионов долларов), но компания отказалась вести переговоры, и преступники опубликовали украденные данные в дарквебе.

Главный способ распространения вымогательского ПО (63% успешных атак) — электронная почта. В 32% случаев используются уязвимости в публично доступных ресурсах организаций.

Социальная инженерия

Социальная инженерия является основным вектором проникновения в инфраструктуру организаций и применяется в 40% успешных атак. Во всем регионе отмечается высокая угроза атак с применением методов социальной инженерии. Например, по сообщениям Министерства информации и коммуникаций Вьетнама, количество атак в стране за первые 11 месяцев 2022 года увеличилось на 44% по сравнению с аналогичным периодом 2021 года. При этом фишинговые атаки составили 35% от общего числа инцидентов. Количество фишинговых атак в Сингапуре за 2022 год увеличилось более чем в два раза по сравнению с предыдущим годом. По данным отчета IBM, электронные письма с вредоносными вложениями — главный вектор распространения вредоносного ПО в Азиатско-Тихоокеанском регионе. При этом эксперты IBM отмечают, что средний ущерб от атаки, которая проводится с помощью фишинга, составляет 4,76 млн долларов — дороже обходятся только атаки со стороны внутренних нарушителей.

Рисунок 14. Каналы социальной инженерии



Социальная инженерия используется как неопытными киберпреступниками, которые покупают готовые инструменты для создания фишинговых рассылок, так и вымогателями, и APT-группировками. Самый популярный вектор фишинговой атаки в отношении организаций — это рассылка электронных писем, но злоумышленники также могут создавать поддельные сайты для хищения учетных данных или распространения вредоносного ПО. Чаще всего подделываются сайты банков и платежных сервисов с целью кражи денег или данных для аутентификации.

Из отчета компании KnowBe4 следует, что около 30% сотрудников организаций в Азии затрудняются распознать фишинговое письмо, то есть в случае атаки злоумышленника каждый третий сотрудник может открыть вредоносное вложение, пройти по вредоносной ссылке или передать злоумышленнику свои учетные данные. С развитием AI-инструментов проблема становится еще серьезнее, поскольку генеративные модели позволяют преступникам создавать максимально правдоподобные письма на различных языках и упрощают проведение атак международным группировкам.

Развитие киберпреступных форумов

На теневых форумах киберпреступники осуществляют торговлю и обмен вредоносным ПО, украденными данными, предлагают различные услуги криминального характера. Здесь злоумышленники могут приобрести готовый доступ к сетям интересующих их организаций. В странах региона наиболее часто встречаются объявления о продаже доступов к компаниям Китая, Таиланда и Индии. В основном это государственные организации, IT-компании и компании из сферы услуг.

Стоимость доступа зависит от размера организации и привилегий учетной записи. Доступ к сети с правами рядового пользователя или к небольшой компании может обойтись в 100–200 долларов, а привилегии администратора домена оцениваются в 500 долларов и выше. Например, одно из самых дорогостоящих предложений — доступ к сети китайского производителя фотоэлектрических модулей с привилегиями администратора домена — оценивается в 20 тысяч долларов. За доступ к инфраструктуре вьетнамской телекоммуникационной компании злоумышленники рассчитывают получить до 4800 долларов.

Рисунок 15. Объявление о продаже доступа к вьетнамской телекоммуникационной компании

Проблемы законодательства

В отличие от других регионов, например Европы или Африки, в Азии (за исключением отдельных инициатив стран ASEAN) нет тенденции к созданию единых стандартов по кибербезопасности во всем регионе. Несмотря на общие цели, каждая страна разрабатывает свой подход в соответствии со своими национальными интересами и спецификой.

Не останавливаясь подробно на всех особенностях законодательства в сфере ИБ каждой страны, мы постараемся выделить основные проблемы, которые важно решить на уровне государства.

- Устаревшее законодательство

Технологии развиваются быстро, поэтому законодательство может не успевать за постоянными изменениями, что делает его не всегда релевантным современным угрозам. Во многих странах региона актуальна проблема устаревшего законодательства. В некоторых странах не существует единого или специализированного закона в области ИБ.

Например, основная проблема регулирования кибербезопасности в Индии заключается в устаревших и непрозрачных законах. В Индии отсутствует единый закон о кибербезопасности, вместо него применяется закон об информационных технологиях и ряд специфических отраслевых регламентов для поддержания стандартов кибербезопасности. Таким же образом устанавливается правовая основа для защиты критической информационной инфраструктуры. Для решения этих проблем Индии необходимы актуальные всесторонние законы, четкие правовые рамки в области кибербезопасности, а также открытый диалог с экспертами в области ИБ. На данный момент правительство разрабатывает новую национальную стратегию кибербезопасности, а также рассматривает вопрос о модернизации закона об IT.

В Малайзии пока что также отсутствует единое или специализированное законодательство в области кибербезопасности. Тем не менее правительство Малайзии объявило о своем намерении принять отдельный закон по кибербезопасности для регулирования вопросов в этой сфере и устранения пробелов в действующем правовом поле. Отсутствие специализированного закона означает, что в Малайзии вопросы кибербезопасности регулируются в рамках различных законодательных актов, включая Закон о связи и мультимедиа 1998 года и Закон о защите персональных данных 2010 года. Эти законы затрагивают различные аспекты кибербезопасности, но не обеспечивают их комплексного регулирования, большая часть существующего законодательства устарела и не соответствует темпам развития современных технологий. Цель предложенного закона о кибербезопасности в Малайзии заключается в создании комплексной правовой основы для регулирования вопросов кибербезопасности и защиты граждан Малайзии от угроз в этой сфере.

- Неясность или фрагментарность требований

Многие организации сталкиваются с проблемами понимания и внедрения необходимых мер безопасности из-за недостаточно ясных требований и фрагментированного законодательства о конфиденциальности данных и кибербезопасности.

В Индии образовалась сложная межведомственная система в области кибербезопасности, в которой несколько министерств, департаментов и агентств выполняют отдельные важные функции. Например, Министерство электроники и информационных технологий (MeitY) занимается политикой в области IT, электроники и интернета, и под его началом был создан национальный центр реагирования на киберинциденты CERT-In. Закон об информационных технологиях устанавливает обязательства по безопасности для организаций, работающих с персональными данными. Правила соответствуют международному стандарту ISO/IEC 27001 по управлению информационной безопасностью, причем корпорации подлежат аудиторской проверке независимым утвержденным правительством аудитором хотя бы раз в год или при значительном обновлении процессов и компьютерных ресурсов. Отраслевые регуляторы и центральные агентства также предписывают меры безопасности. Резервный банк Индии устанавливает стандарты для банков, включая создание механизма для обработки и сообщения об инцидентах и организацию постоянного мониторинга систем и защиты информации клиентов. Он также обязывает банки следовать стандартам ISO/IEC 27001 и ISO/IEC 27002. Разброс требований и большое количество регулирующих органов усложняют понимание того, какие меры защиты необходимо внедрить, и могут снижать их эффективность.

Законодательство Таиланда в сфере ИБ также подвергается критике за недостаточно понятные и точные указания. Учитывая строгость санкций за неисполнение требований, это серьезная проблема для организаций.

- Отсутствие единых стандартов по кибербезопасности в регионе

Каждая страна в Азии имеет свой набор законов в области кибербезопасности, направленных на защиту национальной безопасности, а также на развитие информационных технологий и коммуникаций. Такой подход может влиять на международное сотрудничество между странами и осложнять передачу данных о киберугрозах, заимствование лучших практик и отказ от устаревших, а также препятствовать эффективному взаимодействию между правоохранительными органами стран.

Отдельно стоит упомянуть, что страны ASEAN демонстрируют совместный интерес к созданию надежной системы кибербезопасности. Основная цель — защита пользователей в интернете, обеспечение стабильности цифровых систем и поддержка экономического роста. Страны выработали совместную стратегию кибербезопасности, общий фреймворк по защите данных, также ведется работа над созданием единого CERT ASEAN. Но, несмотря на такое сотрудничество, пока нет гарантий того, что оно приведет к объединению законодательных рамок в Юго-Восточной Азии.

В 2021 году страны ASEAN приняли общий фреймворк по управлению данными (ASEAN Data Management Framework, DMF), схожий с европейским регламентом по защите данных (General Data Protection Regulation, GDPR), и Положение о трансграничной передаче данных (Model Contractual Clauses, MCC). Они были разработаны для согласования стандартов трансграничной передачи данных и практик управления данными по всему региону. Документы носят рекомендательный характер и не обязывают участников вносить изменения в существующие законы о защите данных. При этом от участников ожидается поощрение соблюдения DMF и MCC со стороны бизнеса в соответствующих юрисдикциях. К примеру, Комиссия по защите данных Сингапура выпустила дополнительные рекомендации для организаций в Сингапуре относительно использования MCC.

- Чрезмерно строгие требования и санкции

В 2022 году индийское правительство выпустило новые требования по механизму уведомления о киберинцидентах. Организации по всей Индии должны сообщать о киберинцидентах в CERT-In в течение всего шести часов с момента обнаружения. Специалисты по кибербезопасности сходятся во мнении, что такой промежуток времени недостаточен для проведения всех необходимых процедур по предварительному расследованию, которые нужны для предоставления отчетности. Ранее сообщать о киберинциденте требовалось «в разумные сроки» после его выявления. Теперь окно для уведомления значительно меньше, чем в ЕС или США. Например, Общий регламент ЕС по защите данных (GDPR) требует, чтобы о нарушениях безопасности персональных данных сообщалось в течение 72 часов, что достаточно для подробного анализа инцидента. Организации, которые не соблюдают новые требования о порядке уведомления CERT-In, могут столкнуться с уголовным делом и крупными штрафами за нарушение закона.

В интересах национальной безопасности некоторые страны, к примеру Вьетнам и Китай, приняли законы о локализации хранения и обработки данных. Регуляторы считают, что такой подход более безопасен, но он ведет к снижению экономической конкурентоспособности. Так, закон о кибербезопасности Вьетнама подвергался критике из-за возможного воздействия на иностранные инвестиции и бизнес, работающий в стране. Законодательство Китая также известно своими жесткими мерами ответственности за нарушения в области кибербезопасности и конфиденциальности: для бизнеса это серьезный риск, так как штрафы могут быть весьма велики. Данные являются жизненно важной частью цифровой экономики, и политика локализации данных не способствует ее росту. Вместо этого следует использовать передовые технологии, чтобы поддерживать безопасный трансграничный обмен данными на основе согласованных стандартов.

Излишне строгие требования и санкции в долгосрочной перспективе могут приводить не к повышению эффективности ИБ, а к замалчиванию информации об уязвимостях и инцидентах, и также могут негативно влиять на развитие бизнеса в стране, особенно международного. При разработке законопроектов крайне важен диалог между государством, бизнесом и экспертами по кибербезопасности.

Выводы и рекомендации

Количество атак на азиатские страны увеличивается с каждым годом, поэтому государствам и организациям необходимо усилить свою защиту. Для этого следует создать результативную стратегию кибербезопасности и убедиться в наличии ресурсов для ее реализации. Хорошей отправной точкой для специалистов по информационной безопасности может стать сравнение собственной системы кибербезопасности с мировыми стандартами.

Очень важно эффективное регулирование и сотрудничество на государственном уровне. В этом могут помочь трансграничные инициативы, такие как сотрудничество в области кибербезопасности Ассоциации государств Юго-Восточной Азии (ASEAN), и обновление законодательства в странах региона.

Рекомендации для государств

Актуализация и регулярное обновление законодательства в области кибербезопасности и защиты персональных данных

В некоторых странах региона нет специализированного закона о кибербезопасности, действующие законы устарели и нуждаются в обновлении, требования по обеспечению кибербезопасности фрагментированы, и организациям сложно понять, как правильно внедрять необходимые меры. Эти проблемы необходимо решать для более эффективного выполнения требований. Законодательство должно регулярно обновляться, чтобы соответствовать актуальным киберугрозам и успевать за развитием технологий. Законодательство должно способствовать эффективной координации между различными правоохранительными органами и органами безопасности. При этом следует учитывать, что чрезмерное ужесточение требований и санкций за их неисполнение не будет способствовать повышению защищенности в долгосрочной перспективе.

Желательно рассмотреть возможность унификации стандартов по кибербезопасности среди стран региона для более эффективного взаимодействия между государствами либо предусмотреть общие механизмы международного сотрудничества и обмена информацией о международных киберугрозах.

Защита критической информационной инфраструктуры

Государства должны определить недопустимые события на уровне отраслей и страны. Такой подход позволит эффективно распределять ресурсы для обеспечения защиты наиболее важных систем. В первую очередь необходимо рассмотреть инфраструктуру таких секторов, как государственные предприятия, телекоммуникации, финансы, а также других отраслей, критически важных для экономики и национальной безопасности, например высокотехнологичного производства, фармацевтики, сельского хозяйства. При этом необходимо учитывать скорость цифровой трансформации в стране и уровень зрелости ИБ.

Совершенствование механизмов по взаимодействию с национальными и отраслевыми центрами по реагированию на киберинциденты

В странах Азии уже существуют национальные центры по реагированию на киберинциденты (CIRT), которые отвечают за мониторинг угроз и помощь организациям в восстановлении после серьезных кибератак. Однако механизмы уведомления об инцидентах могут быть недостаточно понятны для специалистов по безопасности, либо требования вызывают возражения и споры среди специалистов. Необходимо разработать понятные и прозрачные механизмы по уведомлению о киберинцидентах, происходящих в организациях, с учетом мнения экспертов и сообщества по ИБ. Улучшенный обмен информацией между организациями и центрами кибербезопасности может помочь предотвращать атаки и своевременно реагировать на новые угрозы.

Реагирование на киберугрозы должно быть интегрировано в общую стратегию по защите и восстановлению критической национальной инфраструктуры.

Повышение уровня осведомленности и поддержка образования в области ИБ

Государства должны инвестировать в кампании по информированию общественности об актуальных угрозах и защите от них. В регионе, как и во всем мире, наблюдается нехватка квалифицированных специалистов по кибербезопасности, поэтому популяризация этой области и связанных с ней профессий, поддержка образовательных программ в учебных заведениях должна быть в приоритете у государства.

Международная кооперация

Киберпреступность давно вышла за пределы границ одного государства, поэтому для стран крайне важно сотрудничать с международными партнерами в борьбе с киберугрозами. Обмениваясь информацией, ресурсами и экспертизой, страны могут коллективно укреплять свои защитные меры и снижать риски, исходящие от киберпреступников из разных юрисдикций. Национальные стратегии по кибербезопасности должны включать в себя задачи по развитию международных отношений в области кибербезопасности.

Рекомендации для бизнеса

Определение недопустимых для бизнеса событий и критически важных активов

Для обеспечения киберустойчивости компаниям в первую очередь необходимо провести анализ основных рисков и составить перечень недопустимых событий, которые могут нанести существенный ущерб их деятельности. Этот шаг позволит определить критически важные активы и сосредоточиться на защите самых ценных ресурсов. Следует разработать стратегию для предотвращения недопустимых событий, включая необходимые меры безопасности и мониторинг сетевой активности с использованием современных средств защиты.

Мониторинг и реагирование на киберугрозы

Системы мониторинга и обнаружения инцидентов необходимы, чтобы своевременно реагировать на потенциальные угрозы и атаки. С этой целью рекомендуется использовать SIEM-системы, которые собирают и анализируют информацию о событиях безопасности из различных источников в реальном времени. Если использовать их совместно с решениями XDR, которые обеспечивают централизованное обнаружение угроз и реагирование на них, а также решениями NTA, которые анализируют сетевой трафик, это позволит повысить эффективность защиты, обнаруживать атаки на ранних стадиях и обеспечивать быструю реакцию на угрозы, снижая риски для организации.

Оценка эффективности кибербезопасности

Следует регулярно проводить практическую проверку эффективности принятых мер кибербезопасности, чтобы оценить работоспособность стратегии и средств защиты. Особое внимание рекомендуется уделять верификации недопустимых для организации событий.

Кроме того, стоит рассмотреть участие в программах bug bounty, которые позволяют привлечь внешних исследователей безопасности для поиска новых уязвимостей. Это поможет обнаружить и устранить уязвимости до того, как они будут использованы злоумышленниками.

Обучение сотрудников и развитие специалистов по ИБ

Важно обучать сотрудников кибербезопасности и проводить тренинги, чтобы повысить осведомленность об актуальных угрозах и укрепить навыки защиты от социальной инженерии.

Для эффективной борьбы с киберугрозами организациям следует инвестировать в развитие своих специалистов по ИБ. Регулярное обучение и сертификация сотрудников в области кибербезопасности помогут улучшить их знания и навыки, а также обеспечат компании экспертную поддержку в предотвращении кибератак и реагировании на них. Одним из наиболее эффективных способов тренировки является участие в киберучениях на специализированных площадках, где специалисты по ИБ могут отработать навыки распознавания техник атак и противодействия им.

Об исследовании

Данные и выводы, представленные в этом отчете, основаны на собственной экспертизе Positive Technologies, а также анализе общедоступных ресурсов, включая публикации правительственных и международных организаций, научно-исследовательские работы и отраслевые доклады.

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 хакерских групп. Наше исследование проводится с целью обратить внимание организаций и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

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

ptsecurity.com
pr@ptsecurity.com