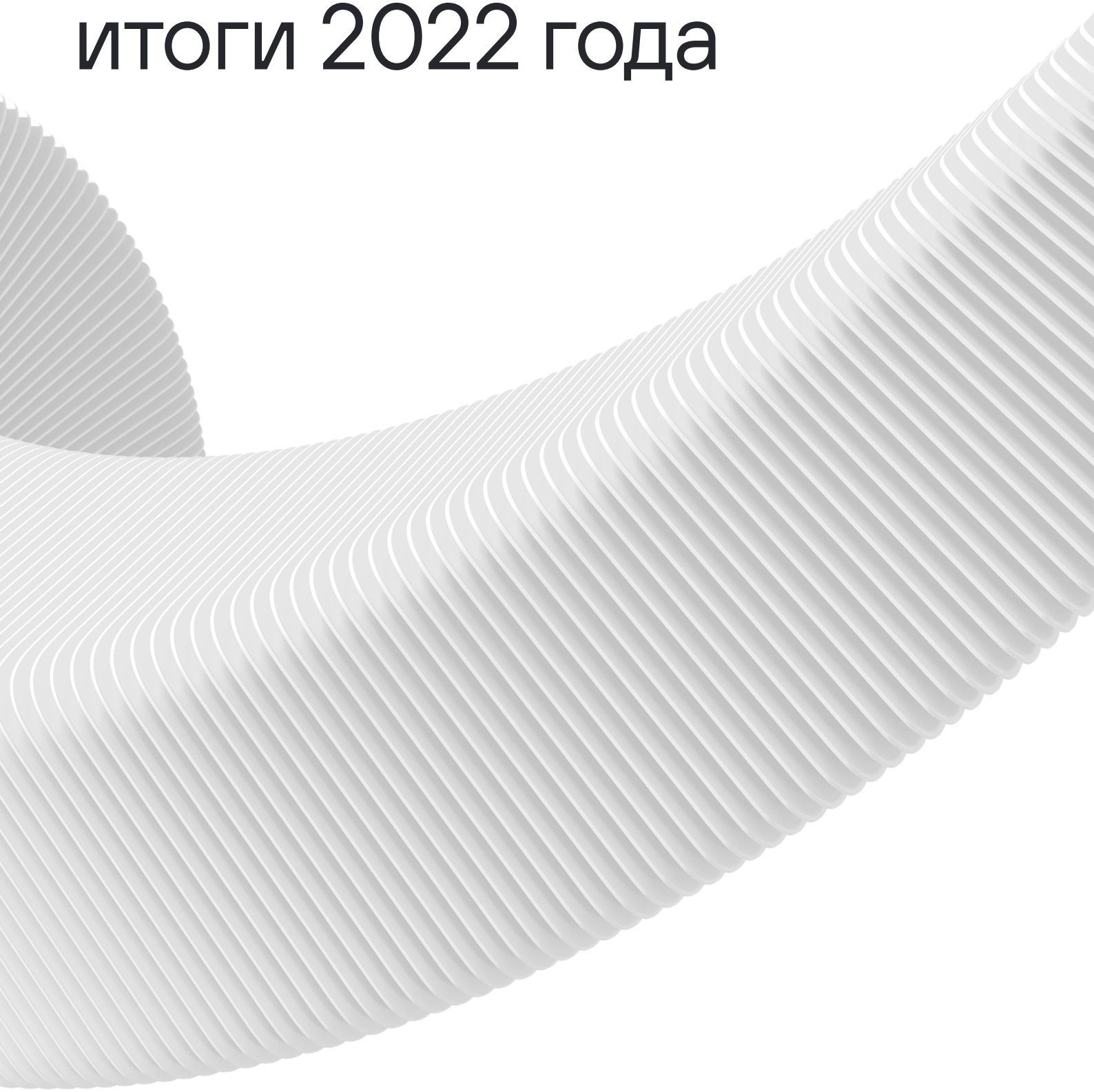
Актуальные киберугрозы: итоги 2022 года



Positive Technologies

ptsecurity.com

Содержание

Ключевые цифры и тренды

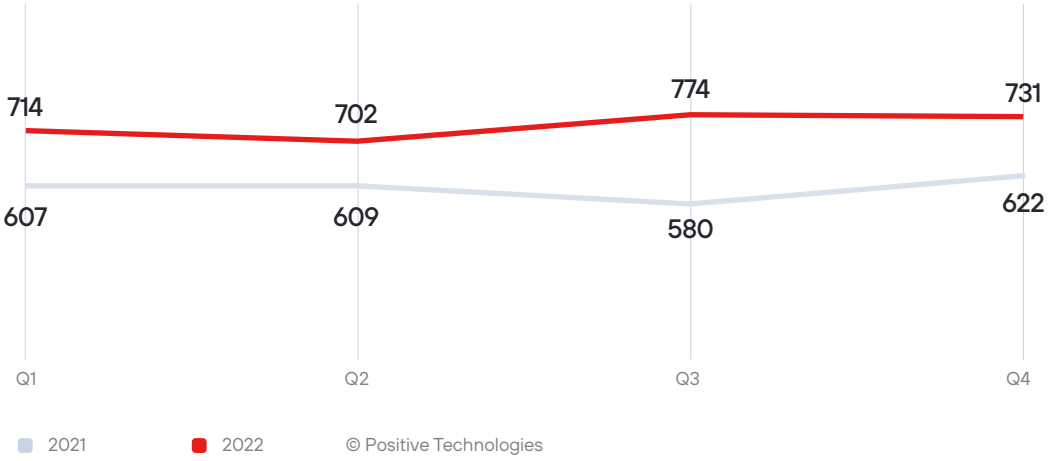
Общее количество инцидентов[1] в 2022 году увеличилось на 20,8%. Мы связываем это с возросшим напряжением в киберпространстве. Значительное влияние оказывает и рост рынка киберпреступности: злоумышленники расширяют теневой бизнес. Тем временем в связи с массовыми утечками данных появляется возможность проведения атак с использованием скомпрометированной информации о пользователях. В 2023 году эти же причины послужат еще большему росту числа атак.

[1] В исследовании мы учитываем только успешные кибератаки (инциденты), которые привели к негативным последствиям для компании или частного лица

67%

успешных атак имели целенаправленный характер

Рисунок 1. Количество инцидентов в 2021 и 2022 годах (по кварталам)



Ключевые тренды 2022 года

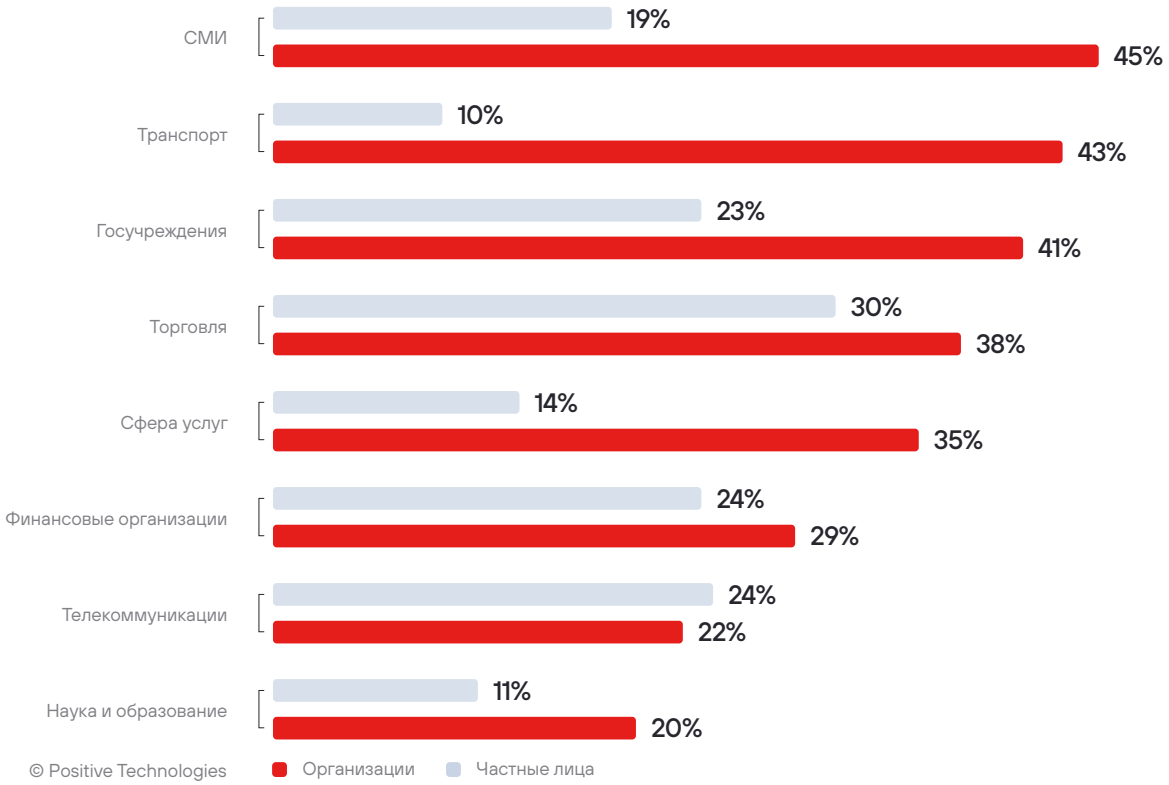
- Наблюдается прирост доли инцидентов, затронувших веб-ресурсы организаций: с 17% до 22% относительно итогов 2021 года. Наибольший удар пришелся на госучреждения: количество успешных атак, направленных на сайты, выросло более чем в два раза.
- Год прошел под знаком массовых утечек: в течение всего периода мы могли наблюдать множество сообщений о компрометации данных различных компаний и их клиентов. В атаках на организации злоумышленникам удалось украсть конфиденциальную информацию в 47% случаев, в атаках на частных лиц — в 64%.
- Растет количество инцидентов с применением шпионского ПО, особенно в атаках на частных лиц: к концу 2022 года эти вредоносы использовались в каждой второй успешной атаке на пользователей.
- Шифровальщики составили 51% используемого ВПО в атаках на организации и продолжают эволюционировать: в 2022 году еще больше группировок переписали используемое ВПО на кросс-платформенные языки или же создали версии, направленные как на Windows, так и на Linux-системы. В 2022 году мы отметили распространение вредоносов для удаления данных — вайперов; некоторые из них маскировались под шифровальщиков.

- Социальная инженерия по-прежнему на высоте (в успешных атаках на организации этот метод применялся в 43% случаев, на частных лиц — в 93%), в частности из-за распространения модели phishing as a service (фишинг как услуга). В атаках на частных лиц злоумышленники активно используют социальные сети и мессенджеры, а среди инцидентов, затронувших организации, отмечены успешные атаки на второй фактор аутентификации; эти тенденции могут усилиться в 2023 году.
- Атаки на IT-компании все чаще приводят к межотраслевым последствиям как за счет последующего взлома инфраструктуры клиентов, так и за счет нарушения бизнес-процессов клиентов из-за сбоев в работе сервисов.
- Криптовалюты продолжают набирать популярность, появляется все больше проектов, основанных на блокчейн-технологиях. Не отстают и злоумышленники: количество атак на блокчейн-проекты увеличилось более чем в два раза относительно показателя 2021 года.

Волна атак на веб-ресурсы

Число успешных атак, направленных на веб-ресурсы организаций, увеличилось на 56%. Если в 2021 году веб-ресурсы компаний становились объектами атак в 17% случаев, то в 2022 году доля таких инцидентов составила 22%. С ростом количества кибератак столкнулись организации многих отраслей, наибольший удар пришелся на госучреждения: количество инцидентов выросло более чем в два раза, а их доля повысилась с 23% до 41%.

Рисунок 2. Доля инцидентов, связанных с атаками на веб-ресурсы, в 2021 и 2022 годах



Наблюдаемое в 2022 году обострение противостояния в киберпространстве вызвало со стороны хактивистов волну атак, направленных на сайты организаций. Последствия таких нападений хорошо заметны и обычно затрагивают основные бизнес-процессы, если компания предоставляет сервисы онлайн. Инциденты с веб-ресурсами приводили к нарушениям деятельности организаций в 53% случаев. В основном злоумышленники старались сделать сайт недоступным или провести его дефейс. Кроме того, компрометация веб-ресурсов позволяет злоумышленнику осуществить массовую атаку на их посетителей, и в III квартале мы отмечали всплеск количества атак, направленных на сбор информации о пользователях: преступники встраивали вредоносный код в веб-страницы скомпрометированных ресурсов.

Прирост доли инцидентов преимущественно произошел в секторе СМИ, транспортной отрасли и госучреждениях в связи с атаками хактивистов, тогда как доля веб-атак, направленных на ритейл, и раньше была высокой: онлайн-магазины обрабатывают большие объемы информации о клиентах и потому всегда вызывают повышенный интерес киберпреступников. Так, злоумышленники могут встраивать в уязвимые сайты вредоносный код для перехвата персональных данных и данных платежных карт.

Увеличение числа атак на веб-ресурсы также обусловлено появлением уязвимостей, найденных, в частности, в популярных плагинах, таких как WordPress, Magento (плагин для e-commerce). Наиболее популярными среди злоумышленников уязвимостями веб-приложений оказались:

- CVE-2021–44228, или Log4Shell (в Apache Log4j 2);
- CVE-2022–22965, или Spring4Shell (в Java Spring Framework);
- CVE-2022–24086 (уязвимость в Adobe Commerce);
- CVE-2021–32648 (уязвимость в October CMS);
- CVE-2022–3180 (уязвимость в плагине WPGateway популярной CMS WordPress).

На рост количества кибератак значительно повлияло и расширение теневого рынка: появляются и открыто распространяются инструменты для эксплуатации уязвимостей и для проведения DDoS-атак. Мы ждем, что в 2023 году продолжит расти число атак на веб-ресурсы организаций, в особенности это коснется компаний, предоставляющих онлайн-услуги и собирающих большие объемы данных о клиентах.

Действия злоумышленников могут привести к реализации недопустимых для организации событий, и поэтому прежде всего необходимо оценить, какие бизнес-процессы зависят от работоспособности веб-приложений и как атака на веб-ресурсы может повлиять на деятельность организации и ее клиентов. Мы рекомендуем регулярно проводить анализ защищенности приложений и обновлять ПО в соответствии с сообщениями вендоров, использовать межсетевой экран уровня приложений. Кроме того, советуем внедрить процесс безопасной разработки веб-приложений.

Массовые утечки приводят к росту популярности социальной инженерии

Массовые утечки данных в 2022 году коснулись многих организаций и частных лиц как в России, так и во всем мире. В нескольких инцидентах пострадали такие известные компании и сервисы, как «Гемотест», «СДЭК», Яндекс.Еда, Delivery Club, DNS. Чаще всего злоумышленники похищали конфиденциальную информацию в медучреждениях (удалось украсть данные в 82% инцидентов), в организациях, занимающихся научными исследованиями или оказывающих образовательные услуги (67%), а также в ритейле (65%).

Ущерб от утечек во всем мире растет: согласно отчету IBM, в 2022 году средняя стоимость утечки данных достигла рекордно высокого уровня — 4,35 млн долларов, что на 2,6% больше, чем в прошлом году.

Злоумышленники скомпрометировали конфиденциальную информацию в 47% успешных атак на организации. Более трети украденной информации (36%) составили персональные данные; также интерес злоумышленников вызывала информация, относящаяся к коммерческой тайне (17%). Учетные данные составили 14% украденных данных. В успешных атаках, направленных на частных лиц, злоумышленникам удавалось украсть данные в 64% случаев. В основном были скомпрометированы учетные данные (41%), а также персональные (28%) и данные платежных карт (15%).

Наблюдается прирост доли персональных данных среди украденной информации относительно итогов 2021 года: для организаций — 4 процентных пункта (с 32% до 36%), для частных лиц — 8 п. п. (с 20% до 28%).

Рисунок 3. Типы украденных данных (в успешных атаках на организации)

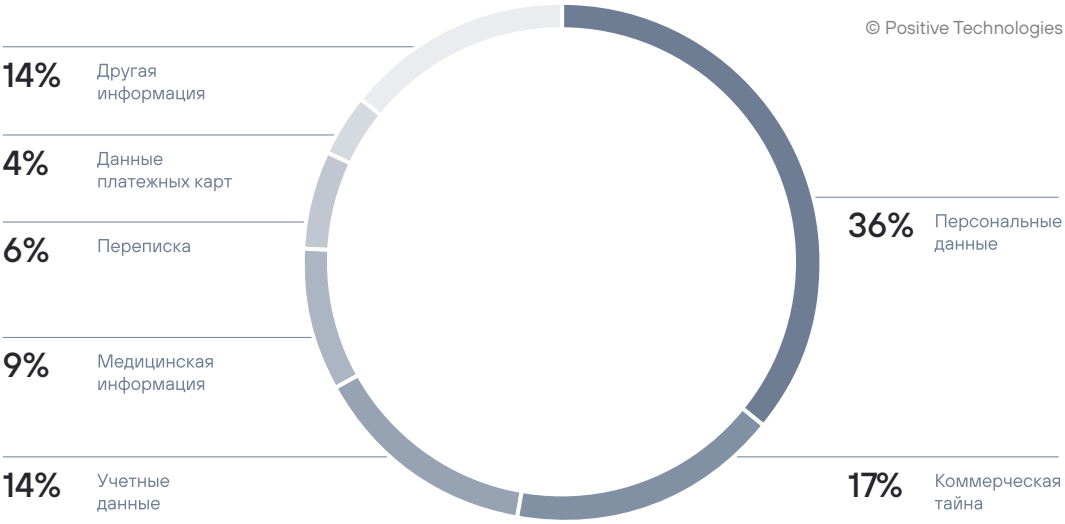
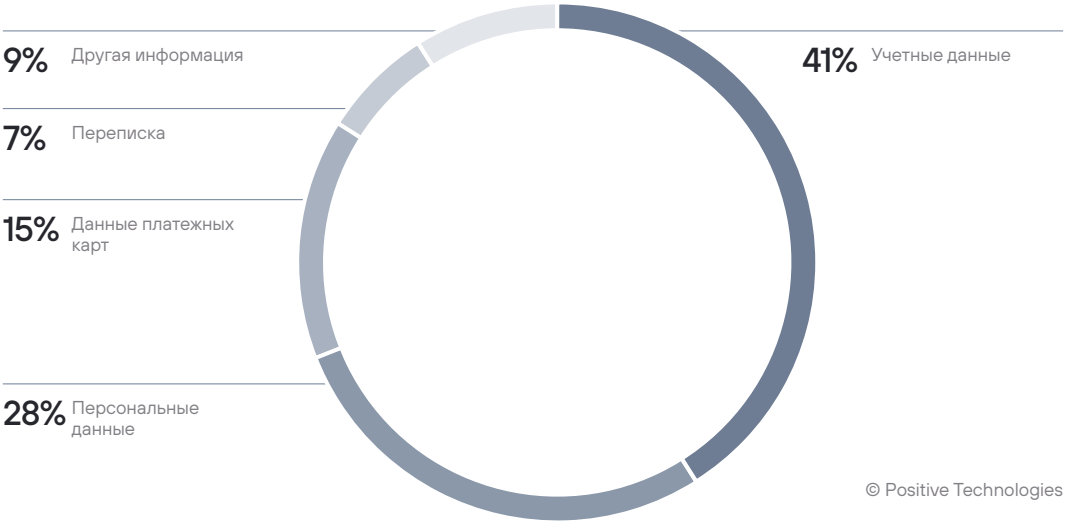


Рисунок 4. Типы украденных данных (в успешных атаках на частных лиц)



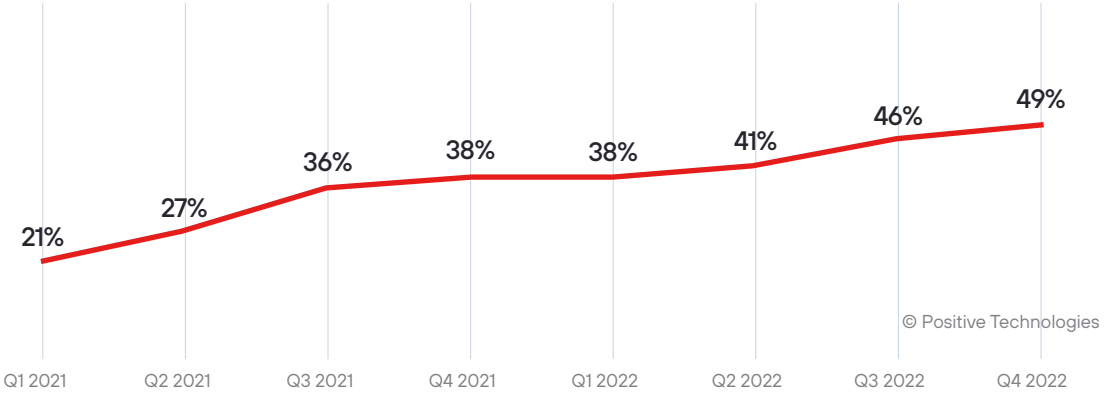
Архивы с украденными данными, как правило, продавались на теневых форумах. В будущем такие объемы данных позволяют злоумышленникам составлять цифровые портреты жертв и проводить более изощренные атаки с применением социальной инженерии.

Мы рекомендуем использовать в организациях инструменты мониторинга событий ИБ для обеспечения безопасности целевых и ключевых систем, а также контролировать внешние ресурсы — потенциальные точки проникновения. Важно своевременно информировать сотрудников о новых техниках атак злоумышленников, проводить учения для поддержания осведомленности в вопросах ИБ. Для каждой компании актуальны свои недопустимые события, связанные с утечкой разного рода информации, и мы советуем их верифицировать для оценки эффективности принятых мер.

Распространенность шпионского ПО растет

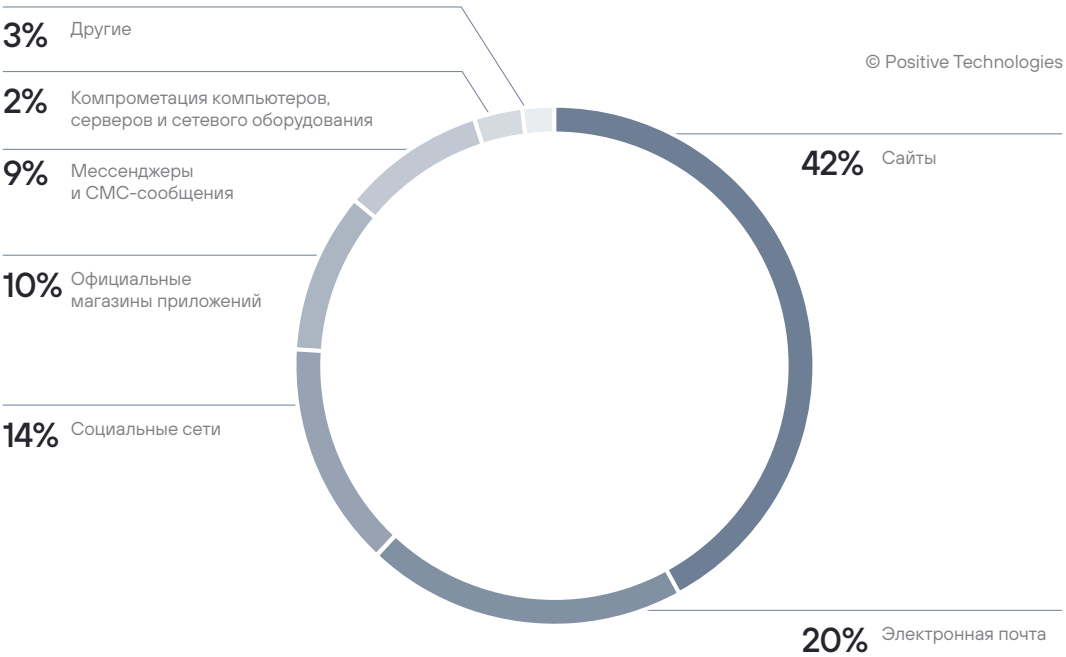
На протяжении года мы наблюдали рост доли использования шпионского ПО. В 2021 году этот показатель равнялся 12% в атаках на организации и 32% в атаках на частных лиц. И в 2022 году количество инцидентов, в которых использовалось шпионское ПО, постоянно увеличивалось: в результате доля этого типа ВПО составила 13% в атаках на организации и 43% в атаках на частных лиц.

Рисунок 5. Использование шпионского ВПО в атаках на частных лиц (доля успешных атак)



В атаках, направленных на частных лиц, шпионское ПО распространяется преимущественно через фишинговые сайты (42%). Традиционный вектор нападений — электронную почту — злоумышленники выбирали реже (20%). В то же время пользователям социальных сетей и мессенджеров стоит быть осторожнее: в 14% случаев для распространения вредоносов преступники выбирали социальные сети, а в 9% атаки проводились с помощью мессенджеров и СМС-сообщений. В 2022 году мы также могли наблюдать множество случаев обнаружения шпионского ПО в официальных магазинах приложений (10%). Большинство таких атак были нацелены на пользователей мобильных устройств под управлением Android.

Рисунок 6. Способы распространения шпионского ПО в успешных атаках на частных лиц



Наиболее используемыми вирусами-шпионами, по оценке экспертов Accenture, стали RedLine, Vidar и Raccoon Stealer. Появление новых игроков (BlueFox, Aurora, Erbium), регулярные обновления и распространение шпионского ПО по схеме malware as a service («ВПО как услуга») делают этот вид вредоносов популярным среди злоумышленников, а также значительно понижают порог вхождения в киберпреступность.

На рост числа атак с использованием шпионского ПО значительно влияет расширение теневого рынка. Еще в середине 2022 года мы проанализировали зрелость рынка криминальных киберуслуг в Telegram и выяснили, что среди вредоносов самыми обсуждаемыми стали ВПО для удаленного управления и шпионское ПО (суммарно на них приходится 48% сообщений на тему ВПО). Стоит отметить, что многие распространенные вредоносы для удаленного управления имеют и функции стилеров: это перехват СМС-сообщений, определение местоположения пользователя, запись экрана и многое другое. Цены на такое ВПО начинаются от 10 $, а некоторые из образцы шпионского ПО распространяются злоумышленниками бесплатно.

При проведении массовых атак преступники нацелены на сбор информации о пользователях и ее продажу на теневых площадках. Особую ценность имеют учетные данные для входа в различные сервисы, социальные сети и мессенджеры, а в связи с ростом популярности криптовалют практически каждый стилер обзавелся функцией перехвата данных для доступа к криптокошельку. Кроме того, в результате заражения устройства шпионским ПО злоумышленники могут скомпрометировать и корпоративные учетные данные в случае, если сотрудники подключаются к рабочим ресурсам с личных устройств.

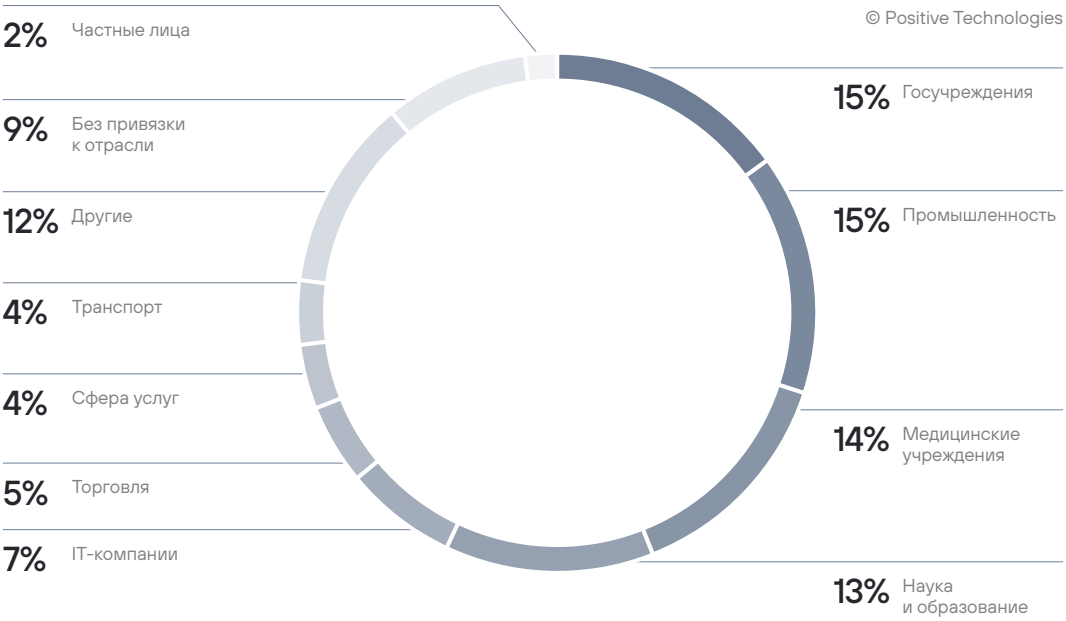
Как защитить свои данные? При загрузке приложения мы рекомендуем проверять информацию о разработчике, а также внимательно изучать отзывы других пользователей. В социальных сетях и мессенджерах помните о безопасности личной информации: не открывайте подозрительные вложения. Если скачиваете приложение с сайта, убедитесь в надежности ресурса.

Организациям стоит обратить внимание на обеспечение защиты личных устройств сотрудников, если гаджеты используются для подключения к корпоративным ресурсам. Вместе с тем мы советуем использовать антивирусное ПО, а подозрительные файлы проверять в песочнице — изолированной среде, предназначенной для анализа поведения файлов и выявления вредоносной активности.

Шифровальщики и вайперы

В 2022 году вымогатели остаются на волне популярности: злоумышленники использовали шифровальщики в каждой второй (51%) успешной атаке на организации с использованием ВПО. В качестве жертв операторы шифровальщиков чаще всего выбирали госучреждения (15%), промышленные предприятия (15%), медицинские организации (14%), научные и образовательные учреждения (13%)

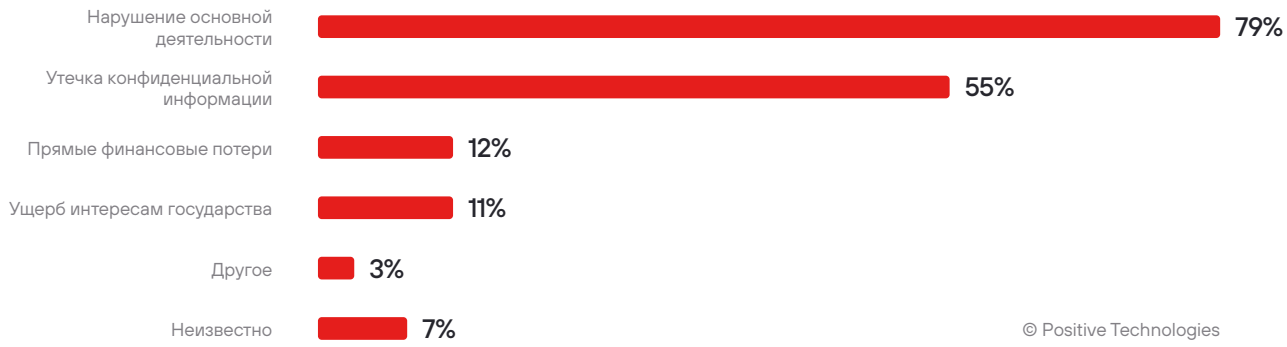
Рисунок 7. Распределение инцидентов с использованием шифровальщиков по отраслям



В 8 из 10 инцидентов с участием шифровальщиков основная деятельность организаций была нарушена: наблюдались потери доступа к инфраструктуре и данным, сбои в предоставлении сервисов клиентам, нарушения внутренних бизнес-процессов. В результате 55% инцидентов у организаций была украдена конфиденциальная информация, преимущественно персональные данные и коммерческая тайна. В 12% случаев жертвы понесли финансовые потери: выплаты выкупа и убытки из-за простоя.

По данным аналитиков Chainalysis, в 2022 году прибыль группировок вымогателей сократилась на 40%. Одна из причин заключается в том, что жертвы все чаще отказывают злоумышленникам в уплате выкупа: исследование Coveware показало, что за последние четыре года доля заплативших выкуп сократилась практически вдвое — с 76% в 2019 году до 41%.

Рисунок 8. Последствия атак шифровальщиков (доля успешных атак)



В 2022 году наиболее заметной была деятельность следующих групп вымогателей, использующих одноименные шифровальщики:

- LockBit — одна из самых активных группировок вымогателей. Пережила несколько итераций обновления своего ВПО, которое также имеет кросс-платформенное исполнение. Отличается тщательностью отбора как аффилированных лиц, так и жертв.
- Hive — отличается особо агрессивным типом поведения, атакует объекты КИИ разных стран, а также социально значимые объекты (больницы, транспорт, полиция). В начале 2023 года ФБР взломало серверы злоумышленников, а также был обнародован дешифратор.
- Vice Society — вымогатели, активные с 2021 года, основными целями которых являются образовательные и научные учреждения, а также медицинские организации.
- BlackCat (ALPHV) — относительно новая, но не менее грозная группа вымогателей, последовательно атакующая крупные организации. Является продолжением DarkSide и BlackMatter, имеет обширный опыт в вымогательстве и одной из первых использовала язык Rust для создания кросс-платформенной версии своего вредоноса.
- Conti — долгоживущая угроза, являвшаяся лидером рынка ransomware as a service (программа-вымогатель как услуга) до ухода со сцены в мае 2022 года из-за преследования спецслужбами и распада на более мелкие формирования.

В 2021 году мы отмечали укрепившийся интерес вымогателей к системам на базе Linux, и закономерным трендом 2022 года стал переход группировок на кросс-платформенные версии вредоносного ПО с использованием языка Rust. Такие экземпляры позволяют нацеливаться как на Linux-системы, так и на Windows, а вследствие малого количества экспертизы средствам защиты труднее зафиксировать использование вредоносов. Среди крупных игроков кросс-платформенными решениями обзавелись RansomEXX, Black Basta, Hive.

При проведении атак вымогатели делают основную ставку на скорость и внезапность: им нужно скомпрометировать как можно больше устройств в сжатые сроки, запустить на них вредонос и дать ему время зашифровать максимальное количество информации. Трендом 2022 года стало использование прерывистого шифрования файлов с определенным побайтовым шагом. Процесс становится быстрым и менее заметным для средств мониторинга подозрительной активности за счет меньшего количества операций над шифруемым файлом и его схожести с оригиналом. Занимательный подход использовала группировка BlackCat: злоумышленники пропустили этап шифрования и использовали инструмент эксфильтрации данных для передачи их на удаленный сервер и для повреждения локальных экземпляров файлов. Такой подход быстрее, менее трудозатратен и гарантирует то, что жертва будет заинтересована в переговорах, так как восстановить файлы нельзя, а рабочие копии находятся у злоумышленников в единственном экземпляре.

Кроме того, в 2022 году были замечены случаи утечек исходных кодов известных шифровальщиков, например Conti и Yanluowang. Это может привести к тому, что в 2023 году рост числа атак вымогателей замедлится, поскольку у исследователей безопасности появляется возможность более тщательного анализа кода вредоносов и используемых техник. В то же время могут сформироваться новые группировки вымогателей, способные использовать утекший исходный код вредоносного ПО для разработки собственных образцов шифровальщиков и применения их в реальных атаках.

Распространение вайперов

Рост количества инцидентов с применением ПО для удаления данных — вайперов — составил 175% по сравнению с прошлым годом. Наибольшее распространение вайперы получили в первом полугодии: тогда были выявлены случаи использования HermeticWiper (Foxblade), DoubleZero, IsaacWiper и других образцов.

Спустя некоторое время появилась новая вариация вайперов, которые маскировались под программы-шифровальщики и требовали выкуп за восстановление информации. Однако ключи для дешифрования не предоставлялись, а сами данные могли шифроваться случайным образом. Восстановление, особенно если ВПО затронуло множество систем, может занять большое количество времени. Особую угрозу представляют вайперы, нацеленные на промышленные организации, так как их применение может вызвать остановку важнейших технологических процессов и аварии на производстве. Стоит отметить, что атаки вайперов ранее часто были направлены на системы под управлением Windows, однако в 2022 году были выявлены образцы вредоносов, угрожающих системам на базе Linux.

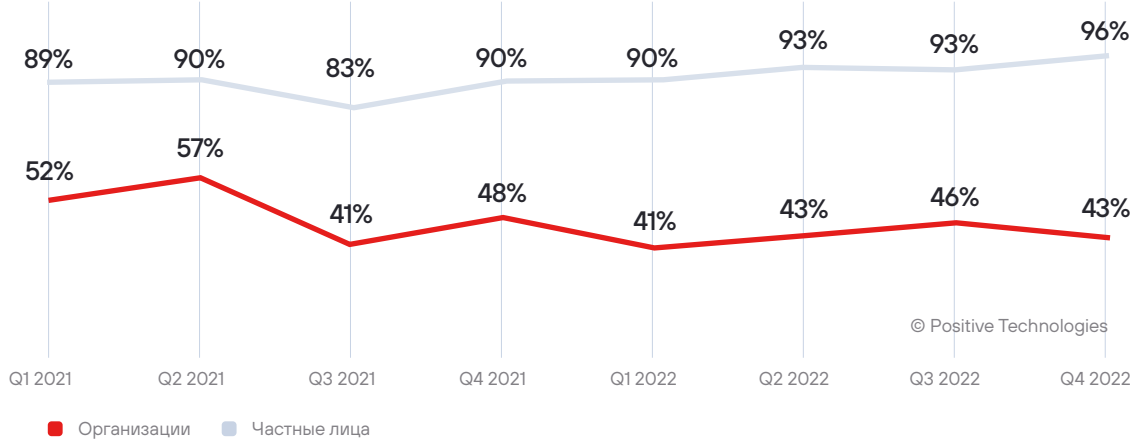
Для защиты от атак с использованием шифровальщиков и ПО, удаляющего данные, мы рекомендуем:

- использовать решения для резервного копирования данных. В случае успешной атаки специалисты смогут быстро восстановить данные и системы из автономных резервных копий (желательно хранить их на серверах вне сетевого периметра офиса);
- использовать антивирусные средства и песочницы;
- вести мониторинг сетевой активности и активности на конечных узлах;
- устанавливать обновления безопасности и оперативно реагировать на инциденты ИБ;
- иметь план восстановления IT-инфраструктуры.

Социальная инженерия: под угрозой многофакторная аутентификация

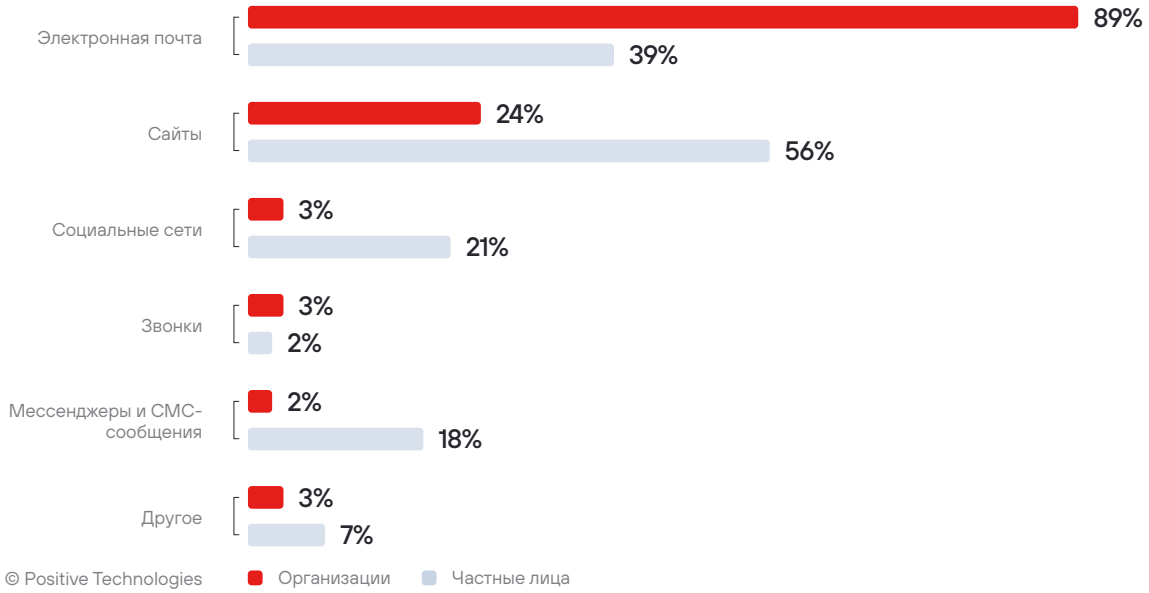
Доля инцидентов с использованием социальной инженерии увеличилась с 88% до 93% в атаках на частных лиц относительно результатов 2021 года. В атаках на организации количество инцидентов остается на прежнем уровне, однако доля использования метода снизилась с 50% до 43%: на фоне многочисленных утечек информации у злоумышленников появляется возможность проводить атаки с использованием скомпрометированных данных, в том числе учетных. В 2022 году в 16% успешных атак, направленных на организации, преступникам удалось получить доступ к целевым системам и ресурсам с помощью компрометации учетных данных. Это могло быть достигнуто как посредством подбора паролей, так и с помощью учетных данных, скомпрометированных в результате утечек.

Рисунок 9. Доля инцидентов с использованием социальной инженерии



Почти в 9 из 10 успешных атак на организации, в которых использовалась социальная инженерия, злоумышленники отправляли вредоносные письма по электронной почте. В атаках на частных лиц мошенники в основном использовали фишинговые сайты (56%), также в течение года мы отмечали рост количества успешных атак через мессенджеры и СМС-сообщения (18%), социальные сети (21%).

Рисунок 10. Используемые злоумышленниками каналы социальной инженерии



В 2022 году активно распространялась модель phishing as a service: злоумышленники используют в атаках готовые фишинговые комплекты, при этом в некоторых из инцидентов использовались инструменты для обхода многофакторной аутентификации. Например, в конце года был отмечен всплеск атак типа MFA Fatigue: в них злоумышленники выполняли множественные попытки входа в аккаунт, используя украденные учетные данные, вызывая бесконечный поток пуш-уведомлений МФА, отправляемых на мобильное устройство владельца учетной записи. В конечном итоге часть пользователей могли подтвердить вход на ресурс, чтобы остановить поток сообщений. В будущем мы ждем увеличения числа атак, направленных на обход второго фактора аутентификации.

Для защиты мы рекомендуем устанавливать лимит на количество попыток входа, при превышении которого следует осуществлять временную блокировку учетной записи. Кроме того, при наличии большого количества уведомлений (если не вы совершаете попытки входа) необходимо сообщить об инциденте сотруднику, отвечающему за информационную безопасность, поскольку это говорит о вероятной компрометации ваших учетных данных. Частным лицам мы рекомендуем быть внимательнее в социальных сетях и мессенджерах: не стоит переходить по подозрительным ссылкам и сообщать собеседнику личную информацию, а также переводить средства, если не уверены в надежности адресата.

Атаки на IT-компании приводят к межотраслевым последствиям

На протяжении 2022 года количество успешных атак, направленных на IT-компании, постепенно росло, и в IV квартале их число почти вдвое превысило показатели I квартала 2022 года. Чаще всего инциденты приводили к утечкам конфиденциальной информации (63%), нарушению основной деятельности (35%), использованию ресурсов компании для проведения атак (13%).

Рисунок 11. Последствия атак на IT-компании (доля успешных атак)

Скомпрометированная конфиденциальная информация в основном включала коммерческую тайну (31%): преимущественно это были многочисленные утечки исходного кода IT-продуктов. Так, в начале года мы наблюдали серию атак группировки Lapsus$, направленную на кражу информации из Globant, Microsoft, Nvidia, Samsung. Скомпрометированные данные впоследствии использовались злоумышленниками: например, украденными сертификатами Nvidia преступники подписывали ВПО, чтобы оно выглядело легитимным.

Решения, предлагаемые IT-компаниями, повсеместно используются другими организациями и частными лицами. Поэтому нарушение деятельности IT-компании может привести к негативным последствиям в отношении клиентов: например, в 46% таких инцидентов у организаций наблюдались сбои в предоставлении сервисов. В ряде успешных атак вмешательство преступников приводило к невозможности работы других организаций из различных отраслей — от медицинских и государственных учреждений до железнодорожных компаний. В некоторых случаях злоумышленники атаковали пользователей через поставщиков IT-продуктов и услуг. Так, на протяжении года компания Okta, предоставляющая решения для многофакторной аутентификации, подверглась серии успешных атак. В результате одной из них злоумышленники смогли получить доступ к данным более 300 клиентов компании.

Кроме того, в 2022 году продолжались атаки на облачные сервисы и на среды виртуализации. В атаках на разработчиков злоумышленники активно распространяли ВПО через библиотеки для популярных фреймворков.

В 2023 году мы ждем продолжения атак на цепочки поставок ПО, а также атак, направленных на компрометацию клиентов IT-компаний. Разработчикам IT-решений необходимо верифицировать такие недопустимые события и предусматривать меры защиты. Мы рекомендуем регулярно анализировать код на безопасность, проверять используемые при разработке сторонние библиотеки, а участие в программах багбаунти позволит находить уязвимости в продуктах и оперативно устранять их.

Рост атак на блокчейн-проекты

Как мы и предполагали ранее, в 2022 году интерес злоумышленников к криптобиржам и DeFi-протоколам значительно вырос: количество атак на блокчейн-проекты увеличилось более чем в два раза по сравнению с 2021 годом. В 78% инцидентов злоумышленникам удалось похитить средства, при этом ущерб в некоторых случаях составлял несколько сотен миллионов долларов. По данным Chainalysis, 2022 год стал самым крупным годом по размеру ущерба: у криптовалютных компаний было украдено 3,8 млрд долларов. Крупнейшими можно считать следующие взломы:

1. Сайдчейн Ronin (украдено 617 млн долларов).
2. BSC Token Hub (украдено 566 млн долларов).
3. Wormhole (украдено 326 млн долларов).

Чаще всего злоумышленники эксплуатировали уязвимости смарт-контрактов (78%), причем особую популярность имели атаки мгновенного кредита (flash loan attacks)[2].

Вместе с этим растет и число атак, направленных на владельцев криптовалютных активов. Злоумышленники распространяют в социальных сетях и мессенджерах сообщения о бесплатных раздачах токенов и NFT, а также предлагают перевести средства, обещая вернуть намного больше. Тем временем практически каждый из стилеров уже обзавелся функцией кражи учетных данных известных криптокошельков.

Мы ждем, что в 2023 году количество атак на блокчейн-проекты продолжит расти, а также увеличится число случаев мошенничества, направленного на владельцев криптовалютных активов.

[2] Атака мгновенного кредита — это эксплуатация уязвимости смарт-контракта определенной платформы. Злоумышленник занимает большую сумму средств, не требующих залога, и затем использует ее для проведения операций на бирже, искусственно завышая или занижая цены на криптовалюты. Все действия проводятся в рамках одной транзакции.

Мы рекомендуем пользователям быть предельно внимательными при получении сообщений с предложениями, обещающими большую выгоду, внимательно изучать информацию о проектах, защищать аккаунты на криптовалютных биржах и кошельки с помощью двухфакторной аутентификации.

Разработчикам рекомендуется проводить аудит смарт-контрактов, внедрять процессы безопасной разработки, а также участвовать в программах багбаунти для выявления уязвимостей.

Сводная статистика

17%

успешных атак были направлены на частных лиц

Рисунок 12. Категории жертв среди организаций

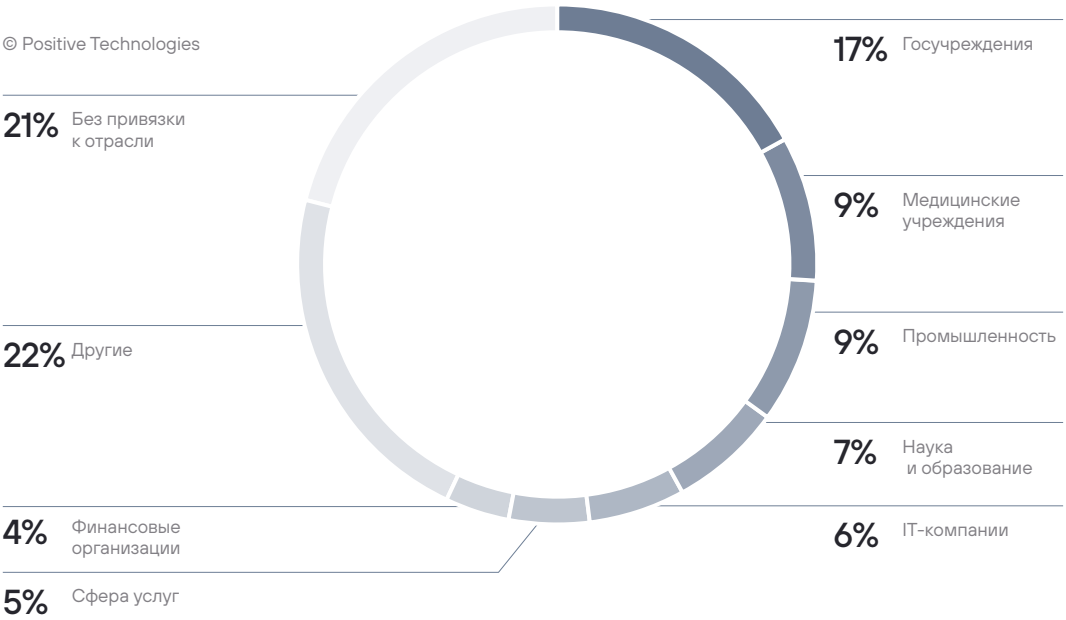


Рисунок 13. Последствия атак (доля успешных атак)

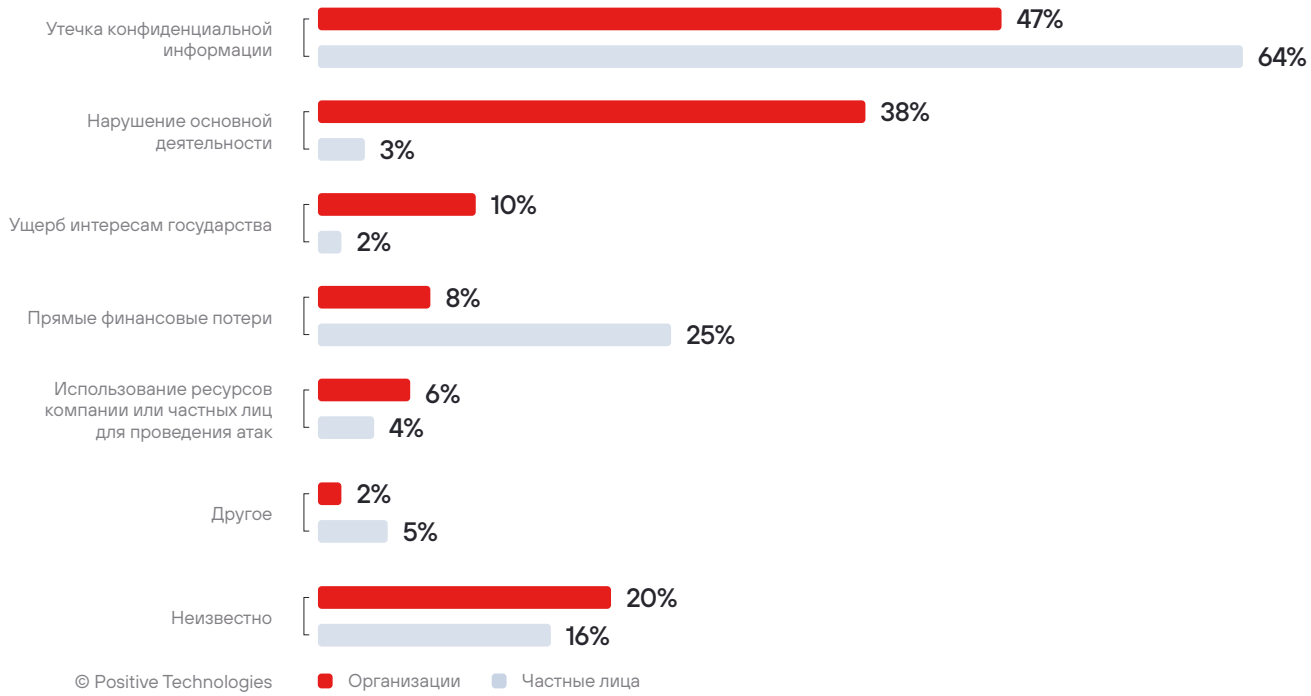


Рисунок 14. Объекты атак (доля успешных атак)

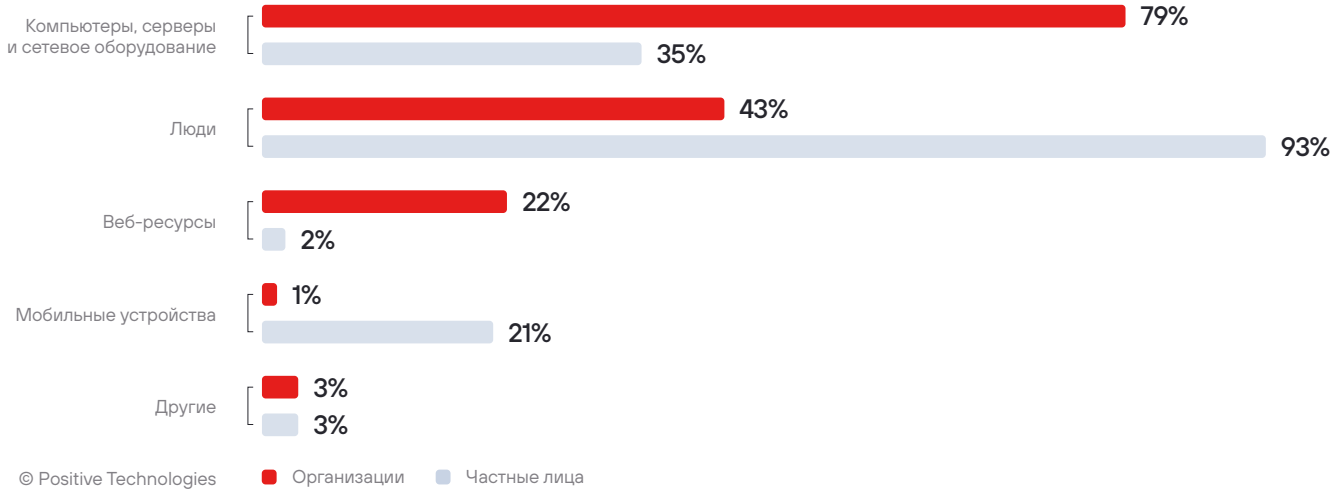


Рисунок 15. Методы атак (доля успешных атак)

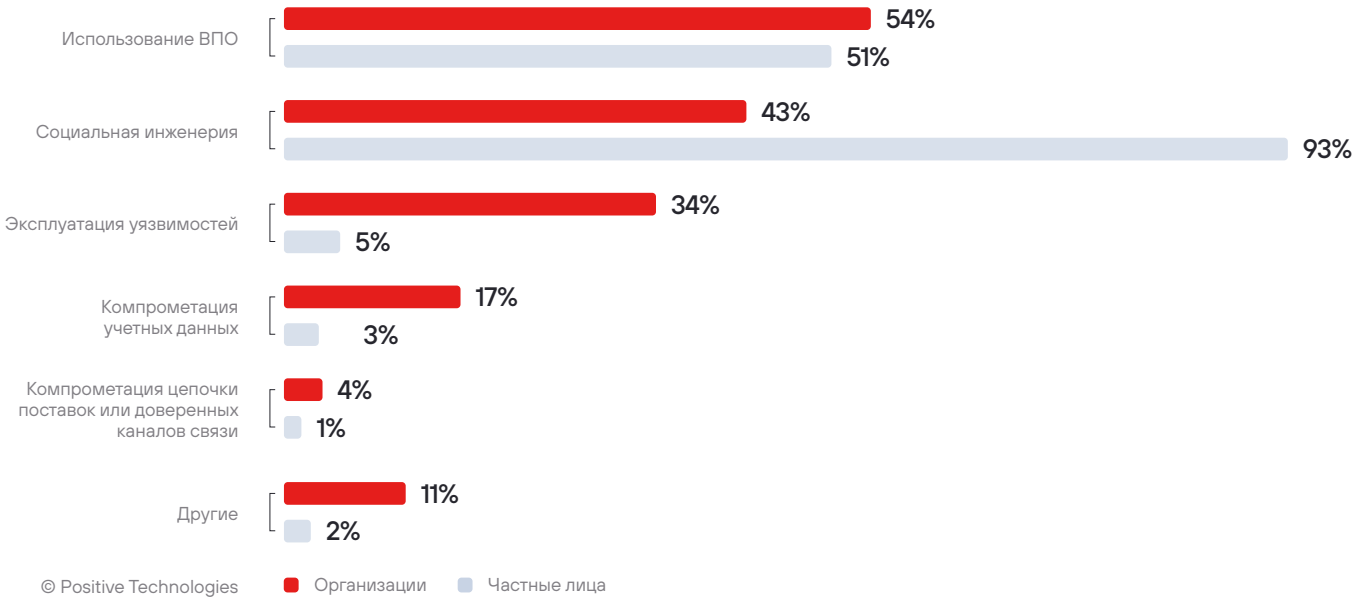


Рисунок 16. Типы вредоносного ПО (доля успешных атак с использованием ВПО)

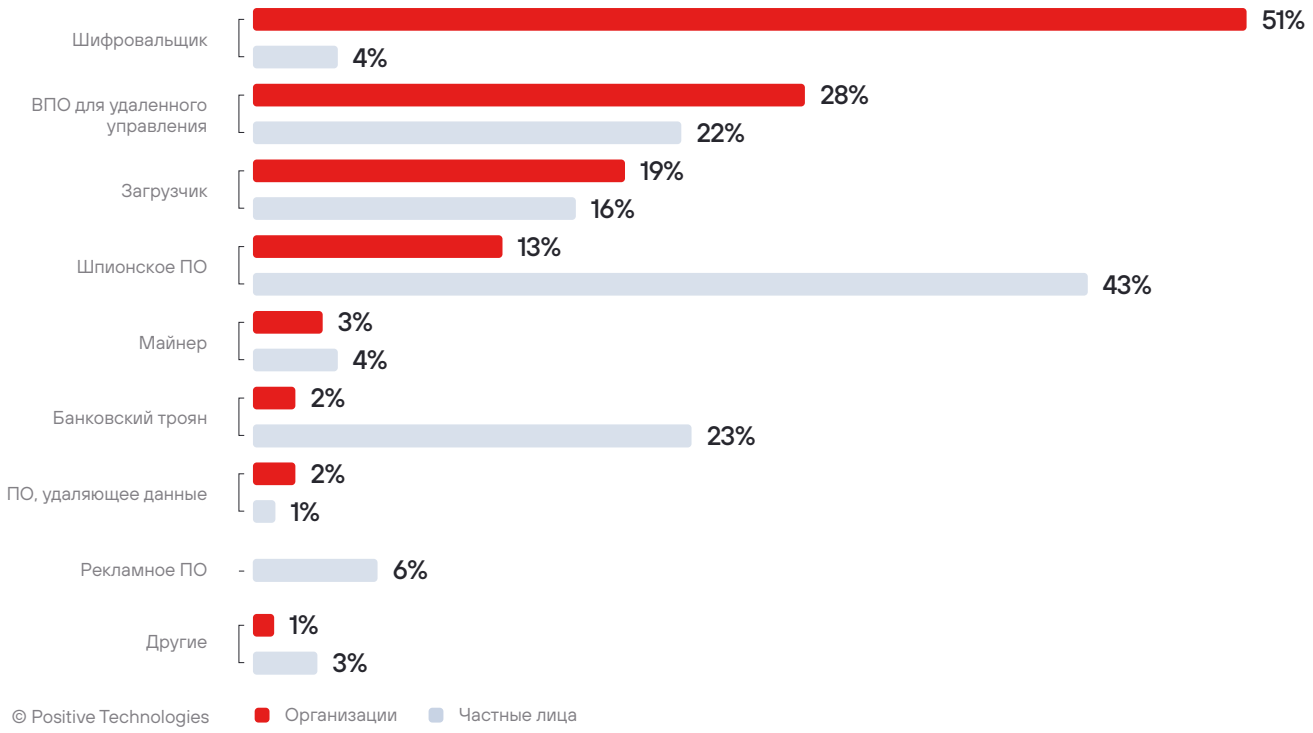


Рисунок 17. Способы распространения вредоносного ПО в успешных атаках на организации

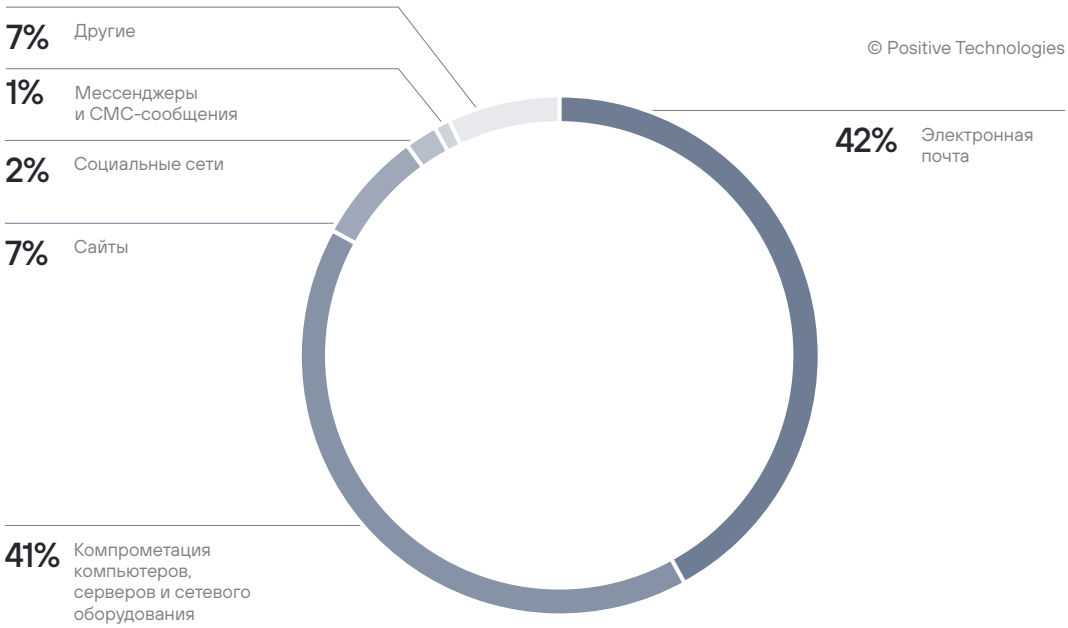


Рисунок 18. Способы распространения вредоносного ПО в успешных атаках на частных лиц

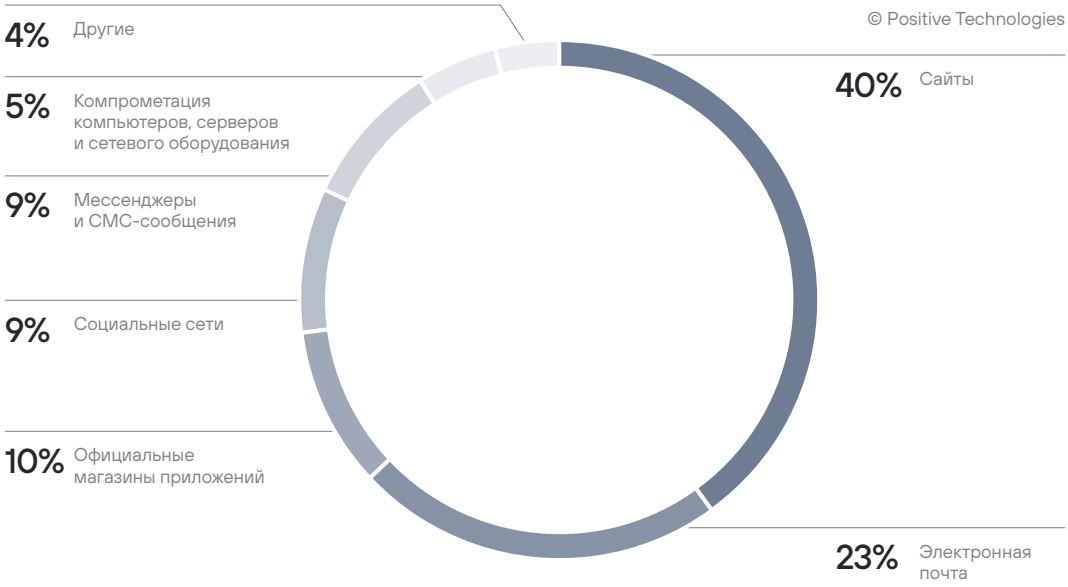
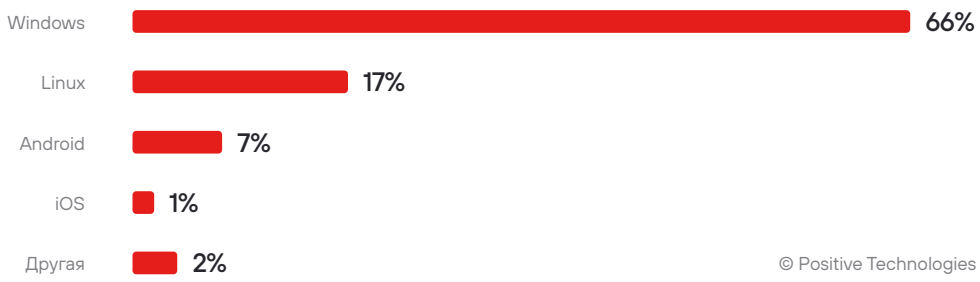


Рисунок 19. Целевые ОС в атаках с использованием ВПО (доля успешных атак)



	Распределение киберинцидентов по метрикам (объекты атак, методы, последствия) и категориям жертв	Категории жертв									
		Госучреждения	Промышленность	Наука и образование	Сфера услуг	IT-компании	Медицинские учреждения	Финансовые организации	Другие	Без привязки к отрасли	Частные лица
	Всего атак	403	223	170	113	136	228	105	528	511	504
Объект	Компьютеры, серверы и сетевое оборудование	289	193	150	70	114	194	92	378	435	177
	Веб-ресурсы	165	26	34	40	20	13	30	161	50	11
	Люди	164	99	100	44	42	118	50	162	265	468
	Мобильные устройства	4	—	1	—	—	1	1	4	10	105
	Другой	5	5	2	—	3	1	2	31	12	17
Метод	Использование ВПО	190	159	124	30	86	121	53	212	337	255
	Социальная инженерия	164	99	100	44	42	118	50	162	265	468
	Компрометация учетных данных	51	47	43	20	47	58	16	81	38	16
	Эксплуатация уязвимостей	106	92	35	40	47	57	28	196	224	26
	Компрометация цепочки поставок	19	5	6	3	7	9	1	18	18	6
	Другой	98	4	5	11	5	2	16	91	39	10
Последствие	Нарушение основной деятельности	206	104	100	29	48	77	43	232	78	14
	Утечка конфиденциальной информации	141	121	114	71	85	187	56	201	165	323
	Ущерб интересам государства	164	13	2	—	1	1	2	63	4	11
	Прямые финансовые потери	15	17	6	7	9	10	6	83	39	124
	Использование ресурсов организаций или частных лиц для проведения атак	9	3	5	13	18	4	6	21	69	18
	Другое	1	3	4	1	2	3	—	12	28	23
	Неизвестно	85	46	24	10	16	9	28	69	200	80

Градацией цвета показаны доли атак внутри одной метрики для каждой категории жертв

0%	10%	20%	30%	40-100%

Об исследовании

Представленный отчет содержит информацию об общемировых инцидентах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах расследований, а также на данных авторитетных источников.

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. Термины, которые мы используем в исследовании, приведены в глоссарии на сайте Positive Technologies.

ptsecurity.com
pr@ptsecurity.com