Актуальные киберугрозы: I квартал 2023 года

Positive Technologies

ptsecurity.com

Содержание

Ключевые цифры и тренды 3

Увеличение случаев использования загрузчиков 3

SEO poisoning 3

Всплеск активности вымогателей 4

QR-фишинг: быстро и незаметно 5

Новые веяния криптовалютного мошенничества 6

Облачные сервисы как плацдарм для фишеров 6

Аресты киберпреступников и закрытие дарквеб-форумов 6

Актуальные уязвимости 7

Последствия атак 8

Сводная статистика 11

Об исследовании 16

Ключевые цифры и тренды

В I квартале 2023 года количество инцидентов увеличилось на 7% по сравнению с показателем предыдущего квартала и стало на 10% больше, чем в начале 2022 года. Наиболее частыми последствиями успешных кибератак на организации стали утечки конфиденциальной информации (51%) и нарушения основной деятельности (44%). Злоумышленники чаще использовали вредоносное программное обеспечение (ВПО) против организаций и частных лиц: доля таких инцидентов увеличилась на 7 и 10 процентных пунктов по сравнению с прошлым кварталом соответственно. Наблюдались крупные перебои в работе бизнеса и критически значимой инфраструктуры, масштабные утечки данных, появились новые схемы обмана пользователей.

Увеличение случаев использования загрузчиков

Мы отмечаем рост числа атак с использованием загрузчиков: доля применения этого вредоносного ПО в атаках на организации (21%) и частных лиц (23%) выросла на 2 и 8 п. п. соответственно. Это обусловлено массовыми фишинговыми кампаниями вымогателей Black Basta, BlackCat, Ragnar Locker и других злоумышленников, которые использовали перепрофилированные в загрузчики вредоносы Qbot и Emotet в качестве полезной нагрузки первого этапа. Такие программы закрепляются в системе, скачивают ПО для удаленного доступа, собирают локальные учетные данные и только после этого загружают шифровальщики. Распространяя Emotet через электронную почту (наиболее популярный канал социальной инженерии для организаций, 86%), преступники прикрепляли к письму искусственно «утяжеленные» документы или архивы размером более 500 МБ, чтобы обойти антивирусную защиту. Ограничение размера файлов для повышения производительности сканирования — распространенная практика. Такой же прием использовался в кампании по распространению стилера[1] RedLine. Из-за блокирования файлов с макросами[2], полученных из интернета, злоумышленники возвращаются к письмам с вложенными вредоносными ISO-образами дисков и LNK-файлами.

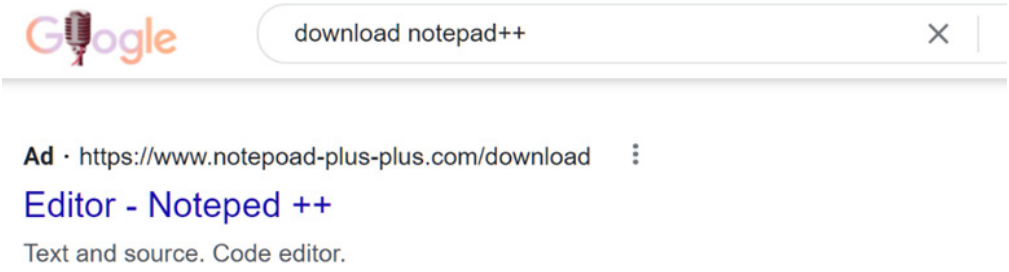
[1] Стилер — вредоносное программное обеспечение, предназначенное для кражи конфиденциальной информации (например, логинов, паролей, данных криптовалютных кошельков) с зараженного устройства.

SEO poisoning

Мы отметили увеличение количества вредоносной рекламы в поисковых системах (отличительная черта атаки SEO poisoning) в течение I квартала 2023 года, о чем также сообщили специалисты SentinelOne. Суть метода заключается в использовании поисковой оптимизации (SEO, search engine optimization) для опережения выдачи незаконного домена над законным. Кроме того, этот способ атаки может применяться для привлечения большого числа пользователей на сайты и для мошенничества с рекламой.

[2] Макрос — небольшая программа, выполняющая заранее заданный набор действий в приложении.

Рисунок 1. Вредоносная реклама в поисковой выдаче Google



В I квартале замечены подставные веб-ресурсы, которые распространяли вредоносное ПО под видом законного через сеть доставки контента (CDN, content delivery network) Discord и Dropbox: злоумышленники маскировали популярные инфостилеры RedLine и Raccoon под популярные продукты (например, Blender и OBS Studio), что приводило к утечке учетных данных, краже денежных средств и NFT-токенов.

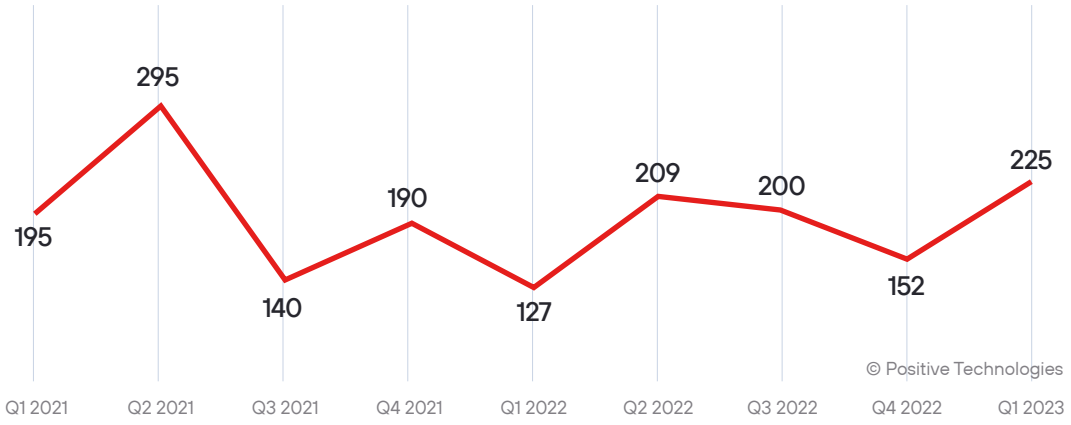
Еще один вид таких атак — распространение сайтов с фишинговыми формами входа в поисковой выдаче. Обман пользователей Amazon Web Services был замечен специалистами Permiso.

Всплеск активности вымогателей

Активность вымогателей в I квартале 2023 года значительно возросла: доля использования шифровальщиков в атаках на организации с использованием ВПО составила 53%, что на 9 п. п. больше показателя прошлого квартала, а число инцидентов выросло на 77% относительно начала 2022 года. Особенно напряженная обстановка наблюдается в секторе науки и образования — на него пришлась немалая доля атак вымогателей (19%): на прицеле злоумышленников были школы и ряд высших учебных заведений по всему миру ([1],[2]).

Новшества продемонстрировали вымогатели BlackCat и HardBit. Первые начали выкладывать похищенные данные на сайты с адресами, похожими на домен скомпрометированной организации, чтобы факт утечки мог стать известен широкому кругу клиентов или партнеров компании. Вторые пытались убедить жертву раскрыть детали киберстрахования, чтобы скорректировать требования выкупа и гарантированно получить выплату от страховщика (о ценности информации о киберстраховании мы писали ранее). Продолжающийся тренд — разработку кросс-платформенных версий вредоносов — подхватили уже известные вымогатели Royal, IceFire и Cl0P, а также новички из Nevada Ransomware.

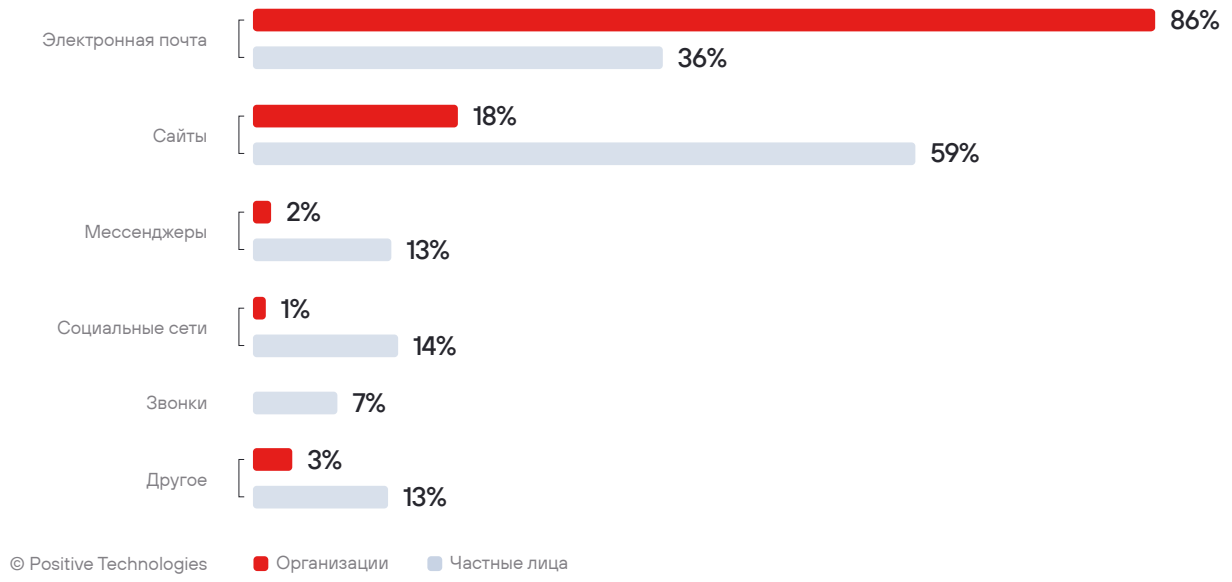
Рисунок 2. Количество атак вымогателей



QR-фишинг: быстро и незаметно

Социальная инженерия остается одним из наиболее популярных методов атак на организации (50%) и частных лиц (91%). Основным каналом социальной инженерии в атаках на организации является электронная почта (86%), а на частных лиц — веб-ресурсы и сервисы (59%).

Рисунок 3. Используемые злоумышленниками каналы социальной инженерии



В I квартале замечено увеличение числа фишинговых писем на темы, связанные с трудоустройством, увольнением, получением льгот и пособий. В таких кампаниях злоумышленники отправляют письма с вредоносными вложениями (стилерами, похищающими учетные данные) либо размещают в письмах ссылки на фишинговые формы входа, например, в Microsoft 365 или Amazon Web Services. Помимо писем с вредоносными ссылками и вложениями атакующие использу-

ют QR-коды, чтобы обойти антиспам-фильтры и другие средства защиты, так как коды являются изображениями и не содержат подозрительных ссылок или отличительных метаданных (по этой причине число подобных фишинговых кампаний может увеличиться).

Новые веяния криптовалютного мошенничества

Для мошенничества злоумышленники создавали сайты с несуществующими криптовалютами, рекламировали их среди потенциальных инвесторов, обзванивали их с якобы уникальными выгодными предложениями после чего получали деньги и исчезали. Несколько таких мошеннических центров закрыты Европолом, а их прибыль исчислялась миллионами в криптовалюте. Кроме того, исследователи Sophos сообщали о поддельных приложениях, распространяемых через официальные магазины: криптоинвесторы предоставляли персональные данные для регистрации и переводили деньги не на свои счета, а на счета преступников. Эти приложения сложно отследить: их вредоносный контент находится не в коде, а на удаленном веб-сервере.

Облачные сервисы как плацдарм для фишеров

Обилие схем мошенничества подстегивает пользователей быть начеку, но что, если сообщения или ссылки приходят от авторитетных источников? Мошенники размещают свои фишинговые ресурсы в доменах облачных сервисов (software as a service, SaaS), чтобы не вызвать подозрений у пользователя и остаться незамеченными для средств защиты. Исследователи Palo Alto Networks сообщили, что количество фишинговых страниц, размещенных на облачных платформах, увеличилось более чем в десять раз с середины 2021 года. Злоумышленники используют такие ресурсы, как Dropbox или OneDrive, для распространения вредоносов из-за того, что средства защиты не всегда срабатывают на файлы, полученные из этих сервисов.

Аресты киберпреступников и закрытие дарквеб-форумов

Отличительной чертой I квартала стала повышенная активность правоохранительных органов и спецслужб в отношении представителей киберпреступного мира. Если ранее деятельность злоумышленников пытались пресечь или осложнить преимущественно в правовом поле, то сейчас правоохранители переходят к активным действиям:

- После продолжительной операции правоохранительные органы Голландии объявили о перехвате контроля над защищенным мессенджером Exclu, популярным в преступном сообществе. Полиция получила доступ к перепискам администраторов, пользователей и владельцев сервиса и провела 79 обысков и 49 арестов.
- После длительного расследования ФБР был арестован Pompompurin — администратор популярного дарквеб-форума Breached, после чего ресурс перестал функционировать. ФБР также сообщило о наличии доступа к базе данных скомпрометированного Breached, что может обернуться новыми эпизодами арестов.
- В январе правоохранительные органы заявили о захвате серверов группировки вымогателей Hive. Наблюдение за злоумышленниками позволило вовремя предотвратить шифрование скомпрометированных организаций, получить ключи для дешифрования жертв, лишить вымогателей сетевой инфраструктуры и многомиллионной прибыли.

Дальнейшее проведение подобных мероприятий может повлиять на активность преступников: из-за закрытия дарквеб-форумов, которые используются для продажи краденых данных, зловредов и других инструментов, труднее получить доступ к этой информации, что осложнит проведение кибератак и уменьшит их количество. Но вероятнее, что в ближайшем будущем нарушители переведут свои коммуникации в другие форматы: мессенджеры или специальные приложения. Волна арестов и обысков показывает действующим злоумышленникам их вероятное будущее, а решившимся войти в мир киберпреступности стоит дважды подумать над своим решением.

Актуальные уязвимости

Согласно данным Национального института стандартов и технологий США (NIST), в I квартале стало известно свыше чем о 7 тыс. уязвимостях, что на 24% больше, чем за аналогичный период прошлого года. Из новых недостатков, по информации исследователей ReliaQuest, 29 замечены в реальных атаках и активно эксплуатируются. Наши прогнозы об актуальности старых брешей в защите становятся реальностью, так как не все пользователи вовремя обновляют ПО и следят за выходом патчей безопасности. Для I квартала стали актуальными следующие уязвимости:

- CVE-2023-23397. Серьезный недостаток, связанный с повышением привилегий и не требующий взаимодействия с пользователем, был выявлен в Microsoft Outlook и использовался в реальных атаках. Злоумышленник может отправить электронное письмо и с его помощью проэксплуатировать уязвимость в Outlook на компьютере пользователя. После получения вредоносного письма на устройстве жертвы инициируется запрос к SMB-серверу[3] преступника. В запросе содержится хеш NTLMv2, который можно перехватить и использовать для аутентификации в других системах либо для восстановления пароля.
- CVE-2023-0669. Уязвимость нулевого дня, выявленная в GoAnywhere MFT, возникла из-за небезопасной десериализации[4] данных и позволила атакующим выполнять произвольный код. Исследователи безопасности выявили более 1000 уязвимых экземпляров решения по всему миру, а вымогателям CIOP удалось скомпрометировать свыше 100 организаций.
- CVE-2021-21974. В феврале атакующие успешно эксплуатировали давнюю и имеющую исправление уязвимость серверов VMware ESXi, которая позволяет удаленно выполнять команды через OpenSLP. Недостаток выявлен на 19 тыс. серверов по всему миру, чем успешно воспользовались новые вымогатели ESXiArgs и известные группировки.
- CVE-2022-41080 и CVE-2022-41082. В сентябре эксплойт ProxyNotShell для Microsoft Exchange Server использовался в атаках, а уже в ноябре уязвимости были устранены Microsoft. Однако в I квартале злоумышленникам удалось найти другой способ[5] эксплуатировать эти недостатки путем подделки запросов со стороны скомпрометированного сервера (server-side request forgery, SSRF) в Outlook Web Access (OWA): вымогатели Cuba и Play — одни из первых атакующих, использовавших новый метод.

[3] SMB-сервер — это сервер, применяемый для обмена данными по протоколу SMB в локальной или глобальной сети, а также для совместного использования принтеров и других устройств.

[4] Десериализация — процесс восстановления структур и объектов из сериализованной строки или последовательности байтов.

[5] Способ был назван OWASSRF из-за наличия уязвимости SSRF в продукте OWA.

Для защиты от атак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. С учетом специфики инцидентов I квартала настоятельно рекомендуем с осторожностью относиться к входящим электронным письмам, сообщениям в мессенджерах и социальных сетях, проверять отправителя и не переходить по подозрительным ссылкам, чтобы не стать жертвой социальной инженерии или компрометации устройства вредоносным ПО. Загружайте приложения только из доверен-

ных источников, используйте решения для резервного копирования файлов и своевременно устанавливайте обновления безопасности. Кроме того, мы советуем проводить тщательные расследования всех крупных инцидентов: это позволит выявить точки компрометации и уязвимости, которыми воспользовались злоумышленники, а также своевременно убедиться в том, что преступники не оставили себе запасных входов. Укрепить защищенность периметра можно с помощью современных средств, к примеру межсетевых экранов уровня приложений (web application firewalls, WAF). Чтобы предотвратить заражение устройства, рекомендуем использовать песочницы, которые анализируют поведение файлов в виртуальной среде и выявляют вредоносную активность.

Последствия атак

Кибератаки I квартала приводили к разным последствиям: злоумышленникам удавалось успешно атаковать как небольшие предприятия, так и отраслевых гигантов; не обошлось без сбоев в работе критической информационной инфраструктуры. Основной фокус преступников был направлен на получение конфиденциальной информации и нарушение основной деятельности организаций. Кроме того, можно выделить несколько случаев серьезных финансовых потерь: атака вымогателей на MKS Instruments вызвала серьезные нарушения в цепочке поставок продукции, а процесс восстановления оказался затруднен. Упущенная прибыль составила 200 млн долларов. Инциденты информационной безопасности могут повлиять и на стоимость ценных бумаг: после атаки на системы DISH Network акции компании упали почти на 7%.

Рисунок 4. Последствия атак злоумышленников (доля атак)

Топ-5 атак начала 2023 года, которые повлекли за собой негативные последствия и вызвали большой резонанс:

- RoyalMail, национальный почтовый оператор Великобритании, считающийся объектом критической инфраструктуры, был атакован вымогателями LockBit, что привело к серьезному нарушению всех зарубежных поставок.
- ION Group, разработчик ПО для финансовых учреждений, банков и бирж, подвергся атаке вымогателей, из-за чего была нарушена работа по крайней мере 42 клиентов, включая некоторые из крупнейших в мире банков, брокерских компаний и хедж-фондов.
- Администрации городов Окленд и Модесто (США) подверглись атаке программ-вымогателей, в результате чего государственные службы были отключены от сети, а полиции пришлось вынужденно работать по старинке, используя портативные радиостанции, ручки и бумагу во время патрулирования.
- Системы телекоммуникационной компании DISH Network и ее дочерних организаций были скомпрометированы, из-за чего на несколько дней отключились веб-сайты, приложения и системы обслуживания клиентов.
- Критически важные системы и доступ к медицинским файлам отключились в результате киберинцидента в госпитале Ross Memorial (Канада). Был объявлен код «серый», что означает невозможность проведения операций и процедур.

Не обошлось и без громких утечек. В атаках с утечками конфиденциальной информации злоумышленники чаще ориентировались на похищение персональных данных (36%) и коммерческой тайны (14%).

Рисунок 5. Типы украденных данных (в атаках на организации)

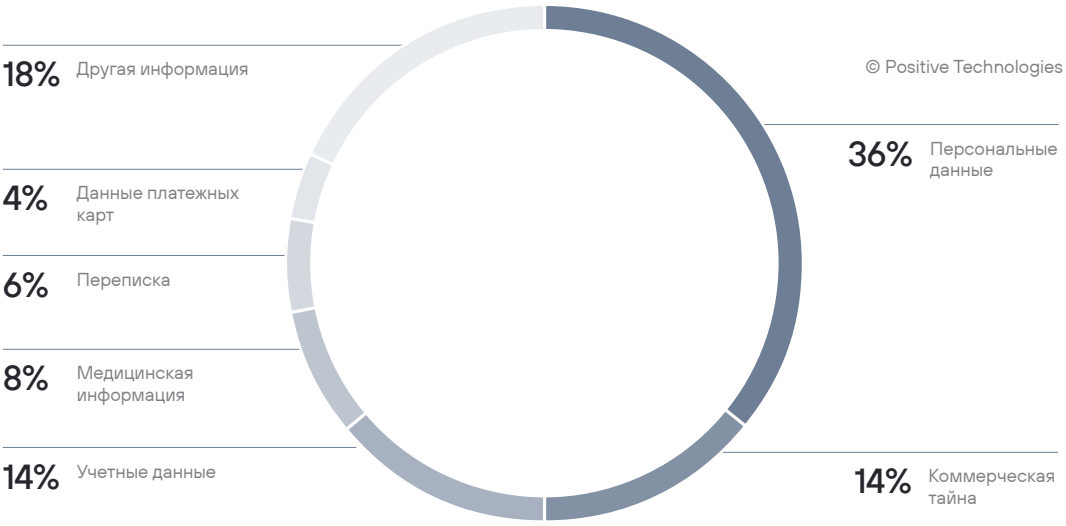
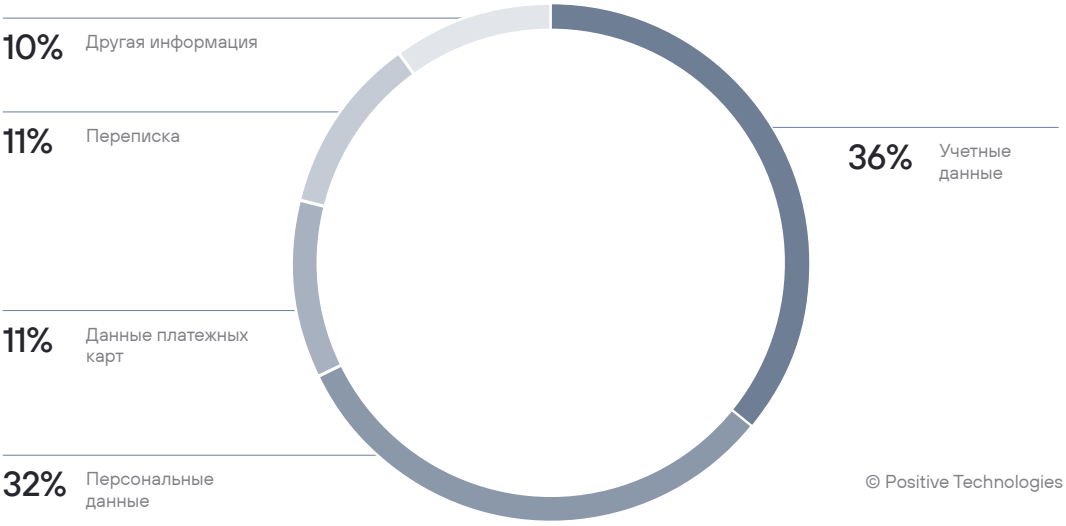


Рисунок 6. Типы украденных данных (в атаках на частных лиц)



Наиболее заметные утечки I квартала:

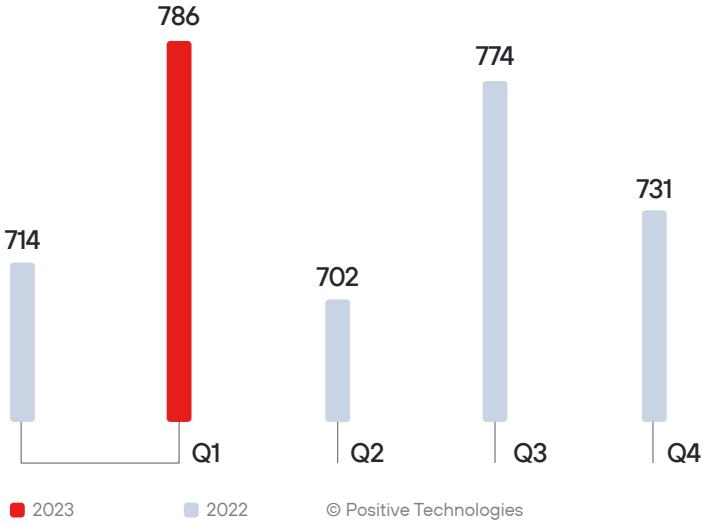
- Неизвестные злоумышленники атаковали GDS Holdings и ST Telemedia и похитили учетные данные (логины и пароли) для входа в центры обработки данных в Азии. Услугами операторов пользуются крупнейшие мировые компании, например AG, Amazon, BMW, Huawei, Walmart. Конфиденциальная информация была выставлена на продажу в дарквебе за 175 тыс. долларов.
- Данные HDB Financial Services, дочерней компании крупнейшего в Индии частного банка HDFC Bank, были опубликованы на форуме Breached[6]. Преступники похитили обширный набор персональных данных клиентов (полные имена, даты и места рождения, сведения о занятости, кредитный рейтинг) и сотрудников. Информация из утечки практически сразу была использована в фишинговых атаках.
- Вымогателям BlackCat удалось извлечь 2 ТБ конфиденциальной информации из сети крупного производителя взрывчатки Solar Industries India. Особо примечательно то, что нарушители получили доступ к документам с технической спецификацией и чертежами действующих образцов вооружения, к данным о цепочках поставок продукции, деталям сотрудничества с правительством Индии и даже к записям камер видеонаблюдения на предприятии. Утечка привлекла значительное внимание правительства и Министерства обороны Индии.
- Тайваньский технологический гигант Acer подтвердил утечку после того, как злоумышленник разместил объявление о продаже похищенных данных на форуме в дарквебе. Информация включала в себя технические руководства, сведения о серверной инфраструктуре, образы BIOS, продуктовую документацию и сервисные ключи активации.
- Вымогатели LockBit взяли на себя ответственность за компрометацию систем Maximum Industries, технологического подрядчика SpaceX: преступникам удалось похитить около 3 тыс. чертежей деталей. Злоумышленники пообещали устроить аукцион для желающих приобрести технологические наработки конкурента в случае неуплаты выкупа.

[6] На момент публикации закрыт, а его владелец арестован.

Сводная статистика

68%
атак имели целенаправленный характер

Рисунок 7. Количество инцидентов в 2022 и 2023 годах (по кварталам)



16%
атак были направлены на частных лиц

Рисунок 8. Категории жертв среди организаций

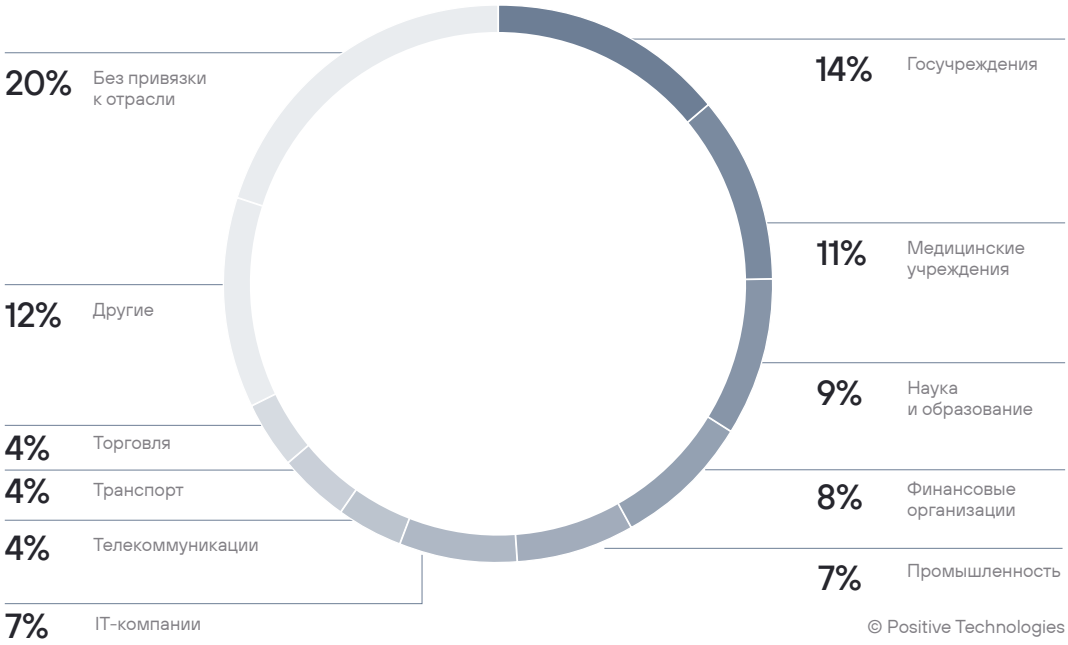


Рисунок 9. Объекты атак (доля атак)

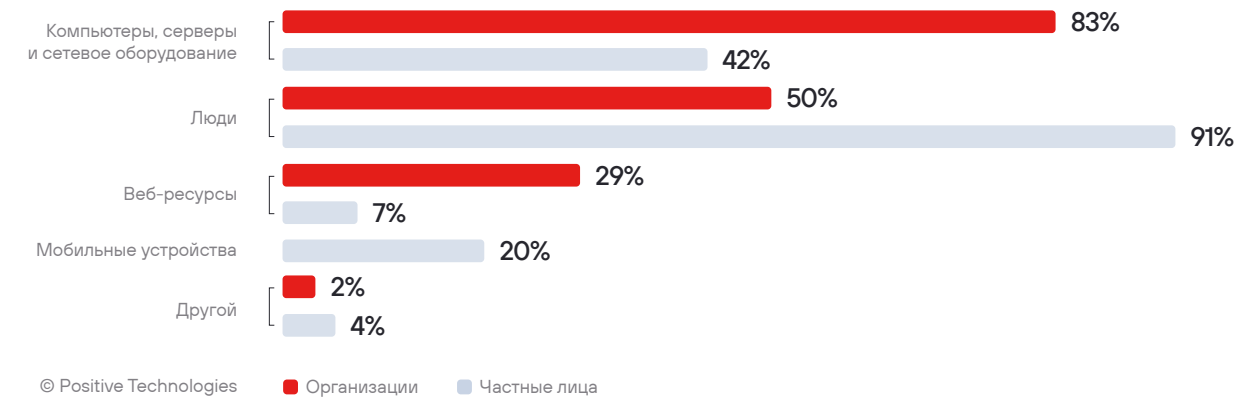


Рисунок 10. Методы атак (доля атак)

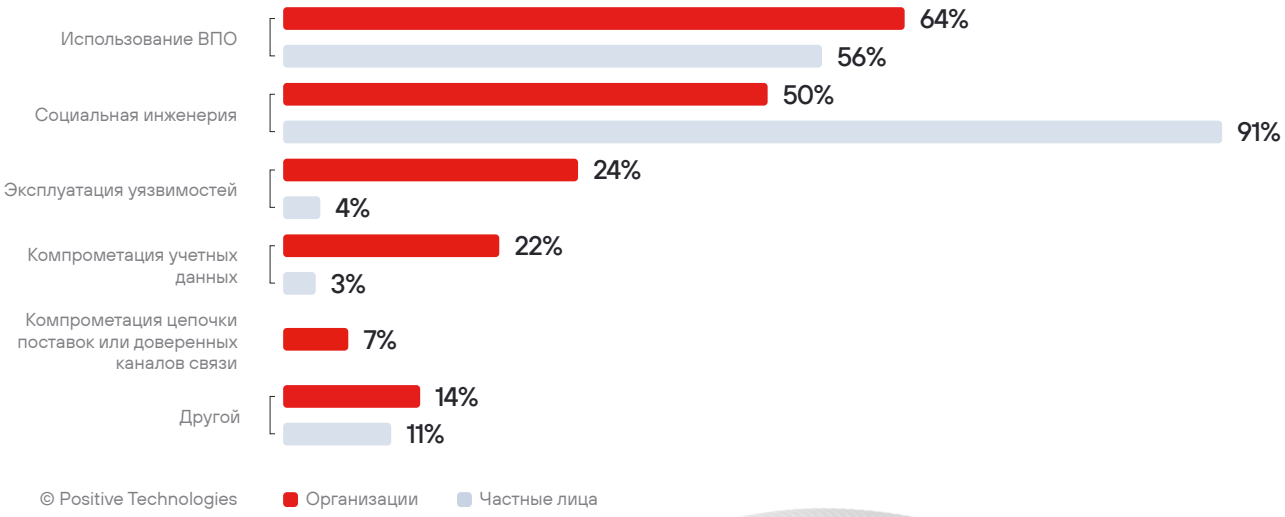


Рисунок 11. Типы вредоносного ПО (доля атак с использованием ВПО)

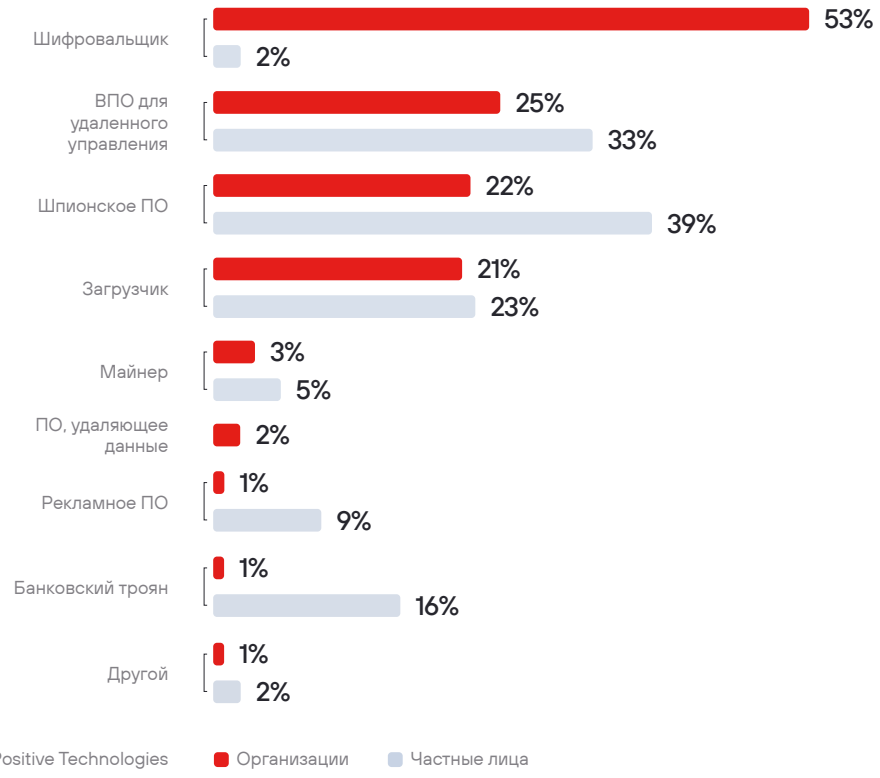


Рисунок 12. Способы распространения вредоносного ПО в атаках на организации

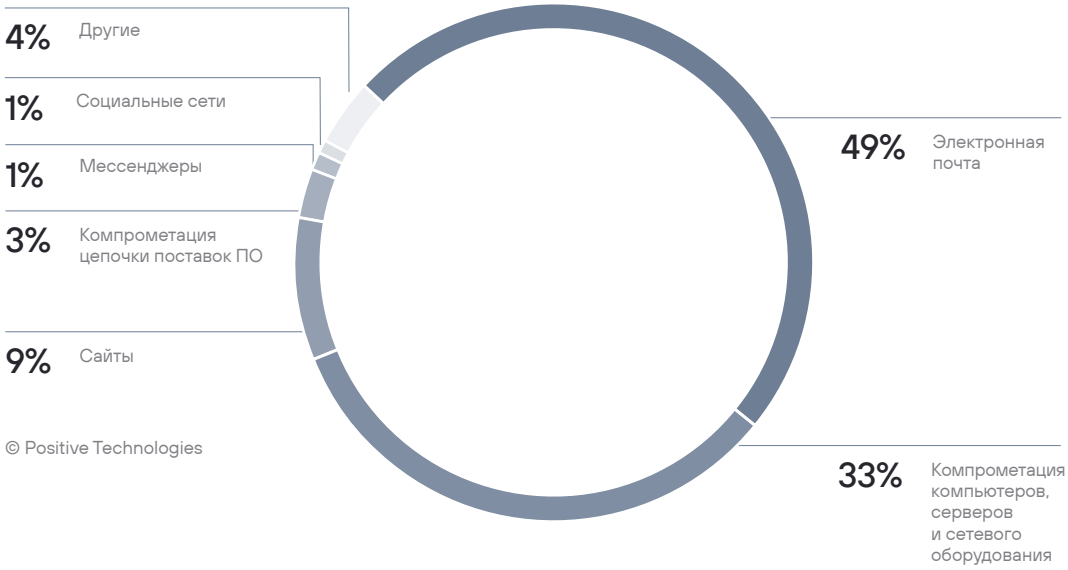


Рисунок 13. Способы распространения вредоносного ПО в атаках на частных лиц

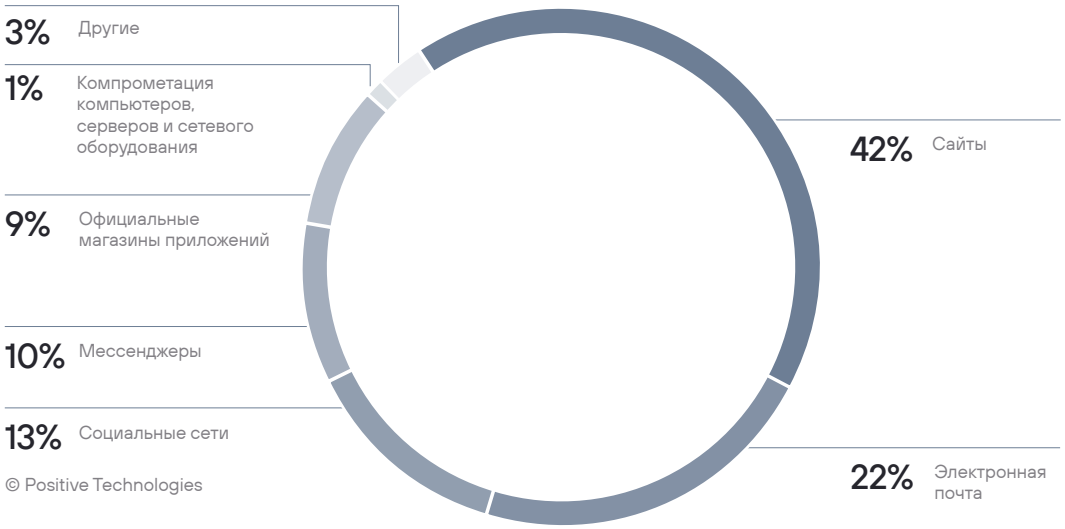
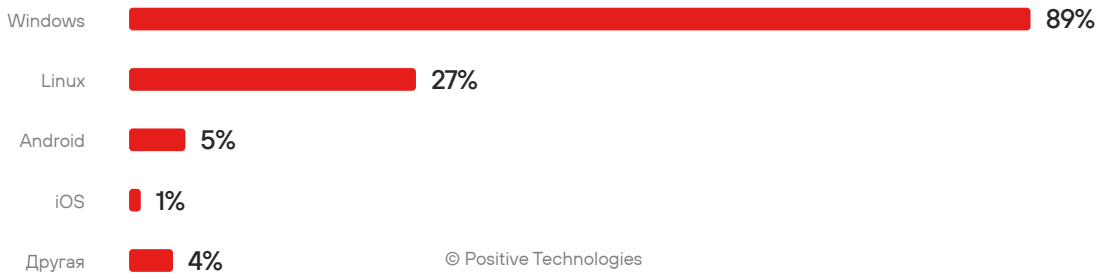


Рисунок 14. Целевые ОС в атаках с использованием ВПО (доля атак)



Категории жертв

	Распределение киберинцидентов по метрикам (объекты атак, методы, последствия) и категориям жертв	Госучреждения	Медицинские учреждения	Наука и образование	Финансовые организации	Промышленность	IT-компании	Телекоммуникации	Транспорт	Торговля	Другие	Без привязки к отрасли	Частные лица
	Всего атак	92	70	59	50	49	47	29	24	23	80	133	130
Объект	Компьютеры, серверы и сетевое оборудование	81	52	54	45	45	36	25	23	14	50	118	55
Объект	Веб-ресурсы	37	27	9	22	5	20	13	15	8	27	10	9
Объект	Люди	43	42	41	17	31	19	5	1	6	43	78	118
Объект	Другой	—	—	—	—	—	—	—	—	—	5	5	5
Метод	Использование ВПО	55	42	50	27	40	18	11	5	17	43	111	73
Метод	Социальная инженерия	43	42	41	17	31	19	5	1	6	43	78	118
Метод	Компрометация учетных данных	18	27	18	8	13	22	4	4	3	14	14	4
Метод	Эксплуатация уязвимостей	18	10	5	6	12	15	10	1	9	22	50	5
Метод	Компрометация цепочки поставок	1	1	—	8	1	1	5	3	4	4	15	—
Метод	Другой	22	9	5	16	—	—	9	15	2	8	4	14
Последствие	Нарушение основной деятельности	47	36	46	31	32	11	19	18	8	22	20	3
Последствие	Утечка конфиденциальной информации	40	45	37	17	32	37	16	9	15	44	42	77
Последствие	Ущерб интересам государства	42	—	—	—	4	1	3	1	—	1	1	—
Последствие	Прямые финансовые потери	3	1	—	3	5	1	4	—	3	15	1	40
Последствие	Использование ресурсов организаций или частных лиц для проведения атак	1	—	—	1	—	6	1	—	1	5	5	3
Последствие	Другое	4	1	—	3	2	2	2	—	—	2	17	17
Последствие	Неизвестно	20	4	4	8	3	3	—	—	4	12	55	19

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

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

Об исследовании

Данный отчет содержит информацию об общемировых актуальных угрозах 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 компаний 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 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. 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

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.