Актуальные киберугрозы: II квартал 2023 года

Positive Technologies

ptsecurity.com

Содержание

Ключевые цифры и тренды

Во II квартале 2023 года количество инцидентов увеличилось на 4% по сравнению с предыдущим кварталом и выросло на 17% относительно II квартала 2022 года. Выросла доля целевых атак — они составили 78% от общего количества. Для организаций самыми распространенными последствиями успешных кибератак стали утечки конфиденциальной информации (67%) и нарушение основной деятельности (44%). Наблюдалось множество крупных утечек персональных данных пользователей, массовые атаки через эксплуатации уязвимостей.

Прицел на решения для безопасной передачи данных

В I квартале группа вымогателей Cl0p отметилась масштабной серией взломов организаций через уязвимость нулевого дня в GoAnywhere MFT (CVE-2023-0669). Во II квартале им удалось успешно проэксплуатировать найденную уязвимость (CVE-2023-34362), которая заключается во внедрении вредоносного SQL-кода в программное обеспечение MOVEit Transfer, продукта компании Progress Software, предназначенного для управления передачей файлов. Для Cl0p эти уязвимости не были новыми: группа пыталась извлечь данные со взломанных серверов MOVEit еще в апреле 2022 года.

Среди пострадавших были и компании, стоящие за созданием известных брендов кибербезопасности. Например, Gen Digital (Avast, CCleaner, Norton LifeLock) подтвердила, что личная информация сотрудников была скомпрометирована в результате недавней атаки на MOVEit[1].

[1] На момент публикации этой статьи группировка добавила более шестисот компаний на свой сайт с данными об утечках с требованием о выкупе за непубликацию информации, украденной через эксплуатацию уязвимости в MOVEit.

Учитывая успех предыдущих кампаний Cl0p по эксплуатации уязвимостей нулевого дня в программном обеспечении для управляемой передачи файлов, в будущем группировка может придерживаться аналогичной стратегии для других решений этого класса. Подход Cl0P к поиску и эксплуатации уязвимостей нулевого дня показывает, что не все вымогатели настроены на моментальную монетизацию своей деятельности, но также способны на игру вдолгую для извлечения максимальной выгоды. Злоумышленники осознают, что одновременная атака на множество жертв оказывает большее влияние и затраченное время впоследствии полностью окупает себя.

Атаки на блокчейн-проекты

Блокчейн-проекты остаются привлекательной целью для атак не только на протоколы, но и на аккаунты в социальных сетях с целью обмана пользователей и кражи денежных средств: во II квартале блокчейн-проекты становились жертвами злоумышленников в два раза чаще, чем в предыдущем. Хорошо подготовленная атака на владельцев серверов криптовалютных бирж в Discord повлекла за собой потерю 3 млн долларов. Используя методы социальной инженерии, злоумышленникам удалось обмануть администраторов серверов: они представились журналистами и, проведя интервью, сообщили о необходимости пройти верификацию личности. После перенаправления администратора на вредоносный сайт у него похищался токен пользователя Discord, выполнялся вход в его аккаунт, проводилось удаление других администраторов с сервера и публиковалась фишинговая запись.

Рисунок 1. Предупреждение пользователей о взломе Discord-сервера

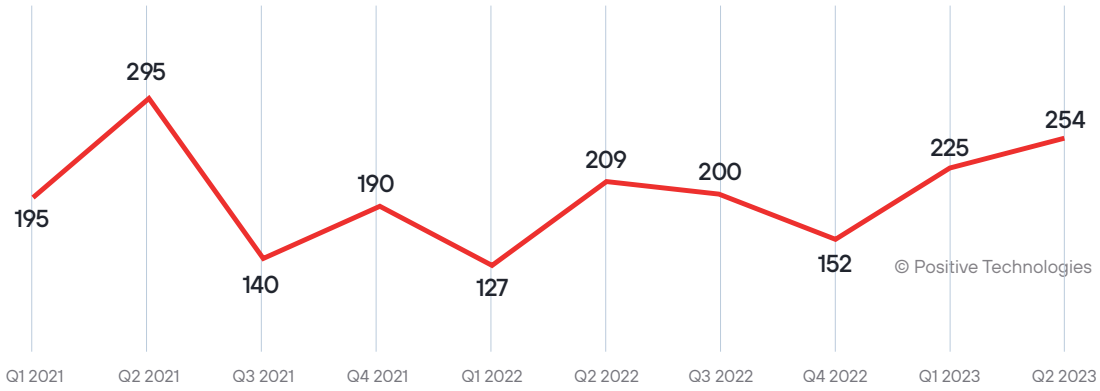
Взлому подвержены и официальные twitter-аккаунты. Так, от имени KuCoin была размещена фишинговая запись о раздаче криптовалюты с обещанием всем, кто переведет какую-либо сумму, вернуть ее в двойном размере. За 45 минут с момента публикации до момента удаления записи пользователи успели осуществить транзакции на сумму 22 600 долларов. Платформа обмена пообещала вернуть жертвам все утерянные средства.

Кроме того, наблюдались крупные атаки на блокчейн-протоколы, в которых принимали участие как анонимные злоумышленники, согласившиеся вернуть большую часть украденных средств в обмен на прекращение расследования их преступлений ([1], [2]), так и APT-группировки (например, Lazarus Group, причастная к взлому Atomic Wallet и краже 35 млн долларов с кошельков криптовладельцев).

Продолжающийся рост активности шифровальщиков

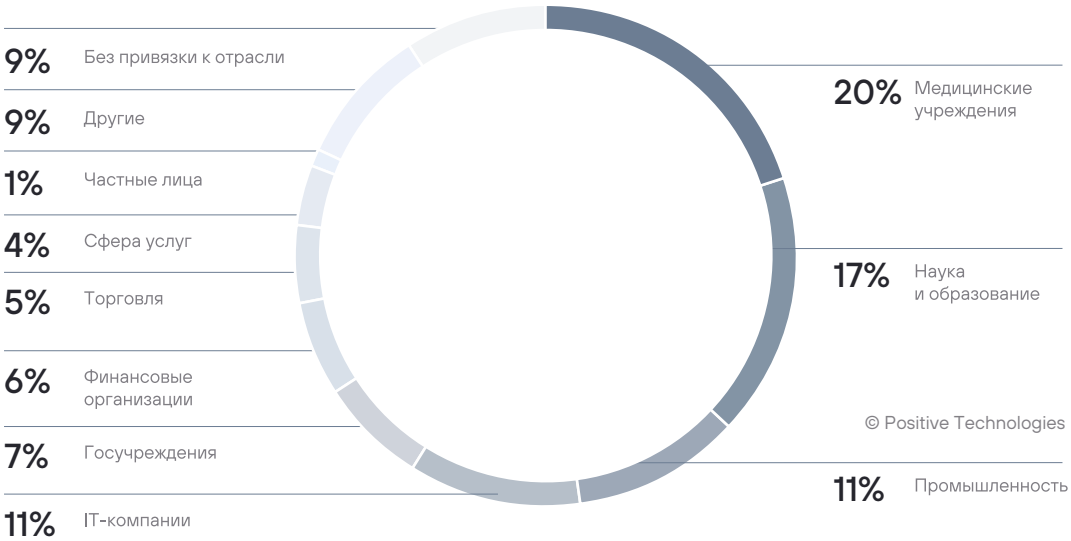
Количество атак шифровальщиков продолжило расти во II квартале и увеличилось на 13%.

Рисунок 2. Количество атак вымогателей (по кварталам)



Напряженная обстановка сохраняется в секторе науки и образования, государственных и медицинских организациях, несмотря на внутренние конфликты злоумышленников и активное преследование спецслужбами: банда вымогателей LockBit заблокировала свой партнерский филиал за атаку на некоммерческую дошкольную организацию Keystone SMILES Community Learning Center, а Cl0p заявили об удалении у себя всех данных, украденных из госучреждений США после того, как правительство объявило награду за информацию о группировке.

Рисунок 3. Распределение атак вымогателей по категориям



Мы отмечаем рост доли IT-компаний среди жертв вымогателей: во II квартале на технологические компании пришлось 11% от общего количества жертв вымогателей, что на 5 процентных пунктов выше показателя предыдущего квартала. Это связано с потенциальной выгодой для злоумышленников, так как успешные атаки на IT-компании позволяют получить доступ к конфиденциальным данным не только самих компаний, но и их клиентов, а также открывают возможность проведения атак типа supply chain и trusted relationship.

Среди активных групп шифровальщиков обретают известность новые имена: 8Base — опытные злоумышленники, активно атакующие организации по всему миру. После долгого периода затишья и малой популярности группировка запустила свой сайт с информацией о жертвах и заняла второе место после LockBit по числу жертв в июне. Обнаруженные в марте 2023 года вымогатели Akira показали себя во II квартале, войдя в топ-10 наиболее активных группировок, но уже в конце июня компанией Avast был выпущен бесплатный дешифратор для систем под управлением Windows. Однако Linux-системы, для которых дешифратор отсутствует, стали новыми мишенями для группировки Akira.

Не обходится и без уникальных кампаний. Отслеживаемая с апреля 2023 года MalasLocker атакует серверы Zimbra с использованием уязвимости CVE-2022-24682, шифрует системы жертв, но в качестве выкупа требует сделать пожертвования в благотворительные организации. За весь II квартал MalasLocker стала второй группировкой по числу жертв. Наибольшее число атакованных компаний располагаются в Италии, США и России.

Вымогательство без шифрования

Вымогательство в киберпространстве прошло путь от требования выкупа за расшифровку данных до шифрования и шантажа публикацией украденных данных (двойное вымогательство).

Компании все больше уделяют внимание кибербезопасности: внедряют протоколы действий в случае кибератак, средства мониторинга и реагирования на инциденты на конечных узлах инфраструктуры, средства резервного копирования. Использование вирусов-шифровальщиков не всегда оказывает желаемое воздействие на жертву и требует от злоумышленника значительных усилий для обхода средств защиты, внедрения и развертки ВПО. Все вышеперечисленное привело к тенденции отказа от этапа шифрования и перехода к использованию похищенной конфиденциальной информации в качестве основного инструмента давления на жертв, о чем также сообщили специалисты Barracuda. Атака CI0p на организации без использования техники двойного вымогательства показала, что такой вид атаки является действенным и актуальным. В то же время группировки Karakurt и RansomHouse, изначально нацеленные только на кражу данных с целью вымогательства, продолжают свои кампании и во II квартале.

Отказ от этапа шифрования и переход к вымогательству через угрозы публикации украденных данных также может быть обусловлен выпуском специалистами безопасности различных дешифраторов. Например, дешифратор White Phoenix позволяет восстанавливать файлы, которые были зашифрованы популярным прерывистым методом. Группировка BianLian продолжила свою кампанию по вымогательству, перестав шифровать системы жертв из-за публикации дешифратора.

Увеличение случаев использования шпионского ПО

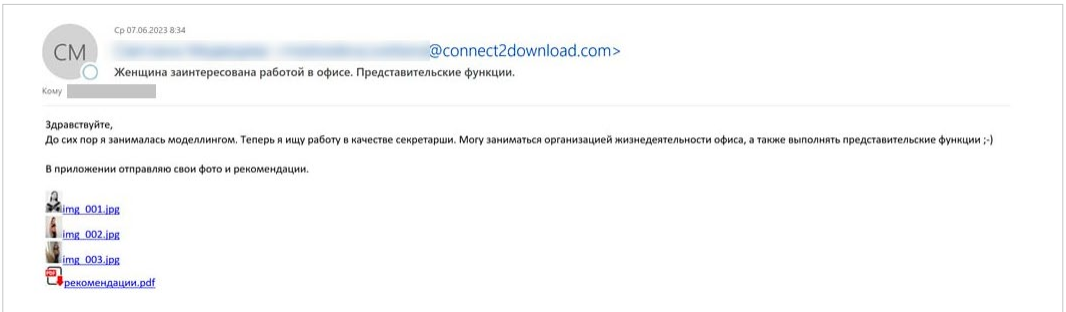
Во II квартале доля атак на организации с применением вредоносного ПО снизилась на 8 п. п. по сравнению с I кварталом. Такое падение связано с ростом количества атак с эксплуатацией уязвимостей (35%). Использование вредоносного ПО в атаках на частных лиц выросло на 5 п. п.

По данным ANY.RUN самым популярным семейством вредоносного ПО стало семейство инфостилеров RedLine с резким скачком во II квартале. Первое место по популярности среди вредоносных программ для Android-устройств согласно исследованию CheckPoint занял SpinOk, также являющийся шпионским ПО. Продолжается тренд использования такого вида ПО в атаках как на организации (21%), так и на частных лиц (62%).

Во II квартале специалистам PT Expert Security Center удалось обнаружить новый легковесный стиллер, написанный на Go и предназначенный для поиска (по расширениям) и отправки на командный сервер файлов из домашнего каталога и локальных дисков, а также содержимого буфера обмена и снимков экрана. Стиллер доставлялся через фишинговые письма — один из наиболее

популярных каналов доставки ВПО в атаках на организации с использованием вредоносов (57%) — со ссылкой на установщик NSIS. После запуска установщик открывал PDF-файл, и одновременно с этим совершалась попытка доставки полезной нагрузки на устройство пользователя.

Рисунок 4. Фишинговое письмо с вредоносным вложением, зафиксированное PT ESC



В атаках на частные лица вредоносное ПО доставляется преимущественно через сайты (40%). Тренд на использование метода SEO poisoning (отравление поисковой выдачи), о котором мы писали ранее, остается актуальным и во II квартале. Злоумышленники распространяют вредоносное ПО, комбинируя методы SEO poisoning и вредоносной рекламы на сайтах ([1], [2], [3]).

Актуальные уязвимости

Количество обнаруженных за квартал уязвимостей растет: во II квартале их было выявлено на 7% больше, чем в начале года. Количество новых уязвимостей составило более 7,5 тыс. согласно данным Национального института стандартов и технологий США (NIST). Злоумышленники также используют старые уязвимости, поскольку некоторые системы остаются необновленными. Для II квартала стали актуальными следующие уязвимости:

- **CVE-2023-34362.** Широко эксплуатируемая уязвимость нулевого дня в MOVEit MFT, которая позволяет злоумышленникам получать доступ к любым файлам и повышать свои привилегии на сервере, используя внедрение вредоносного SQL-кода в запросы к серверу.
- **CVE-2023-27350 и CVE-2023-27351.** Критически опасные уязвимости в программном обеспечении PaperCut MF и NG для управления печатью принтеров. Группировке Lace Tempest удалось скомпрометировать уязвимые серверы, получить удаленный доступ и доставить на них шифровальщики, а затем похитить конфиденциальную информацию.
- **CVE-2023-2868.** Уязвимость нулевого дня в продукте Barracuda Email Security Gateway, связанная с неполной проверкой входящих данных в модуле проверки вложений входящих писем. Недостаток позволяет провести внедрение удаленных команд специально сформированными вредоносными TAR-файлами. Этой уязвимостью воспользовалась APT-группировка UNC4841, проведя кампанию по кибершпионажу с помощью рассылки электронных писем с вредоносным вложением. Несмотря на то что Barracuda выпустила обновление безопасности для подверженных уязвимости устройств, этого оказалось мало: компания настаивает на необходимости полной замены скомпрометированных устройств.

- **CVE-2018-9995 и CVE-2016-20016.** В апреле 2023 года исследователями FortiGuard были зафиксированы значительные всплески попыток атак с использованием уязвимостей CVE-2018-9995 в DVR-устройствах компании TBK (более чем 50 тыс. уникальных попыток) и CVE-2016-20016 в цифровых видеорегистраторах MVPower. Эксплуатация CVE-2018-9995 позволяет злоумышленникам обходить аутентификацию на устройстве и получать доступ к уязвимой сети, а CVE-2016-20016 — выполнять команды без проверки подлинности с использованием вредоносных HTTP-запросов. Эти вспышки показывают, что старые и уязвимые устройства легко могут подвергнуться атаке спустя несколько лет существования эксплойта.

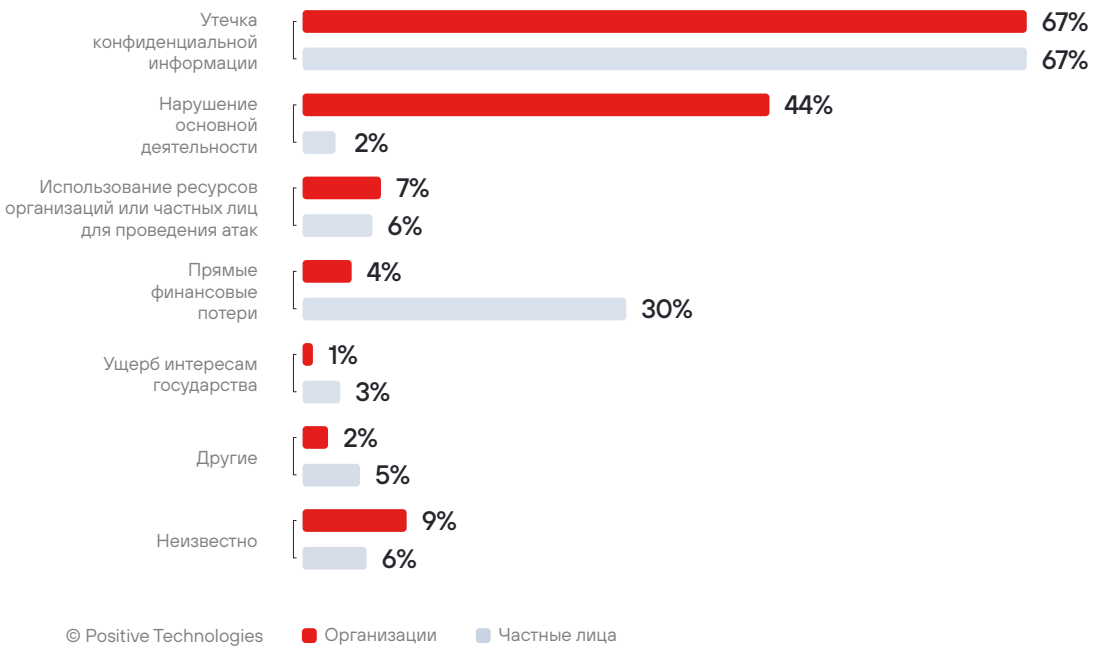
Рекомендации

Для защиты от атак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. С учетом специфики инцидентов II 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 атак с использованием метода социальной инженерии или компрометации устройства вредоносным ПО. Будьте рассудительными и обдумывайте принимаемые решения, особенно когда видите выгодные предложения. Загружайте приложения только из доверенных 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

Последствия атак II квартала носили разнообразный характер: успешные кибератаки затрагивали предприятия и малого, и крупного бизнеса, оказывали влияние на города и округа. Наиболее частыми последствиями атак были получение злоумышленниками конфиденциальной информации и нарушение основной деятельности организаций. Примером влияния кибератаки на город является атака программы-вымогателя на американский мегаполис Даллас. Атака нарушила работу городских служб: полиции пришлось вручную направлять службы экстренной помощи на вызовы, некоторые суды присяжных были отложены, службы водоснабжения не могли обрабатывать онлайн-платежи.

Рисунок 5. Последствия атак злоумышленников (доля атак)



Топ-5 атак II квартала, которые повлекли за собой негативные последствия и вызвали большой резонанс:

- Кибератака на крупного IT-провайдера Германии Bitmarck вынудила компанию отключить все клиентские и внутренние системы. Недоступность сервисов негативно повлияла на работу организаций обязательного медицинского страхования, пользующихся IT-услугами Bitmarck. Так, был потерян доступ к медицинским картам пациентов, стали невозможными обработка электронных листов нетрудоспособности, центральная обработка данных компаний, а также ежемесячная передача статистических сведений и оказание услуг цифровой связи.
- Больницы Айдахо-Фолс и Маунтин-Вью, а также их клиники-партнеры подверглись атаке шифровальщика, из-за которой некоторые учреждения были закрыты. Представители Айдахо-Фолс подтвердили, что некоторые машины скорой помощи были перенаправлены в близлежащие больницы. Клиникам понадобилось более месяца для полного восстановления рабочих процессов.
- Крупные DDoS-атаки на приложения Microsoft вызвали сбои в работе веб-порталов Outlook, OneDrive и Azure. Клиенты наблюдали перебои в работе сервисов: не могли воспользоваться службой электронной почты и облачными сервисами. На пике атаки Outlook был недоступен для 18 000 пользователей. Атаки на сервисы были поочередно проведены хактивистской группировкой Anonymous Sudan в течение трех дней.
- LockBit потребовали от компании TSMC, самой дорогой компании в Азии и одного из крупнейших в мире производителей полупроводников, выкуп в размере 70 млн долларов за непубликацию украденных данных. Утечка данных произошла с неправильно настроенного сервера поставщика IT-оборудования Kinmax Technologies.
- Оператор связи АО «Инфотел», обеспечивающий подключение банков и юридических лиц к автоматизированной системе электронного взаимодействия с ЦБ РФ, подвергся атаке хакактивисткой группировки Cyber.Anarchy.Squad. Атака привела к отключению нескольких крупных банков-клиентов от доступа к банковским системам страны. Для восстановления работы оператору связи понадобилось около 32 часов.

В атаках с утечками конфиденциальной информации злоумышленники чаще ориентировались на похищение персональных данных (53%) и коммерческой тайны (18%) у организаций. В атаках на частных лиц злоумышленники в большей степени были нацелены на кражу их учетных данных (43%).

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

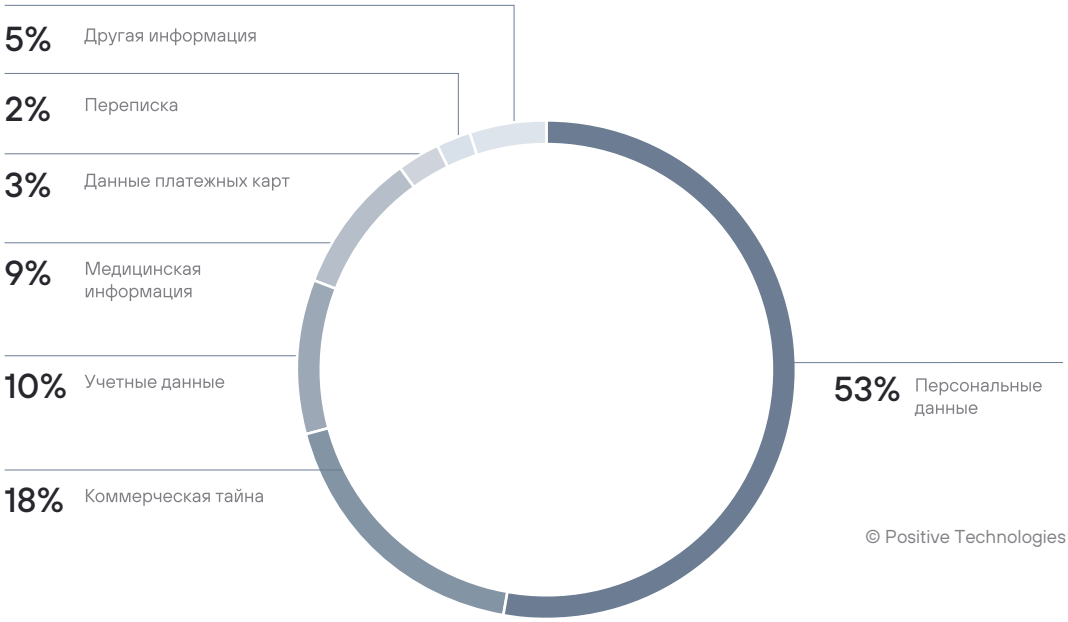
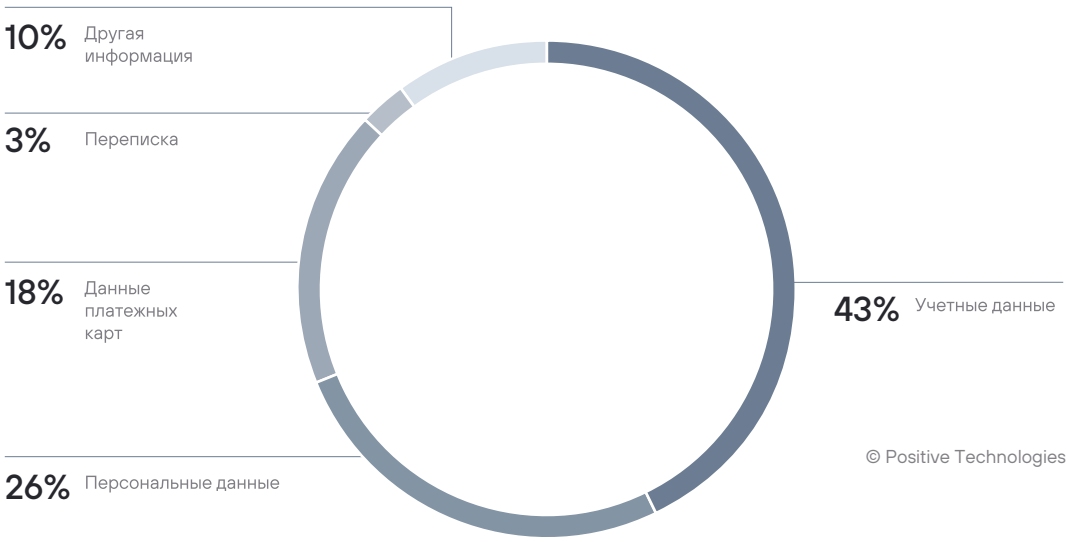


Рисунок 7. Типы украденных данных (в атаках на частных лиц)



Наиболее заметные утечки II квартала:

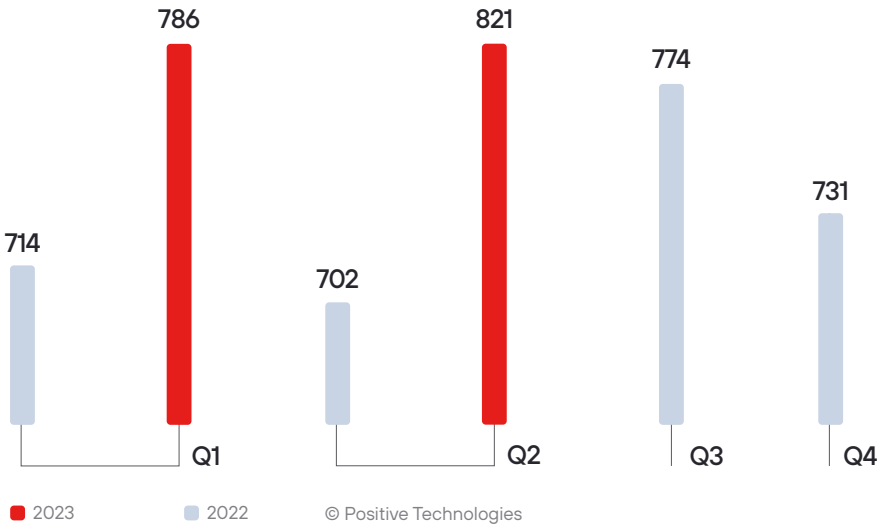
- Одними из крупных жертв атаки Cl0p на MOVEit Transfer стали Управление транспортных средств штата Луизиана (OMV) и Департамент транспорта штата Орегон (ODOT). В результате утечки пострадало 3,5 млн обладателей водительских прав и удостоверений личности штата Орегон и 6 млн штата Луизиана.
- Пострадавшие клиенты Harvard Pilgrim Health Care подали четыре коллективных иска на компанию, обвинив ее в необеспечении безопасности личной и медицинской информации. Организация подверглась атаке программы-вымогателя в апреле, в результате нападения произошла утечка данных 2,5 млн человек.
- В течение трех дней в сети публиковались данные клиентов (Ф. И. О., номер телефона, адрес электронной почты, а в некоторых случаях хешированные пароли) двенадцати российских компаний, в список которых вошли торговые гипермаркеты «Ашан», «Твой Дом», «Леруа Мерлен», сайты магазинов Gloria Jeans, book24.ru, «Аскона», «Буквоед», «ТВОЕ», «Читай-город» и кулинарный сайт edimdoma.ru, сайты издательств «АСТ» и «Эксмо», а также горного курорта «Роза Хутор». Утечку подтвердили представители «Ашана», Gloria Jeans, book24.ru, «Асконы» и издательской группы «Эксмо-АСТ».
- Вымогатели Money Message опубликовали украденные закрытые ключи Intel Boot Guard и ключи прошивки MSI после того, как не смогли договориться о выкупе — группировка требовала 4 млн долларов. Как заявили вымогатели, они украли 1,5 ТБ данных у MSI. Эта утечка затронула всю экосистему Intel и стала прямой угрозой для клиентов MSI. С помощью ключей подписи злоумышленник может создать вредоносные обновления прошивки, а затем доставить их через процесс обновления BIOS и инструменты обновления MSI.
- Медицинские данные о лечении и лабораторной диагностике 2,5 млн пациентов Enzo Biochem были скомпрометированы во время атаки шифровальщика. Часть данных была вовсе удалена из информационной системы компании. Enzo Biochem не останавливала предоставление услуг клиентам, несмотря на нарушение внутренних бизнес-процессов во время сдерживания атаки. Против Enzo Biochem и ее дочерней компании Enzo Clinical Labs было подано четыре коллективных иска, в которых компания обвиняется в недостаточном обеспечении безопасности хранения данных клиентов.

Сводная статистика

78%

атак имели целенаправленный характер

Рисунок 8. Количество инцидентов в 2022 и 2023 годах (по кварталам)



15%

атак были направлены на частных лиц

Рисунок 9. Категории жертв среди организаций

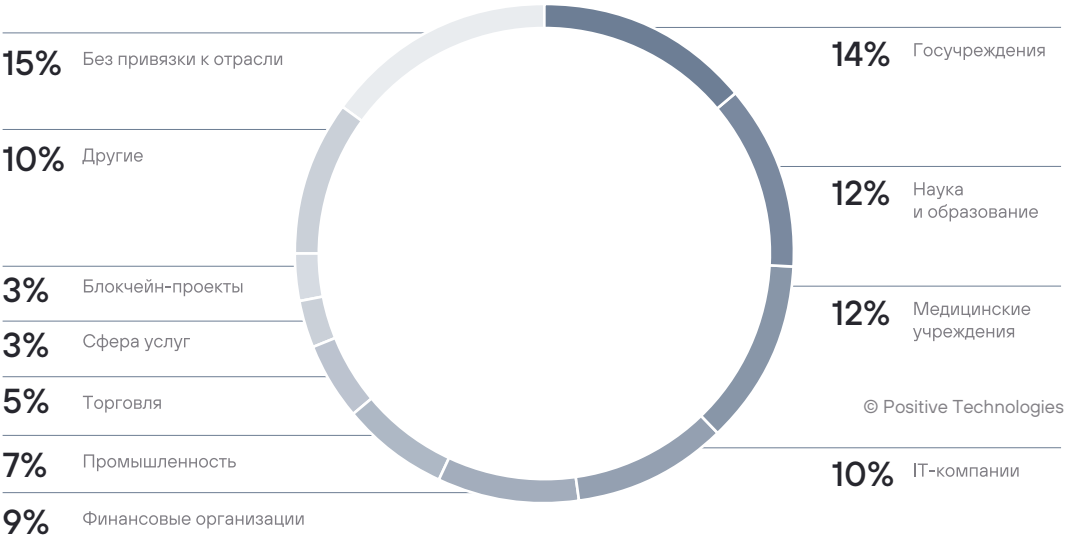


Рисунок 10. Объекты атак (доля атак)

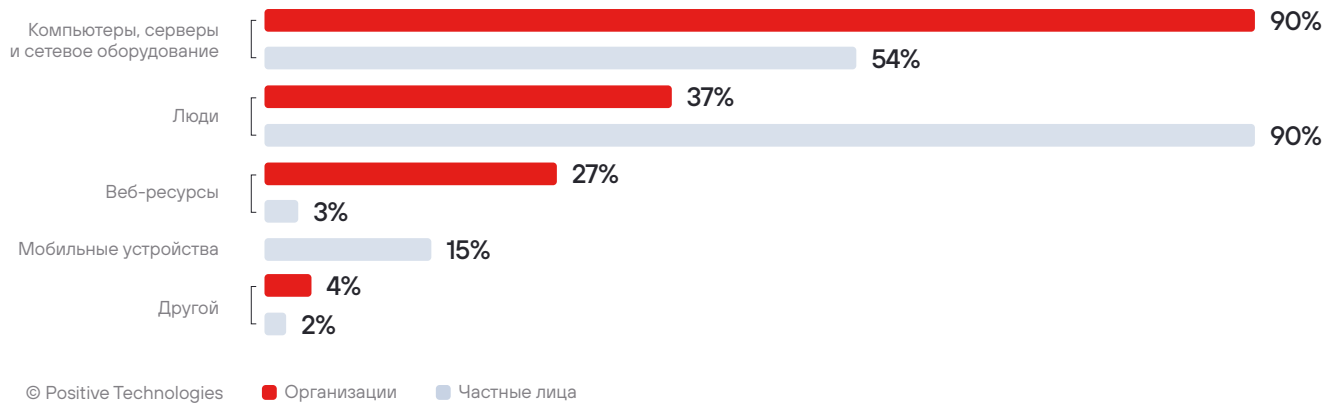


Рисунок 11. Методы атак (доля атак)

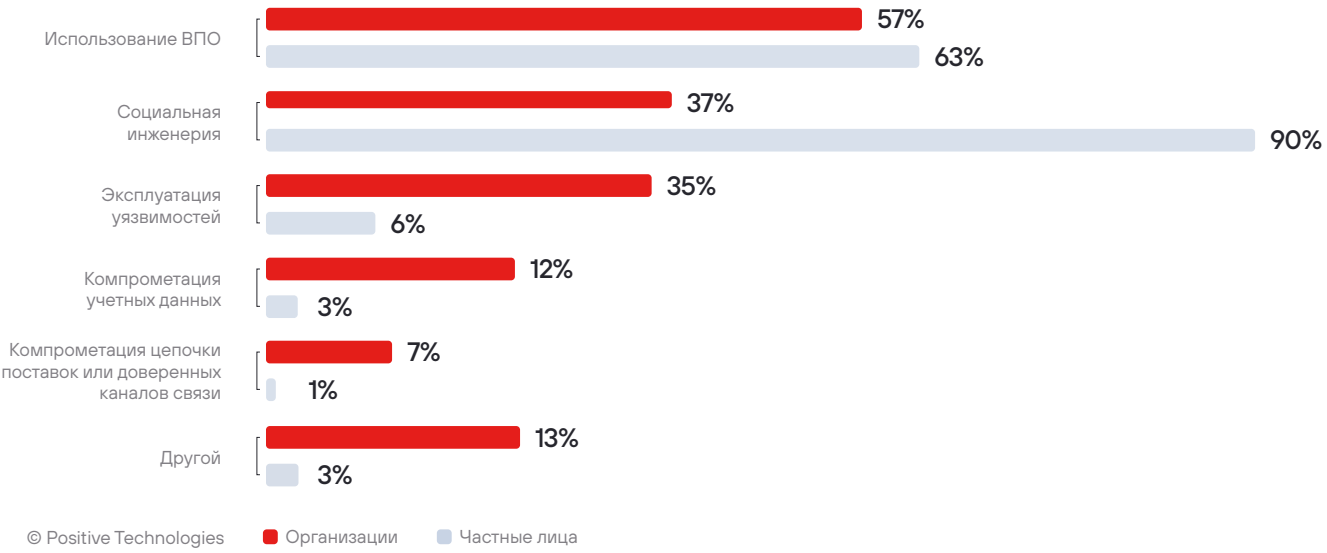


Рисунок 12. Типы вредоносного ПО (доля атак с использованием ВПО)

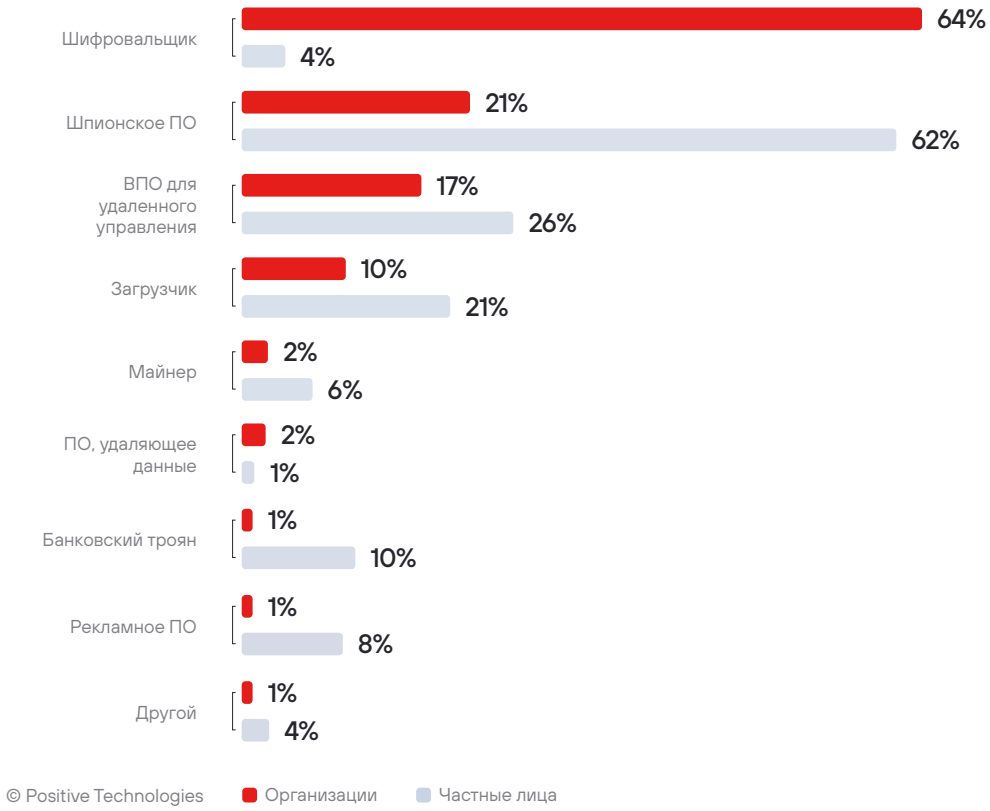


Рисунок 13. Способы распространения вредоносного ПО в атаках на организации

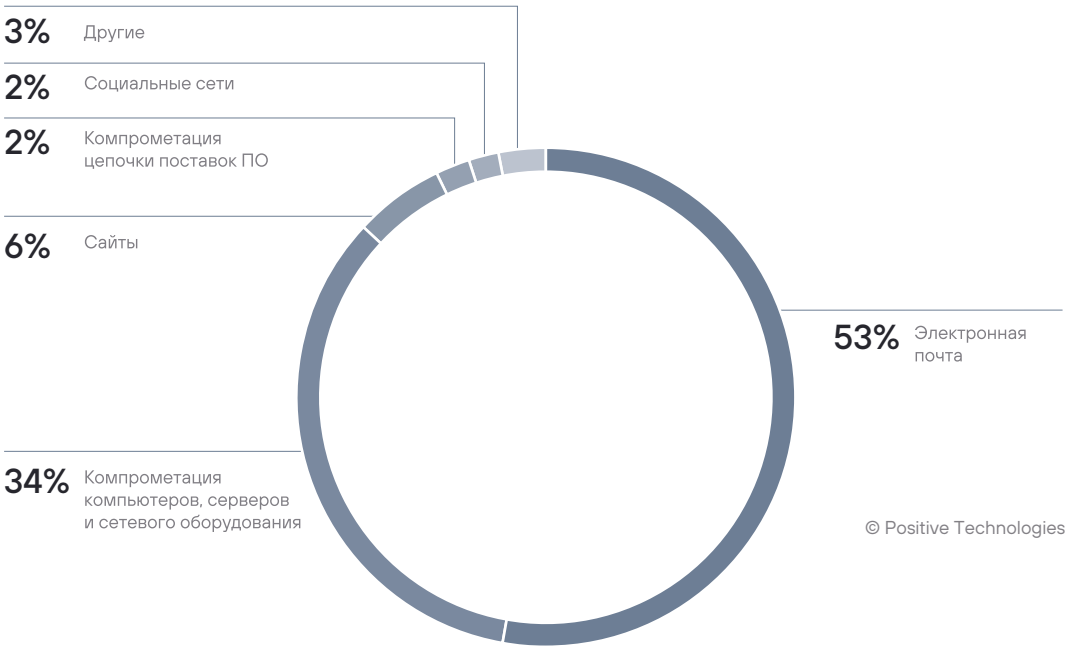


Рисунок 14. Способы распространения вредоносного ПО в атаках на частных лиц

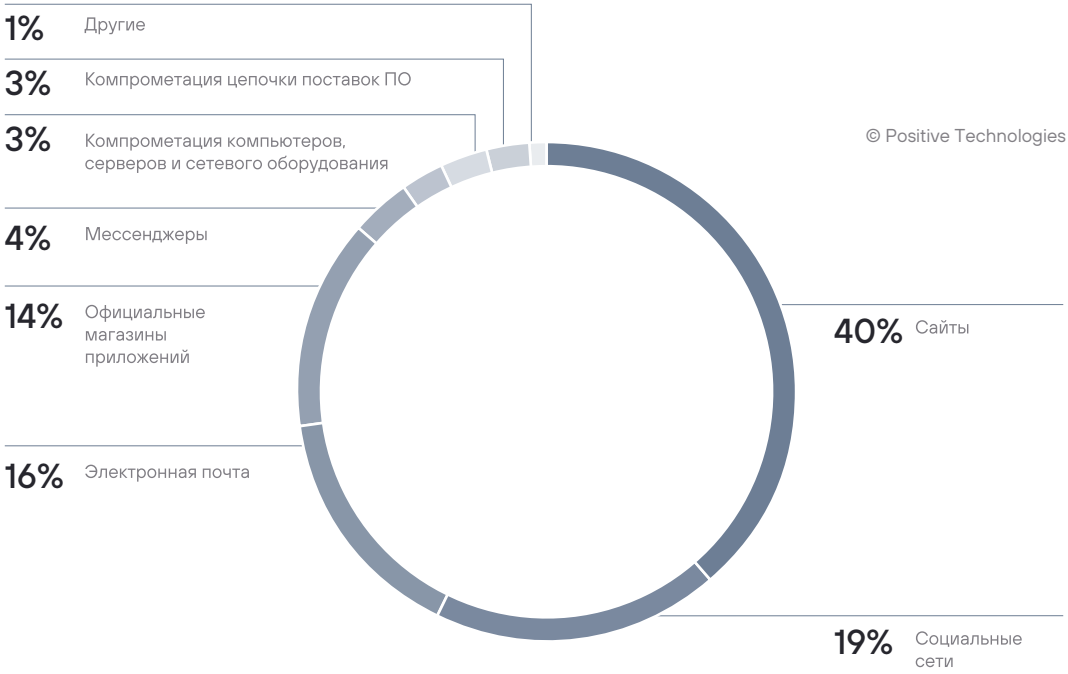


Рисунок 15. Целевые ОС в атаках с использованием ВПО (доля атак)

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	95	49	84	23	71	82	21	66	32	71	103	124
Объект	Компьютеры, серверы и сетевое оборудование	94	47	79	22	64	81	1	63	21	65	93	67
	Веб-ресурсы	42	5	23	5	25	5	2	19	16	19	25	4
	Люди	37	23	46	10	14	39	2	16	8	18	46	112
	Мобильные устройства	–	–	–	–	1	–	–	–	1	–	–	19
	Другой	–	1	–	–	–	–	18	–	–	2	8	2
Метод	Использование ВПО	47	35	48	14	34	64	1	23	12	39	79	78
	Социальная инженерия	37	23	46	10	14	39	2	16	8	18	46	112
	Компрометация учетных данных	8	4	7	5	11	16	1	6	4	11	13	4
	Эксплуатация уязвимостей	27	17	18	7	36	20	2	16	19	36	49	8
	Компрометация цепочки поставок или доверенных каналов связи	6	3	7	1	4	5	–	18	1	2	2	1
	Другой	25	5	10	–	7	3	17	11	1	5	5	4
Последствие	Нарушение основной деятельности	45	30	53	9	33	45	–	27	9	29	24	3
	Утечка конфиденциальной информации	45	37	54	21	58	67	–	50	31	46	60	83
	Ущерб интересам государства	7	1	–	–	–	–	–	–	–	1	–	4
	Прямые финансовые потери	1	2	3	–	–	–	19	1	–	1	2	37
	Использование ресурсов организаций или частных лиц для проведения атак	4	2	3	1	13	1	2	3	2	4	13	8
	Другое	–	1	1	2	1	1	–	1	1	–	6	6
	Неизвестно	13	1	2	2	2	6	1	4	–	9	25	7

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

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

Об исследовании

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 группировок. 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.

ptsecurity.com
pr@ptsecurity.com