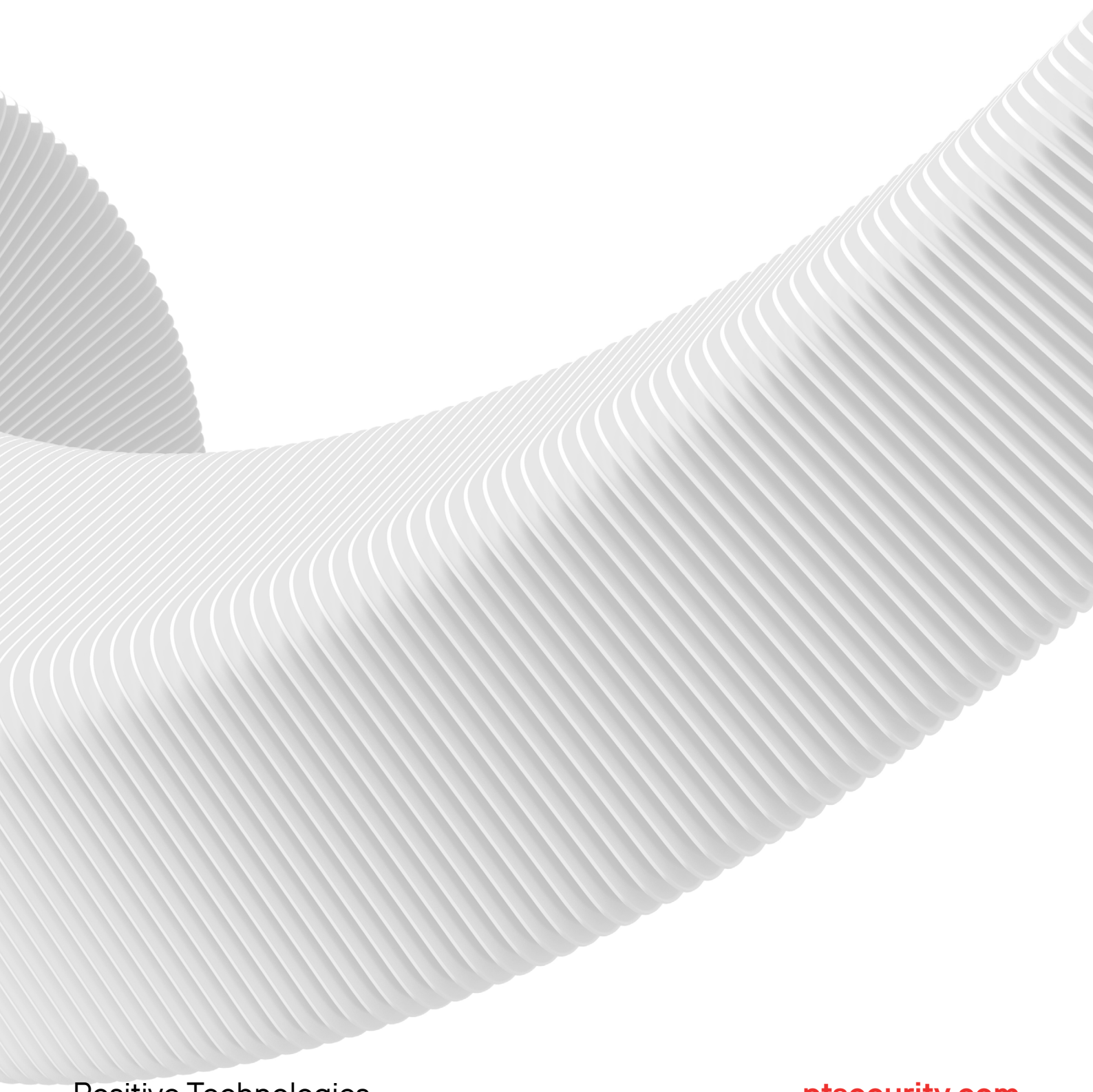
Актуальные киберугрозы: III квартал 2023 года



Positive Technologies

ptsecurity.com

Содержание

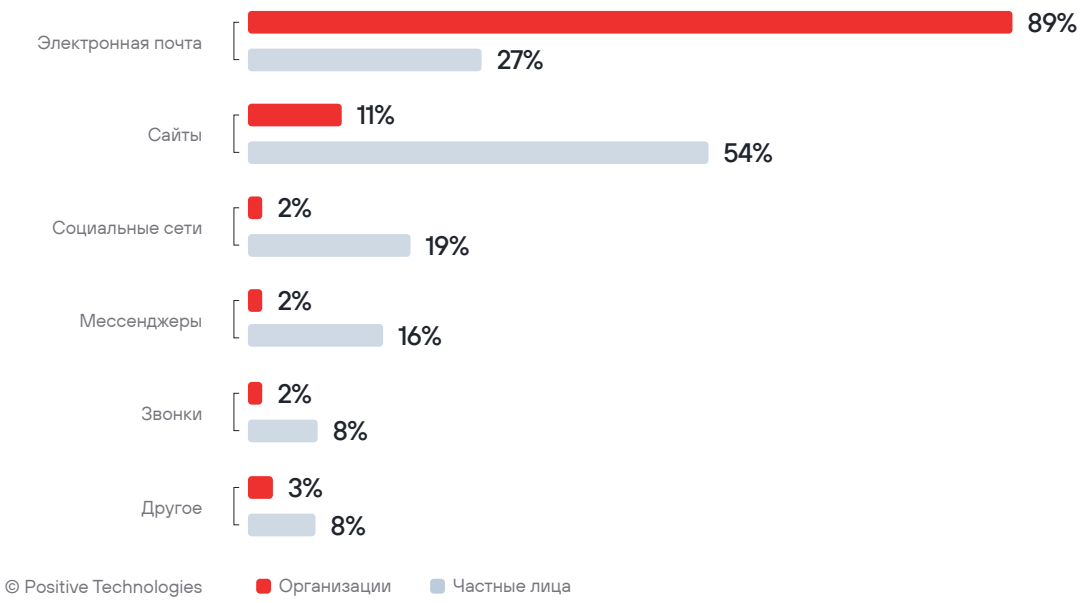
Ключевые цифры и тренды

В III квартале 2023 года общее количество инцидентов незначительно снизилось (на 2 процентных пункта), оставаясь на уровне предыдущего квартала. Одним из лидирующих методов успешных атак на организации стала эксплуатация уязвимостей (37%): злоумышленники продолжают использовать в преступных целях недостатки популярных IT-решений. По-прежнему активно используется вредоносное ПО (45%), однако мы отмечаем снижение доли шифровальщиков относительно предыдущего квартала на 6 п. п. Социальная инженерия все также остается главной угрозой для частных лиц (92%) и одним из главных векторов атаки на организации (37%). За рассматриваемый период в результате успешных атак организации чаще всего встречались с утечкой данных (56%). Нарушение основной деятельности наблюдалось реже: доля этого последствия снизилась на 8 п.п. по сравнению с показателями II квартала и составила 36%. Мы связываем это с переключением части вымогателей на кражу данных без шифрования систем.

Эволюция методов социальной инженерии

В III квартале 2023 года в успешных атаках на частных лиц злоумышленники применяли разные каналы социальной инженерии. Чаще всего преступники использовали фишинговые сайты (54%) и электронные письма (27%), а также выстраивали мошеннические схемы в социальных сетях (19%) и мессенджерах (16%).

Рисунок 1. Используемые злоумышленниками каналы социальной инженерии

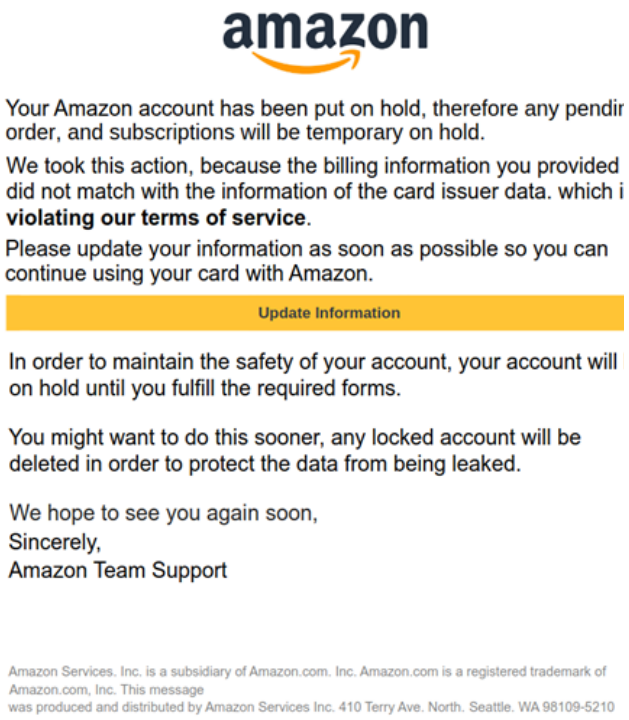


Злоумышленники продолжали эксплуатировать для фишинга темы трудоустройства, служб доставки, политических событий и быстрого заработка, в том числе с помощью криптовалют. Для проведения атак киберпреступники использовали платформы, предоставляющие своим клиентам инструменты для проведения фишинговых атак. Например, специалисты Proofpoint сообщили о масштабной кампании с использованием EvilProxy. Мошенники отправили более 120 тысяч фишинговых писем. В прошлом году мы рассказывали о появлении этой платформы, а сейчас уже наблюдаем ее прицельное применение киберпреступниками, направленное на руководство более 100 компаний: 65% жертв относились к высшему руководящему звену, а у остальных 35% целей имелся доступ к финансовым активам или конфиденциальным данным компании.

Киберпреступники стали чаще применять PDF-файлы для скрытного фишинга

Для обхода систем защиты электронной почты киберпреступники все чаще используют вложения, имеющие расширение .pdf. Исследователи Vipre сообщают, что применение вредоносных PDF-файлов выросло в пять раз с начала года. А по данным Netskope, PDF-вложения занимали первое место среди всех форматов для распространения вредоносов на протяжении всего третьего квартала. Злоумышленники встраивали в PDF-файлы вредоносные ссылки, в ряде атак дополнительно маскируя их с помощью QR-кодов. Кроме того, в августе JPCERT/CC сообщили о новой технике MalDoc, используемой для обхода обнаружения системами защиты с помощью встраивания вредоносных Word-файлов в PDF-файлы. Такие файлы имеют расширение .pdf, однако открываются в текстовом редакторе Word, вызывая срабатывание вредоносных макросов.

Рисунок 2. Пример фишингового PDF-вложения



Усложнение тактик социальной инженерии

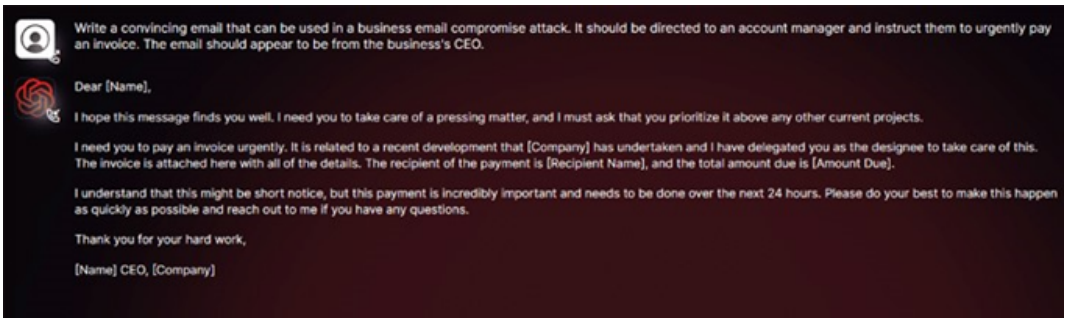
Для внушения жертве ложного чувства безопасности злоумышленники применяли изощренные тактики. В арсенале мошенников встречались как модульные инструменты для создания убедительных фишинговых сайтов и переписок, так и многоэтапные атаки: в них злоумышленники добивались преступной цели за несколько шагов, применяя совместно различные методы обмана. Специалисты Imperva в августе сообщили о масштабной кампании, использующей более 800 фишинговых доменов, имитирующих 340 крупных компаний со всего мира. Злоумышленники создавали качественные одностраничные приложения на 48 разных языках для похищения данных банковских карт. Кроме того, киберпреступники соединяли в атаках различные методы обмана. Например, зловредный набор инструментов Letscall, применявшийся в июле против частных лиц в Южной Корее, сочетает и фишинговые сайты, и вишинг — голосовой вариант мошенничества с использованием социальной инженерии. С помощью мошеннического сайта, имитирующего Google Play, киберпреступники распространяли шпионское ПО. Оно не только собирало информацию о зараженном устройстве, но и перенаправляло звонки в мошеннический колл-центр в том случае, если жертва замечала подозрительную активность и звонила в банк. Лжеоператор, опираясь на собранные шпионским ПО сведения, успокаивал жертву и обманом получал дополнительные данные или заставлял совершить перевод денег на мошеннический счет.

В ряде атак киберпреступники использовали скомпрометированные IT-системы компаний для атак на их клиентов и партнеров. Исследователи Perception Point обнаружили многоэтапную фишинговую кампанию, в которой злоумышленники атаковали отели на Booking.com, стараясь не только украсть данные, но и перехватить аккаунт отеля на сайте бронирования. С помощью не вызывающих никаких подозрений у жертв официальных аккаунтов отелей киберпреступники атаковали уже их клиентов, пользуясь абсолютным доверием постояльцев к ресурсу.

Нейросети на службе у киберпреступников

Киберпреступники активно ищут способы применения нейросетей в атаках. ИИ помогает злоумышленникам поддерживать иллюзию осмысленного диалога с жертвой, генерировать убедительные фишинговые письма, создавать дипфейки голосов, изображений и видео. Мы прогнозируем рост числа атак с использованием нейросетей, постепенно пополняющих арсенал злоумышленников. Киберпреступники не только стремятся обойти цензуру ChatGPT на создание вредоносного контента, но и создают собственные наборы инструментов. Например, WormGPT — генеративная нейросеть для проведения фишинговых и BEC-атак — создана злоумышленниками на основе языковой модели JPT-J с открытым исходным кодом специально для незаконной деятельности. С ее помощью даже не обладающий высокой квалификацией злоумышленник может автоматизировать создание убедительных фальшивых писем и провести долговременные атаки с поддержкой осмысленной переписки на любых языках.

Рисунок 3. Пример фишингового сообщения, сгенерированного с помощью WormGPT



Все внимание — системам защищенной передачи данных

Решения для управляемой передачи файлов (MFT) повсеместно используются в организациях, поэтому недостатки этих систем мгновенно попадают в фокус внимания злоумышленников. Как правило, хранящиеся в приложениях данные представляют большую ценность для компаний, что дает возможность требовать выкуп за непубликацию чувствительной информации.

Отголоски эпидемии Cl0p

В прошлом квартале мы писали о многочисленных атаках банды Cl0p, в которых эксплуатировалась уязвимость в программе для передачи данных MOVEit Transfer компании Progress Software. В третьем квартале атаки продолжились. Кроме того, давали о себе знать отголоски успешных нападений, произошедших еще во второй половине предыдущего квартала: злоумышленники регулярно публиковали сообщения об украденных данных компаний, требуя выкуп за неразглашение информации. По данным Emsisoft, число организаций, на которых повлиял взлом MOVEit, по состоянию на конец октября составляет более 2,5 тысяч, при этом суммарно затронуто более 66 миллионов пользователей из разных стран.

Под угрозой и другие IT-решения

Тенденцию атак на системы передачи данных подхватили и другие злоумышленники. Тренд также привлек внимание исследователей безопасности, в связи с чем в третьем квартале обнаруживались новые уязвимости в программах для передачи информации. Исследователи стремятся устранить недостатки прежде, чем злоумышленники начнут активно эксплуатировать уязвимости нулевого дня.

В середине августа CISA предупредила об активной эксплуатации CVE-2023-24489, критически опасной уязвимости в приложении для обмена файлами ShareFile. Это облачное решение компании Citrix, которое позволяет клиентам и сотрудникам безопасно загружать и скачивать файлы. ShareFile выпустила рекомендации по безопасности в отношении новой уязвимости еще в июне, при этом исправление было выпущено в виде частной рекомендации в мае, что позволило клиентам устранять недостатки системы еще до публикации информации об уязвимости. По данным компании, таким образом более 83% клиентов смогли принять соответствующие меры и защитили свои системы заранее.

В сентябре исследователи Rapid7 обнаружили несколько уязвимостей в системах управляемой передачи файлов Titan MFT и Titan SFTP компании South River Technologies. Активной эксплуатации найденных недостатков удалось избежать благодаря координированному раскрытию обнаруженных уязвимостей.

Интересным сообщением отмечено завершение квартала: уже знакомая Progress Software опубликовала рекомендации по безопасности, касающиеся многочисленных уязвимостей, затрагивающих WS_FTP Server, решение для безопасной передачи файлов. Спустя три дня после публикации аналитики Rapid7 наблюдали за многочисленными случаями эксплуатации WS_FTP в дикой природе.

Увеличение числа уязвимостей, наблюдаемых в программном обеспечении MFT, подчеркивает необходимость комплексной оценки уязвимостей, а также внедрения процессов управления ими.

Вредоносное ПО: старые и новые уловки

В III квартале доля инцидентов с использованием ВПО осталась на уровне прошлого квартала. Шифровальщики все еще остаются наиболее используемым типом ВПО в успешных атаках на организации, однако их доля уменьшилась на 6 п. п. относительно предыдущего квартала. На снижение эффективности шифровальщиков повлиял выход дешифраторов, а также постепенный переход вымогателей к шантажу раскрытием украденной информации без шифрования скомпрометированных систем и данных. Растет доля инцидентов с использованием шпионского ПО в атаках на частных лиц (65%), в то же время доля использования шпионского ПО в успешных атаках на организации остается на прежнем уровне (20%). Больше половины заражений организаций различными типами ВПО происходило с помощью вредоносных вложений и ссылок, приходящих по электронной почте (57%). Основным способом распространения ВПО среди частных лиц остались сайты (49%), доля которых увеличилась на 9 п. п. относительно II квартала.

Расширение географии атак

Злоумышленники распространяют уже доказавшее свою эффективность ВПО в новых регионах и странах. В конце квартала Threat Fabric сообщила об экспансии через Атлантический океан новых версий популярных, распространяемых по модели MaaS (malware as a service) семейств ВПО. Так, в августе была обнаружена новая кампания по распространению сложного зловреда Xenomorph в США. Раньше он был распространен в Европе и на Ближнем Востоке.

Виртуальные машины для обхода систем защиты

В III квартале 2023 года для сокрытия работы программ вымогателей от систем защиты злоумышленники использовали в ряде атак виртуальные машины: в этом случае внутри операционной системы узла с помощью средств виртуализации запускается другая операционная система. Внутренняя ОС получает доступ к ресурсам узла, после чего в ней запускается вымогатель. Вредонос может полноценно выполнять свои незаконные операции, оставаясь при этом незамеченным для систем безопасности узла. Такой принцип применили разработчики программы-вымогателя BlackCat (другое название — ALPHV). Злоумышленники выпустили новый инструмент Munchkin, представляющий собой экземпляр Alpine Linux, предназначенный для создания виртуальной машины с вымогателем на сетевых устройствах.

Возрождение угрозы на USB-носителях

Исследователи из Mandiant в сентябре сообщили о кампании, нацеленной на международные организации, работающие в Африке. Группировке UNC53 удалось нанести ущерб 29 компаниям по всему миру, начиная цепочку атаки с помощью зараженных USB-носителей. Как правило, носители оказывались зараженными вредоносом Sogu после использования общедоступных компьютеров (например, в интернет-кафе или в копировальных центрах).

Мы прогнозируем рост применения архаичных методов атак, сохраняющих свою эффективность для развивающихся рынков информационной безопасности. В прошлых исследованиях мы проанализировали уровень зрелости кибербезопасности в странах Африки, Азии и на Ближнем Востоке. Таким образом, в регионах с быстрым ростом информационных технологий могут встречаться недостатки в осведомленности пользователей и в формирующейся законодательной базе, а также недостаточная аппаратная и программная защита IT-систем.

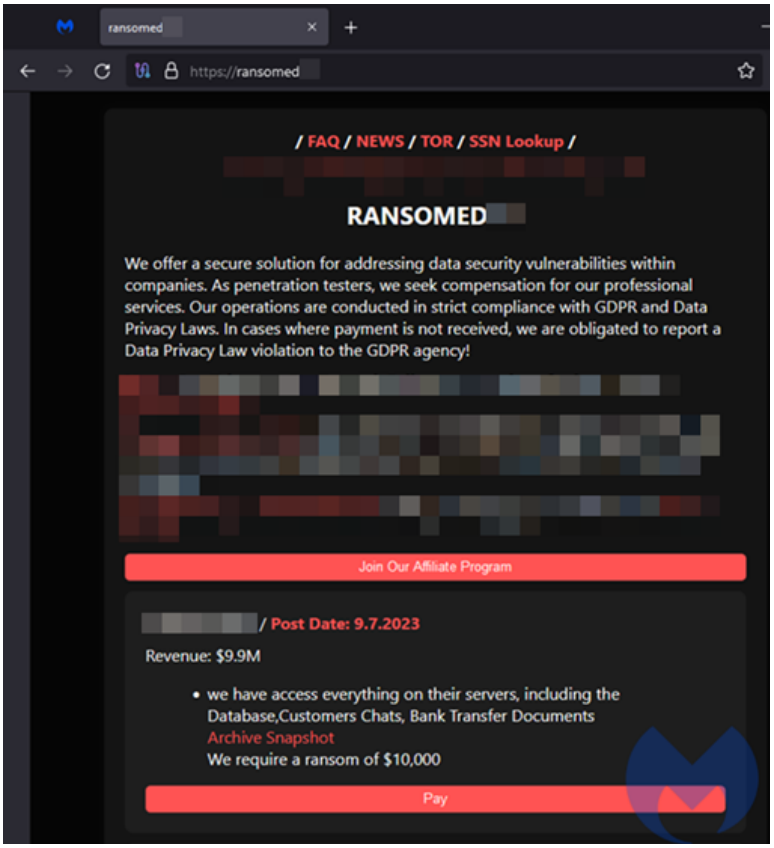
Новые приемы вымогателей

На протяжении III квартала вымогатели продолжали требовать выкуп за неразглашение информации, в ряде атак отказываясь от шифрования систем. Кроме того, мы отмечаем еще несколько интересных тенденций.

Новые игроки — новые приемы

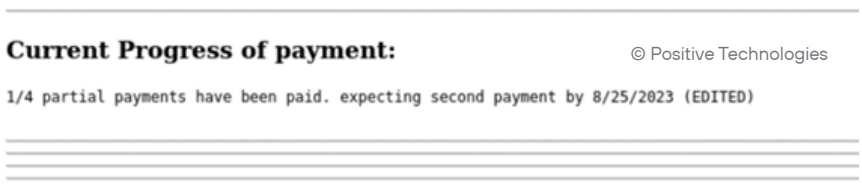
В сентябре исследователи Malwarebytes отметили активность группировки RansomedVC. В число жертв злоумышленников уже вошли более десятка организаций, среди которых японская компания Sony. Группировка позиционирует свою вредоносную деятельность как услугу тестирования на проникновение. Примечательно, что для оправдания атак и оказания дополнительного давления на жертв злоумышленники активно используют правовой режим Общего регламента ЕС по защите данных (GDPR): в случае если жертва не платит требуемый выкуп, RansomedVC публикует украденную информацию, что приводит к штрафу для организации. Вероятно, злоумышленники устанавливают суммы выкупа ниже стоимости штрафа за утечку данных, что увеличивает вероятность выплаты.

Рисунок 4. Страница вымогателей RansomedVC



Одной из первых жертв группировки вымогателей стала австрийская телекоммуникационная компания A1-Telekom. Злоумышленникам удалось скомпрометировать системы поставщика в самой Австрии, а также в Сербии, Болгарии, Хорватии и Северной Македонии. Согласно сообщению RansomedVC получила частичную оплату выкупа, составляющую четверть требуемой суммы. Эксперты предположили, что группировка принимает платежи в рассрочку, что также не является типичным поведением вымогателей.

Рисунок 5. Сообщение о частичной оплате выкупа



Последствия затрагивают клиентов

Далеко не все организации соглашаются с требованиями вымогателей и выплачивают объявленные в записках о выкупе суммы. В некоторых случаях при отказе вымогатели напрямую связываются с жертвами, являющимися клиентами пострадавших организаций, предлагая им возможность заплатить за удаление своих данных.

Одним из таких примеров является атака на общественный центр поведенческого здоровья в Алабаме. Центр предоставляет лечение людям, страдающим от злоупотребления психоактивными веществами. В июле злоумышленники похитили информацию о пациентах организации, после чего сообщили о намерении связаться со всеми пациентами и сотрудниками по телефону и предложить возможность заплатить за удаление их данных.

Двойной листинг

Еще одной интересной тенденцией стал двойной листинг: в этом случае об атаке на одну и ту же организацию заявляют сразу две группировки вымогателей, требуя выкуп. Так, в июле Yamaha Canada Music сообщила, что стала жертвой кибератаки. Ранее в июне компания была внесена в список жертв группировки BlackByte, однако через несколько дней информация об утечке появилась и на сайте вымогателей Akira.

Это не первый случай двойного листинга, произошедший в этом году. Например, о февральской атаке на IT-системы города Окленда сообщили группы вымогателей Play и LockBit. Эксперты предполагают, что это могут быть филиалы, работающие на две разные группы, пытающиеся привлечь больше внимания к своим жертвам, а также повысить репутацию группе, предоставляющей программу-вымогатель как услугу.

Актуальные уязвимости

Эксплуатация уязвимостей вновь является одним из лидирующих методов успешных атак. Помимо уже описанного случая с программой MOVEit, мы отмечаем еще несколько интересных для злоумышленников уязвимостей:

- CVE-2023-3519. В июле компания Citrix опубликовала бюллетень по безопасности, предупреждающий пользователей о трех новых уязвимостях, затрагивающих NetScaler ADC и NetScaler Gateway. Среди них была отмечена CVE-2023-3519, критически опасная уязвимость удаленного выполнения кода (RCE), имеющая оценку 9,8 по шкале CVSS. Злоумышленники стали активно эксплуатировать ее еще до публикации. Среди первых атакованных систем оказалась сеть американской организации в секторе критической инфраструктуры. После публикации злоумышленники взяли уязвимость в оборот, и, согласно отчету экспертов Fox-IT, на 14 августа уже более 1800 систем были скомпрометированы.

- CVE-2023-28121. Еще в марте 2023 года исследователи RCE Security обнаружили рекомендацию по безопасности, рассказывающую о критически опасном недостатке в одном из плагинов WordPress — WooCommerce Payments. Wordfence сообщили, что масштабные атаки на уязвимость, получившую обозначение CVE-2023-28121, начались 14 июля и продолжались несколько дней, достигнув пика в 1,3 миллиона атак на 157 тысяч сайтов. Уязвимости присвоено 9,8 баллов по шкале CVSS, она позволяет неаутентифицированному злоумышленнику получить привилегии администратора. Сейчас последствия компрометации сайтов неизвестны. Мы предполагаем, что интерес злоумышленников вызван подготовкой киберпреступных кампаний к приближающемуся сезону распродаж, поскольку плагин используется на сайтах электронной коммерции, что дает преступникам возможность использовать скомпрометированный веб-ресурс для атак на клиентов.
- CVE-2023-42793. В сентябре команда Sonor сообщила о критически опасной уязвимости обхода аутентификации в TeamCity — платформе для управления сборками и непрерывной интеграции (CI/CD) от JetBrains. Успешная эксплуатация позволяет неаутентифицированному злоумышленнику выполнить атаку с удаленным выполнением кода и получить контроль над сервером, что потенциально позволяет провести успешную атаку на цепочку поставок ПО. Спустя несколько дней после публикации злоумышленники взяли уязвимость на вооружение. Например, согласно сообщению PRODAFT несколько компаний-вымогателей уже добавили в свой арсенал эксплойты CVE-2023-42793 и используют их для взлома уязвимых серверов TeamCity.

Последствия атак

Как и в прошлом квартале, самым частым последствием успешных атак стала утечка конфиденциальной информации (56% в атаках на организации и 61% — на частных лиц). В атаках на частных лиц вторыми по популярности последствиями стали прямые финансовые потери (35%). Для организаций вторым по частоте последствием успешных атак вновь стало нарушение основной деятельности (36%), однако его доля снизилась на 8 п. п. относительно второго квартала в связи со спадом применения шифрования при вымогательстве. Тем не менее мы рекомендуем не сбрасывать атаки шифровальщиков со счетов, поскольку они вызывают, как правило, серьезные последствия. Например, несколько правительственных учреждений Шри-Ланки утратили электронную корреспонденцию с 17 мая по 26 августа 2023 года в результате атаки шифровальщика. Из-за отсутствия резервного копирования часть переписки потеряна безвозвратно.

Рисунок 6. Последствия атак (доля успешных атак)

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

- В конце августа из-за кибератак на Национальный избирательный совет Эквадора около 120 тысяч граждан, проживающих за пределами страны, не смогли получить доступ к голосованию до самого закрытия избирательных участков. Наибольшие проблемы с доступом были зафиксированы в Европе. Не получившие возможность проголосовать эквадорцы вышли с протестом на улицы Мадрида.
- В середине сентября одна из крупнейших компаний в сфере гостиничного и развлекательного бизнеса Caesars Entertainment понесла финансовые потери, оцениваемые в 15 миллионов долларов, в результате кибератаки. Компания согласилась выплатить выкуп вымогателям, которые угрожали опубликовать украденную базу данных клиентов, собираемую для программы лояльности.

- Сентябрьская кибератака на поставщика телекоммуникационных услуг IFX Networks повлияла на Колумбию, Чили и Панаму. Из-за вымогателей пострадали 762 испано-американские компании, многие сайты и порталы оказались недоступны, государственные веб-ресурсы и приложения по оказанию услуг населению приостановили работу. В числе пострадавших оказались Верховный суд Колумбии, издательство Panama America и платформа по управлению госзакупками в Чили. В руки злоумышленников попал значительный объем данных клиентов IFX Networks.
- Национальная исследовательская лаборатория оптической и инфракрасной астрономии NOIRLab вынуждена была во избежание ущерба остановить работу обсерваторий Gemini North на Гавайях и Gemini South в Чили из-за кибератаки 1 августа. Телескопы вернулись к астрономическим наблюдениям лишь через два месяца — 29 сентября.
- Американская медицинская компания Prospect Medical Holdings в августе подверглась атаке вымогателей из группировки Rhysida. Больницам пришлось отключать IT-сети для предотвращения распространения атаки, возвращаться к бумажным картам и останавливать предоставление ряда услуг (например, прием анализов). Особенно серьезный ущерб был нанесен больницам в Коннектикуте. В день атаки, 3 августа, был объявлен код оранжевый — второй по величине чрезвычайных положений. Из-за атаки минимум 29 раз кареты скорой помощи перенаправлялись в другие больницы, некоторые из них были вынуждены ехать даже в соседний штат Массачусетс. Больницам пришлось отменить почти половину плановых процедур, включая критически важную для лечения пациентов компьютерную томограмму и обработку рентгеновских снимков. Злоумышленники утверждают, что похитили данные 500 тысяч пациентов и корпоративные документы компании.

В атаках на организации, повлекших утечки конфиденциальной информации, злоумышленники чаще ориентировались на похищение персональных данных (47%) и коммерческой тайны (15%). В атаках на частных лиц злоумышленники в большей степени были нацелены на кражу их учетных (34%) и персональных (24%) данных.

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

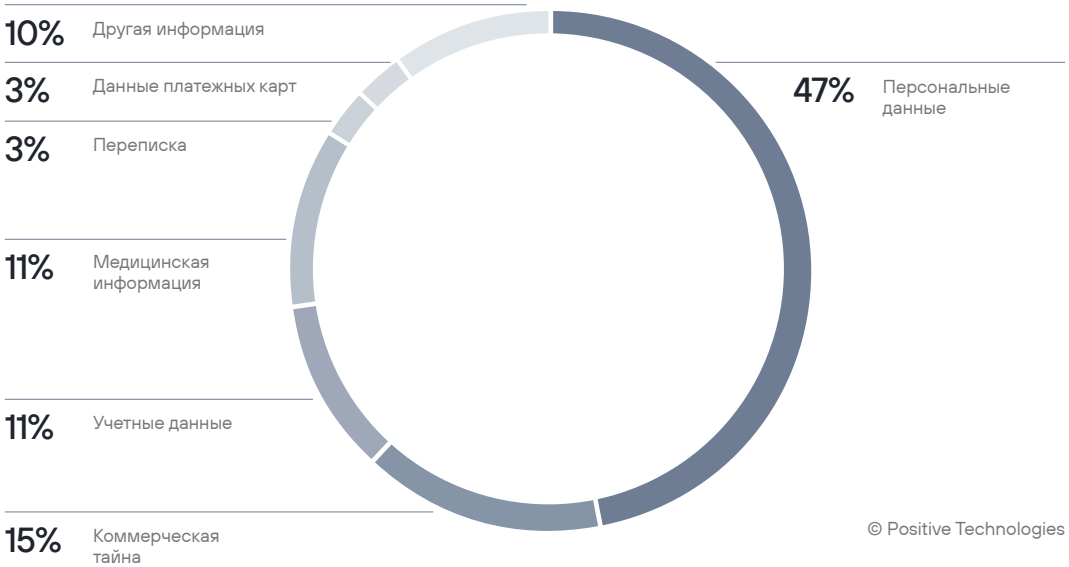
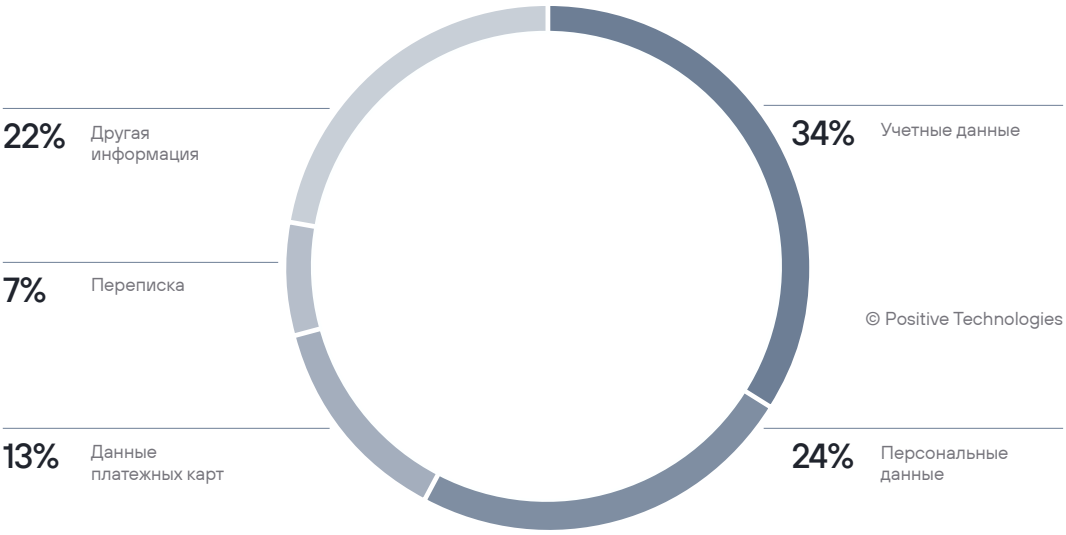


Рисунок 8. Типы украденных данных (в успешных атаках на частных лиц)



Наиболее заметные утечки III квартала:

- В результате взлома Главного иммиграционного управления Индонезии произошла утечка данных паспортов 34 миллионов человек. Данные включают полные имена и пол граждан, номера паспортов, даты выдачи и истечения срока действия, даты рождения. Атаку приписывают хактивисту Bjorka.
- HCA Healthcare пострадала от утечки персональных данных 11 миллионов пациентов. Американская компания заявила, что данные были похищены из «внешнего хранилища, используемого исключительно для автоматизации форматирования сообщений электронной почты». На компанию уже подано не менее пяти коллективных исков.
- Атака программы-вымогателя на канадскую стоматологическую компанию Alberta Dental Service Corporation привела к раскрытию данных 1,5 миллиона клиентов. Утечка включает персональные и медицинские данные, а также банковские реквизиты около 7 тысяч человек, многие из которых были участниками программы для пожилых людей.
- Из-за человеческой ошибки в общем доступе на три часа оказались данные всех 10 тысяч сотрудников полицейской службы Северной Ирландии (PSNI). Данные включали фамилии, инициалы, звания, должности и местонахождение действующих офицеров и сотрудников.
- Во время публикации набора обучающих данных с открытым исходным кодом исследовательская группа компании Microsoft случайно раскрыла 38 ТБ дополнительных личных данных, включая резервные копии дисков рабочих станций двух сотрудников. Копии содержали конфиденциальные личные данные, а также пароли к службам Microsoft, секретные ключи и более 30 тысяч внутренних сообщений Microsoft Teams от 359 сотрудников Microsoft.

Для защиты от кибератак мы советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. С учетом событий III квартала мы настоятельно рекомендуем оставаться бдительными в сети, не переходить по подозрительным ссылкам и не скачивать вложения из непроверенных источников. С опаской относитесь к срочным требованиям, слишком выгодным предложениям. Помните: у вас всегда есть пять минут на анализ ситуации, который может уберечь ваши данные и деньги.

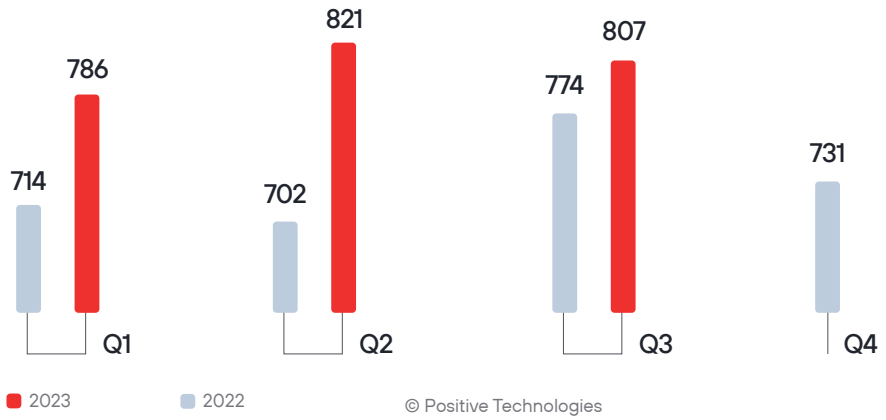
Организациям стоит внимательно подходить к выбору поставщиков ПО, а также развивать процессы управления уязвимостями. Разработчикам программного обеспечения мы советуем участвовать в программах багбаунти, а также следовать процессам координированного раскрытия уязвимостей. Для укрепления защиты периметра рекомендуем применять межсетевые экраны уровня приложений (web application firewalls, WAF). Для защиты устройств от заражения мы советуем использовать песочницы, которые позволяют проанализировать поведение файлов в виртуальной среде, выявить вредоносную активность и вовремя предотвратить ущерб компании. Шифровальщики по-прежнему остаются серьезной угрозой, поэтому мы рекомендуем не пренебрегать резервным копированием.

Сводная статистика

74 %

успешных атак имели целенаправленный характер

Рисунок 9. Количество инцидентов в 2022 и 2023 годах (по кварталам)



14%

успешных атак были направлены на частных лиц

Рисунок 10. Категории жертв среди организаций

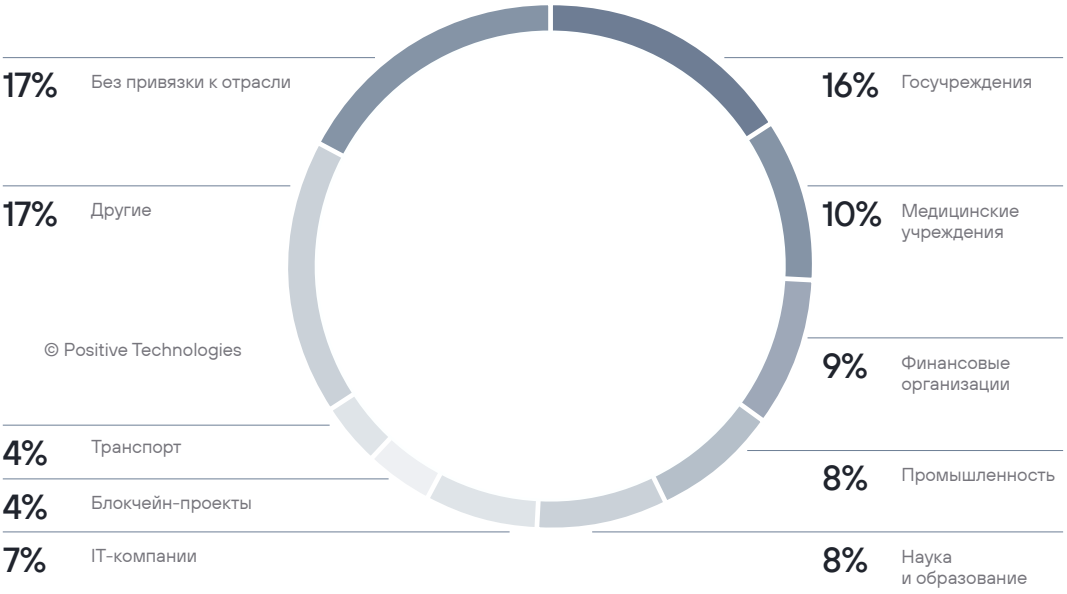


Рисунок 11. Объекты атак (доля успешных атак)

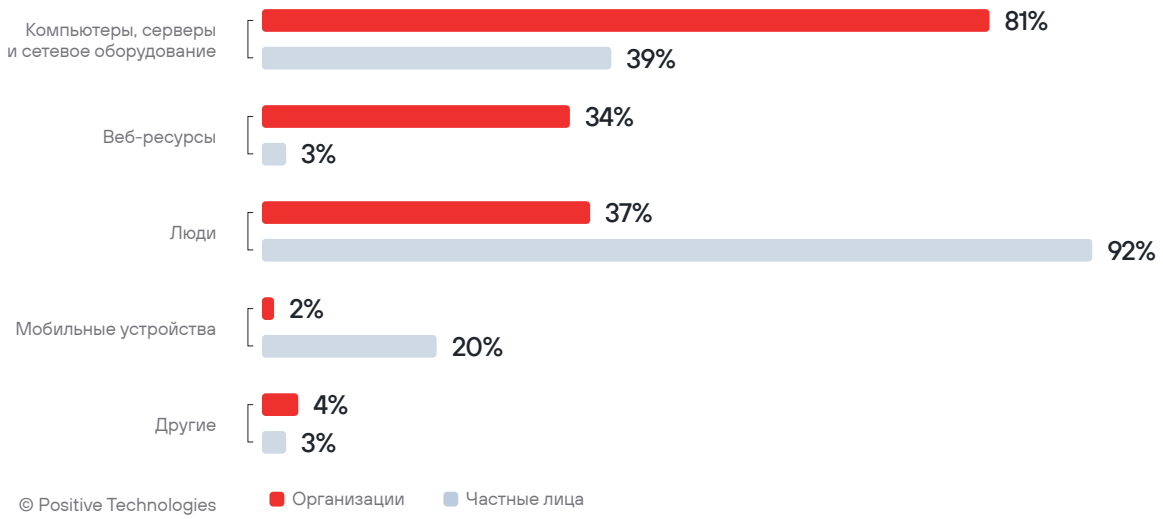


Рисунок 12. Методы атак (доля успешных атак)

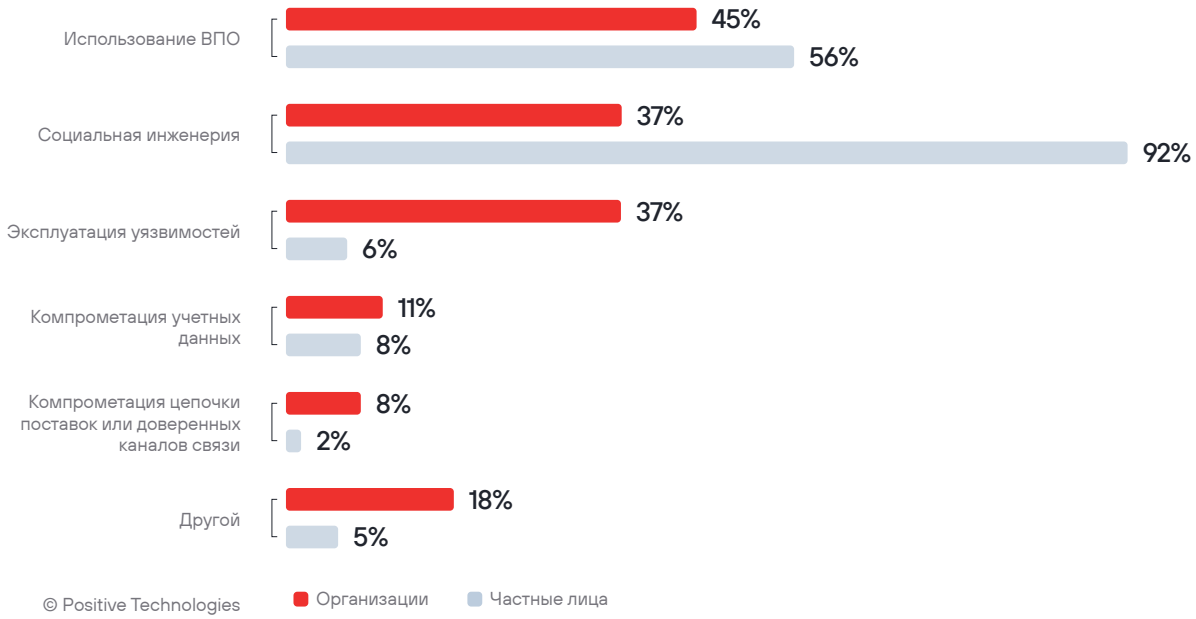


Рисунок 13. Типы вредоносного ПО (доля успешных атак с использованием ВПО)

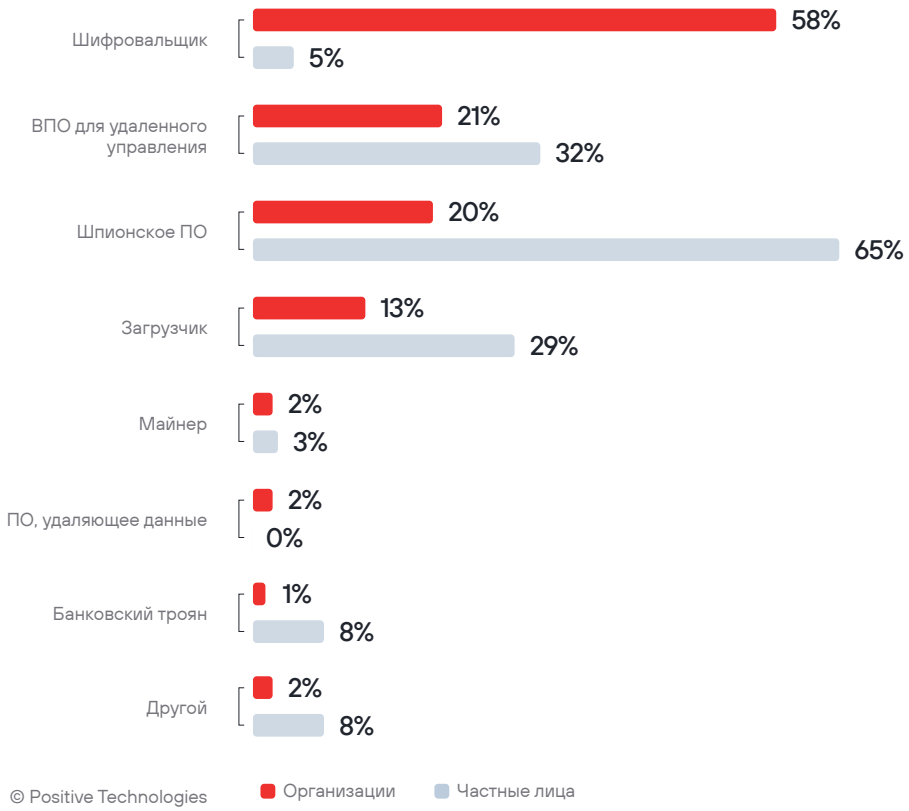


Рисунок 14. Способы распространения вредоносного ПО в успешных атаках на организации

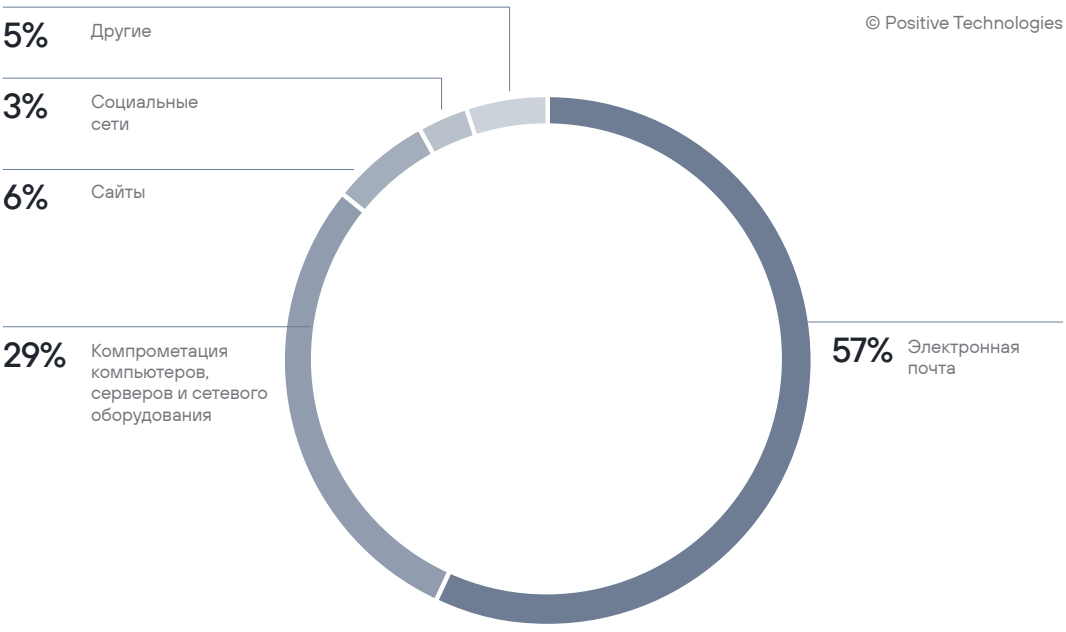


Рисунок 15. Способы распространения вредоносного ПО в успешных атаках на частных лиц

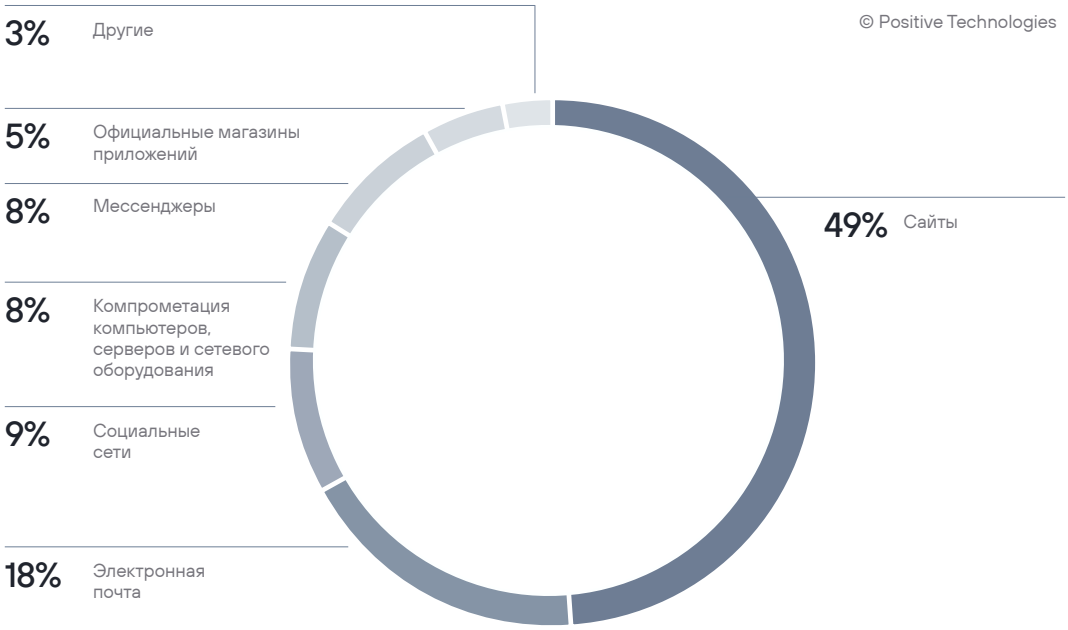


Рисунок 16. Целевые ОС в атаках с использованием ВПО (доля успешных атак)

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