Актуальные киберугрозы: IV квартал 2022 года

Positive Technologies

ptsecurity.com

Содержание

Ключевые цифры и тренды

В IV квартале 2022 года количество инцидентов уменьшилось на 5% по сравнению с предыдущим кварталом, хотя все еще остается достаточно высоким — на 15% больше, чем за аналогичный период 2021 года. Продолжается увеличение доли массовых атак: в IV квартале она выросла на 2 процентных пункта. Чаще всего успешные кибератаки приводили к утечкам конфиденциальной информации (51%) и нарушениям основной деятельности предприятий (36%). Наблюдались случаи перебоев в работе критически значимой инфраструктуры, крупные утечки данных пользователей и исходных кодов продуктов.

Растет доля использования шпионского ПО

[1] Кибератака, в ходе которой злоумышленники взламывают компанию путем компрометации поставщиков ПО или оборудования. Например, преступники могут внедрить вредоносный код в исходный код продукта или распространить вредоносные обновления, чтобы заразить инфраструктуру целевой организации.

Увеличивается доля атак с использованием шпионского ПО: 17% таких атак было совершено в отношении организаций, 49% — в отношении частных лиц; это соответственно на 5 п. п. и 3 п. п. больше показателей прошлого квартала. Злоумышленники создают новые вредоносы и работают над расширением их функциональности: так, в новом стилере Aurora появилась функция кражи данных не только из браузеров или буфера обмена, но и непосредственно с диска устройства. Распространение вирусов-шпионов по схеме «вредонос как услуга» позволяет использовать их даже неопытным злоумышленникам: исследователи Positive Technologies проанализировали новый стилер BlueFox, который активно продвигается на подпольном рынке по такой схеме. Кроме того, участились случаи встраивания вредоносного кода, который выполняет функции шпионского ПО, в пакеты для разработчиков Python — это может привести к росту числа атак типа supply chain[1] и компрометации сетей IT-компаний.

Ботнеты и ВПО для удаленного управления

[2] ВПО, проверяющее буфер обмена на наличие адреса криптокошелька и подменяющее его на указанные злоумышленником реквизиты.

[3] Вредоносная полезная нагрузка для получения удаленного доступа к скомпрометированным системам, сбора данных или загрузки дополнительного ВПО.

В IV квартале был отмечен рост числа случаев использования вредоносов для удаленного управления: доля использования этого вида ВПО в атаках на организации выросла на 6 п. п. относительно прошлого квартала. Были обнаружены новые ботнеты: MCCrash, способный атаковать Windows- и Linux-системы, и GoTrim, взламывающий уязвимые сайты WordPress и способный обходить защиту от ботов. Вернулись и старые угрозы: ботнет SmokeLoader был замечен исследователями из Cyble за распространением нового криптоклиппера[2] Laplas; ботнеты QakBot и вернувшийся после затишья Emotet были использованы для доставки различного ВПО, в том числе шифровальщика Black Basta, маяков[3] Brute Ratel и Cobalt Strike.

Новые кроссплатформенные шифровальщики и способы шифрования

Группировки RansomExx и Qilin обзавелись кроссплатформенными версиями своих программ-вымогателей, написанными на Rust, что позволило им нацеливаться на Windows- и Linux-системы. Злоумышленники все чаще используют прерывистое шифрование файлов с определенным побайтовым шагом — такой подход делает шифрование быстрым и менее заметным для средств мониторинга за счет меньшего количества операций над шифруемым файлом и его схожести с оригиналом. После некоторого затишья вновь стали активны вайперы, маскирующиеся под шифровальщики: такое ВПО преобразует данные и оставляет записку о выкупе, однако платеж не поможет вернуть данные, так как они не подлежат восстановлению.

Список громких атак не перестает пополняться: атака вымогателей на правительство французского заморского департамента Гваделупа вывела из строя практически всю государственную IT-инфраструктуру; группировке Daixin Team удалось похитить информацию о пяти миллионах пассажиров авиакомпании AirAsia и зашифровать ее серверы.

Рост числа кибератак на страховой сектор

В IV квартале мы отмечаем рост количества успешных кибератак на страховые компании более чем в два раза по сравнению с прошлым кварталом. В 73% атак результатом стала утечка информации о клиентах: в основном это персональные данные; в ряде случаев была также скомпрометирована медицинская информация. Украденные данные продаются на теневом рынке либо используются злоумышленниками для последующих атак. Информация о страховании может иметь особое значение для вымогателей: если они узнают о наличии у организации киберстраховки, покрывающей выкуп, и сумму покрытия, то такие организации могут стать следующими целями для шифровальщиков — ведь вероятность отказа в уплате выкупа минимальна.

Атаки на IT-компании и межотраслевые последствия

IT-компании вызывают интерес злоумышленников, поскольку их компрометация может позволить провести атаки на клиентов — пользователей продуктов и сервисов (атаки типа supply chain и trusted relationship[4]), которые приведут к серьезным последствиям. Количество инцидентов, связанных с IT-компаниями, выросло за квартал на 18%. В 62% из них использовалось ВПО; преимущественно это были атаки шифровальщиков, направленные на кражу конфиденциальной информации и получение выкупа.

Жертвами злоумышленников становились в том числе поставщики ПО для различных отраслевых организаций. Нашумевшей стала атака на Supeo, поставщика IT-услуг для датской железнодорожной компании: в результате действий злоумышленников было временно приостановлено движение поездов. Сбои в работе приложения поставщика не позволяли машинистам получить доступ к критически важной информации — данным о работах на путях и об ограничениях скорости, вследствие чего составы были остановлены.

[4] Кибератака, в ходе которой злоумышленники взламывают инфраструктуру сторонней компании, у сотрудников которой есть легитимный доступ к ресурсам жертвы.

Частных лиц все чаще атакуют в социальных сетях и мессенджерах

В IV квартале частные лица чаще становились жертвами злоумышленников: доля атак на граждан в общем числе атак стала больше на 5 п. п., чем в предыдущем квартале. Продолжается рост количества успешных атак на частных лиц через социальные сети и мессенджеры. В III квартале 2022 года 18% атак с использованием социальной инженерии были направлены на пользователей социальных сетей, а мессенджеры и SMS-сообщения использовались в 15% таких атак. В IV квартале злоумышленники были не менее активны: на пользователей в социальных сетях было направлено 19% атак, а мессенджеры и SMS-сообщения применялись в 17% случаев использования социальной инженерии. Увеличивается доля украденных учетных данных: с 39% в III квартале до 44% в IV квартале.

Большинство успешных атак в социальных сетях и мессенджерах направлены на сбор учетных данных и взлом аккаунтов, а скомпрометированные учетные записи используются для дальнейших атак на пользователей. В одной из таких атак мошенники просили проголосовать онлайн якобы за родственника или знакомого в детском конкурсе, при этом ссылка вела на фишинговый сайт. В другой атаке, зафиксированной в декабре, пользователям Telegram массово приходили фейковые сообщения о подаренной подписке Telegram Premium. Чтобы ее активировать, предлагалось ввести код авторизации, однако это приводило к компрометации аккаунта и дальнейшей рассылке фишинговых писем контактам жертвы.

Спросом пользуются не только учетные данные, но и персональные, а также данные платежных карт. В одной из атак, нацеленной на граждан Индии, злоумышленники действовали необычным образом: они отслеживали сообщения пользователей Twitter, содержащие жалобы на Индийскую железнодорожную корпорацию общественного питания и туризма, связывались с ними, притворяясь сотрудниками службы поддержки, и запрашивали личную информацию.

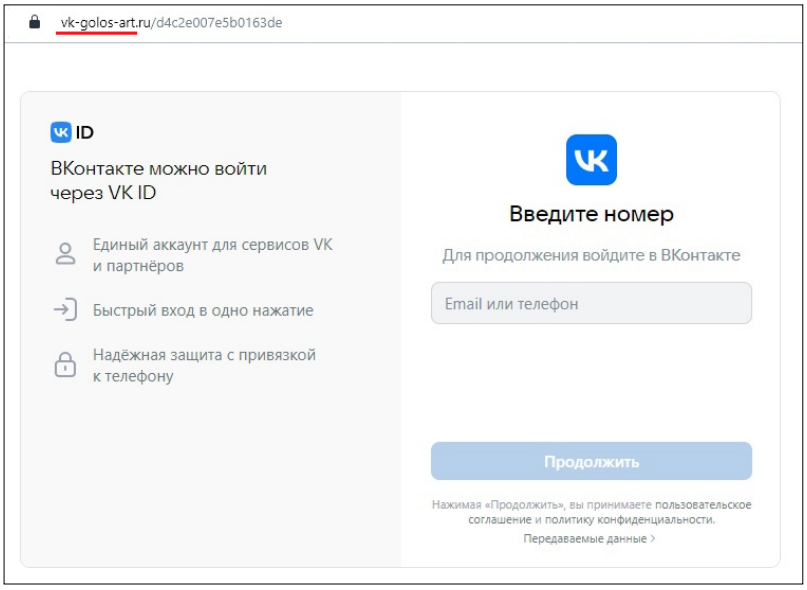

Рисунок 1. Фишинговая форма ввода

Для защиты от кибератак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. С учетом специфики инцидентов в IV квартале 2022 года 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; загружать приложения только из доверенных источников; применять открытый код только после проверки на наличие вредоносных модулей; использовать решения для резервного копирования файлов и своевременно устанавливать обновления безопасности. Кроме того, мы советуем проводить тщательные расследования всех крупных инцидентов, чтобы выявить точки компрометации и уязвимости, которыми воспользовались злоумышленники, а также своевременно убедиться в том, что преступники не оставили себе запасных входов. Укрепить безопасность на периметре компании можно с помощью современных средств защиты, к примеру межсетевых экранов уровня приложений (web application firewalls, WAF) для защиты веб-ресурсов. Чтобы предотвратить заражение вредоносным ПО, советуем использовать песочницы, которые анализируют поведение файлов в виртуальной среде и выявляют вредоносную активность.

Последствия атак

Последствия атак IV квартала носили разнообразный характер и оказывали разное влияние: успешные кибератаки затрагивали как малые предприятия, так и группы компаний или даже целые государства. Основной целью преступников было получение конфиденциальной информации. Кроме того, наблюдались случаи крупных финансовых потерь из-за действий злоумышленников, нарушения основной деятельности организаций, а иногда — критически значимой инфраструктуры.

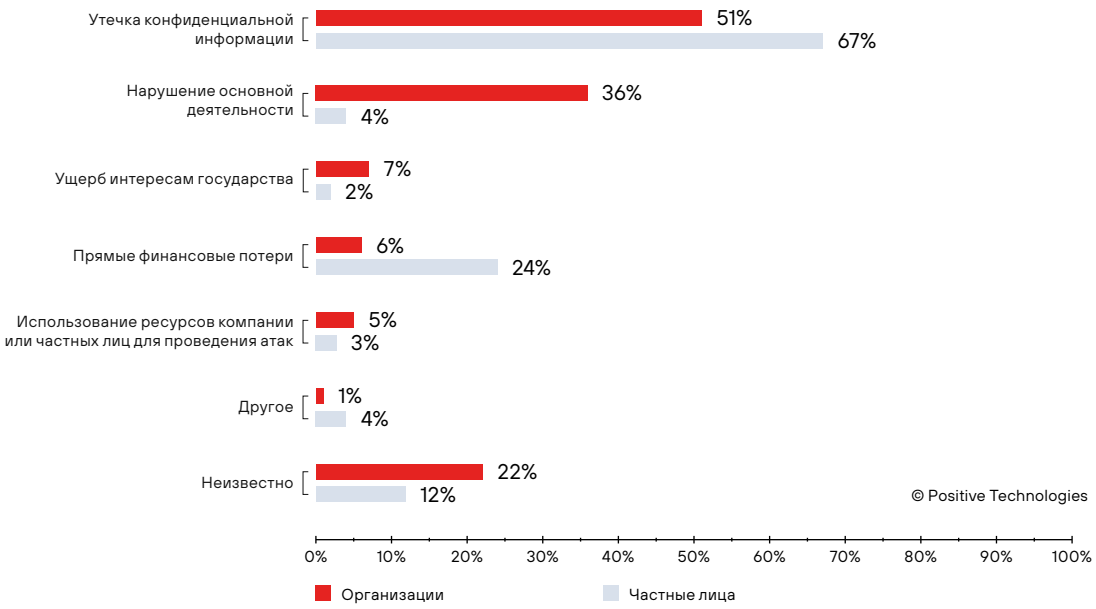

Рисунок 3. Последствия атак злоумышленников (доля атак)

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

- Атака на поставщика электроэнергии ECG в Гане. В результате атаки программы-вымогателя были недоступны сервисы для оплаты и покупки электроэнергии, что вызвало перебои в электроснабжении. В некоторых областях страны жители несколько дней оставались без электричества.

- Страховая компания Medibank подтвердила факт атаки программы-вымогателя, в результате которой была нарушена работа онлайн-сервисов и IT-инфраструктуры компании, после чего злоумышленники выложили в открытый доступ информацию о клиентах, в том числе сведения о состоянии здоровья и поставленных диагнозах.

- Пароли и другая информация для получения доступа к системе — лучшая находка для преступников. Взлом хранилища паролей LastPass позволил злоумышленникам получить очень ценные данные, такие как URL-адреса клиентов, их IP-адреса, логины и шифрованные пароли.

- Атаки на разработчиков решений многофакторной аутентификации и идентификации набирают обороты: в IV квартале компания Okta стала жертвой очередной успешной кибератаки злоумышленников — она стала для компании четвертой по счету в 2022 году. Преступникам удалось скопировать исходный код продукта Workforce Identity Cloud, который используется для идентификации пользователей и управления привилегированным доступом в облаке.

- Один из крупнейших майнинговых пулов BIT Mining был атакован злоумышленниками. В результате были украдены активы пользователей BTC.com на сумму 700 тыс. долларов, а сам пул потерял 2,3 млн долларов в криптовалюте. Позже стало известно, что злоумышленникам удалось отправить украденные активы в миксер Tornado Cash, а акции BIT Mining потеряли 20% своей цены.

Четвертый квартал отметился громкими утечками данных, похищенных в результате кибератак на организации. Злоумышленники в таких атаках чаще ориентировались на похищение персональных данных (38%) и коммерческой тайны (20%).

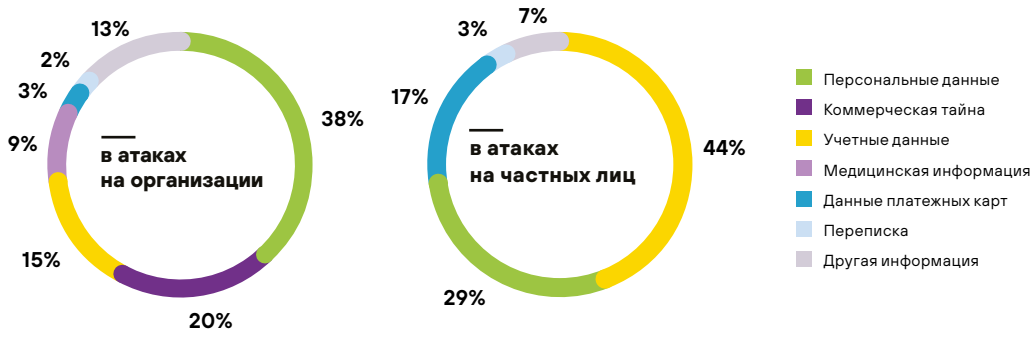

Рисунок 4. Типы украденных данных

Наиболее заметные утечки IV квартала:

- Утечка исходного кода UEFI (BIOS) процессоров Intel поколения Alder Lake: 5,97 ГБ информации — проприетарный исходный код, закрытые ключи шифрования, журналы и инструменты компиляции — были опубликованы в открытом доступе на GitHub. Такой тип данных может быть использован для поиска уязвимостей, в том числе позволяющих внедрить буткит.

- В результате фишинговой атаки на Dropbox было похищено 130 репозиториев, содержащих сведения о текущих и бывших клиентах, а также ключи API разработчиков Dropbox.

- Вымогатели Ragnar Locker опубликовали информацию, похищенную в ходе атаки на полицейское управление муниципалитета Звейндрехт (Бельгия). Утекли данные о штрафах, отчеты о преступлениях и расследованиях, а также данные о сотрудниках управления.

- Группировка NLB выложила в открытый доступ дамп базы данных со сведениями о 400 тыс. бронирований и личными данными 900 тыс. туристов компании Level.Travel. База содержала полные имена, контактные данные, IP-адреса и сведения о паспортах.

Сводная статистика

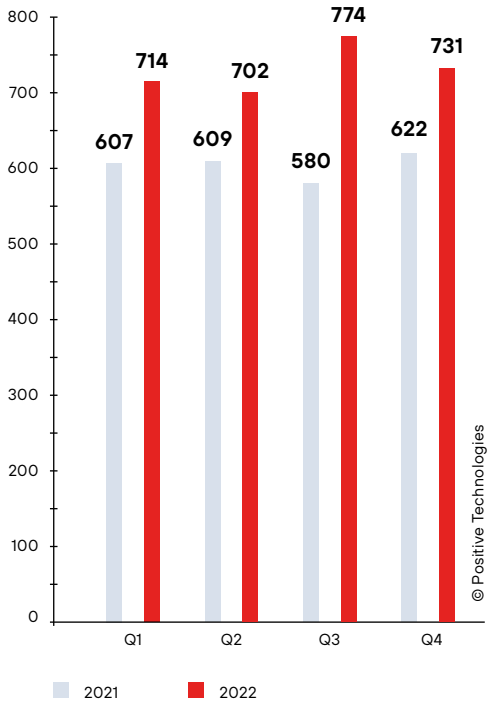

Рисунок 5. Количество инцидентов в 2021 и 2022 годах (по кварталам)

65% атак имели целенаправленный характер

Рисунок 6. Категории жертв среди организаций

19% атак были направлены на частных лиц

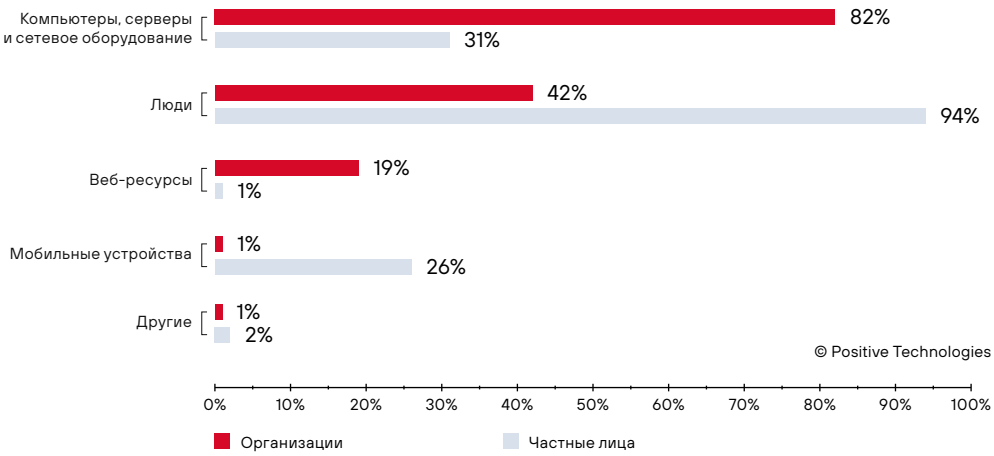

Рисунок 7. Объекты атак (доля атак)

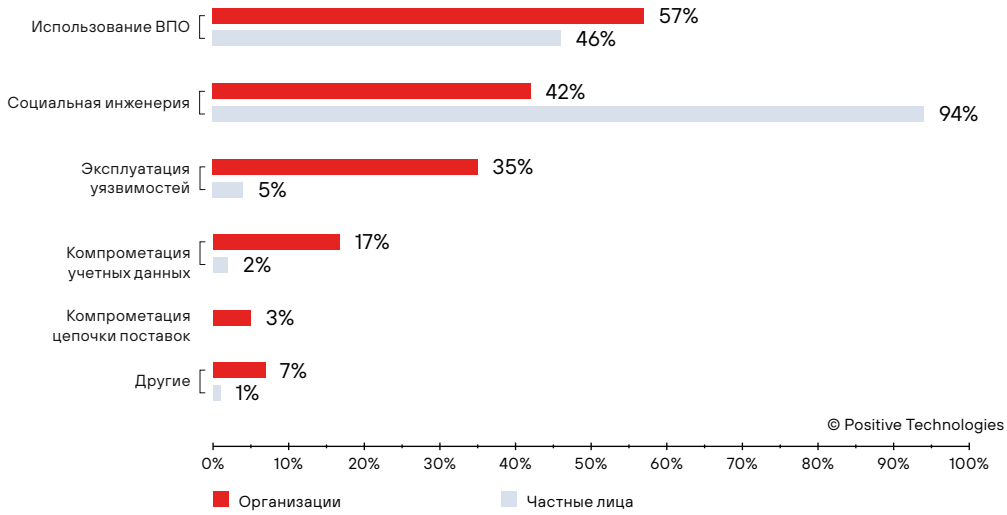

Рисунок 8. Методы атак (доля атак)

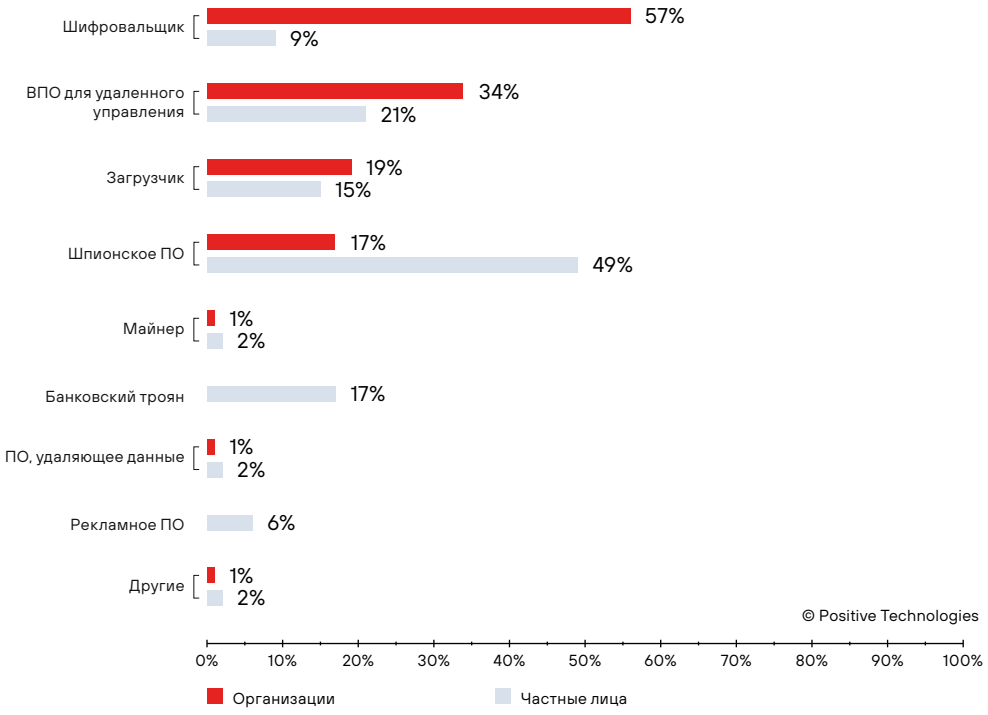

Рисунок 9. Типы вредоносного ПО (доля атак с использованием ВПО)

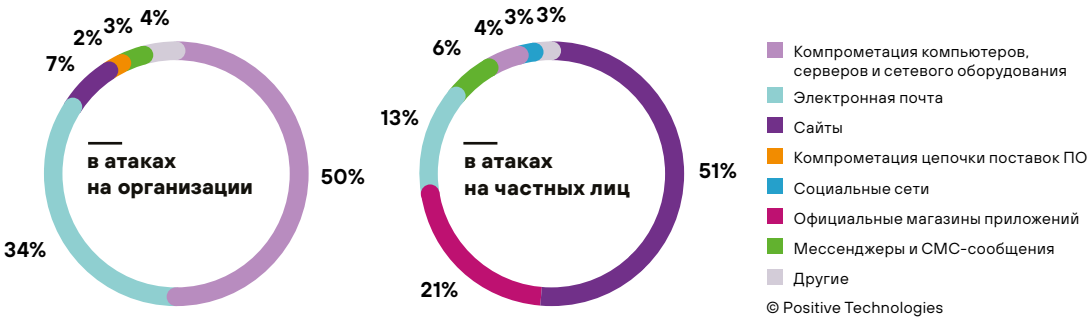

Рисунок 10. Способы распространения вредоносного ПО

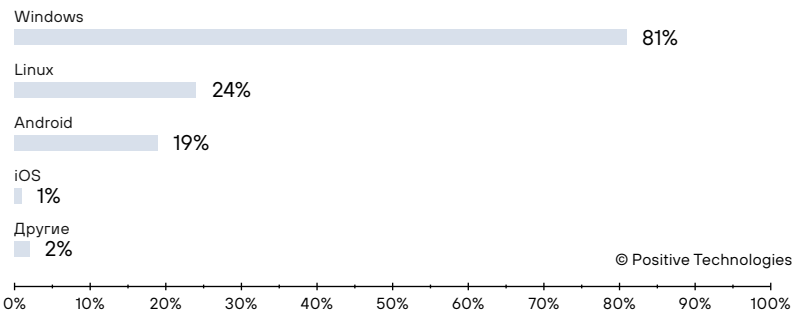

Рисунок 11. Целевые ОС в атаках с использованием ВПО (доля атак)

Категории жертв

	Распределение киберинцидентов по метрикам (объекты атак, методы, последствия) и категориям жертв	Госучреждения	Промышленность	Наука и образование	IT-компании	Медицинские учреждения	Финансовые организации	Торговля	Другие	Без привязки к отрасли	Частные лица
	Всего атак	**82**	**48**	**44**	**45**	**67**	**36**	**26**	**110**	**133**	**140**
Объект	Компьютеры, серверы и сетевое оборудование	57	43	39	36	57	32	19	86	115	43
	Веб-ресурсы	33	5	10	6	2	10	8	24	13	2
	Люди	33	16	28	13	30	19	6	34	70	131
	Мобильные устройства	1							1	2	37
	Другой	1		1	1				1	1	3
Метод	Использование ВПО	39	37	33	28	39	15	12	41	92	64
	Социальная инженерия	33	16	28	13	30	19	6	34	70	131
	Компрометация учетных данных	8	11	11	14	16	5	7	17	9	3
	Эксплуатация уязвимостей	24	21	12	14	17	9	12	39	57	7
	Компрометация цепочки поставок	4	1	1	3	2		1	4	4	1
	Другой	20	1	1			3	1	9	7	3
Последствие	Нарушение основной деятельности	39	21	26	13	19	24	9	40	19	5
	Утечка конфиденциальной информации	24	26	38	27	53	21	18	48	45	94
	Ущерб интересам государства	30	3						7	1	3
	Прямые финансовые потери	2	2	1	2	3	1	2	13	11	33
	Использование ресурсов организаций или частных лиц для проведения атак	1		1	5	1		1	3	16	4
	Другое			1					1	6	6
	Неизвестно	17	8	8	5	5	12	1	17	55	17

© Positive Technologies

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.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для информационной безопасности. Уже 21 год наша основная задача — предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.

Наши технологии и сервисы используют более 2900 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).

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.