4RAYS by SOLAR

ЛАНДШАФТ ВРЕДОНОСНЫХ АТАК: АНАЛИТИКА С СЕНСОРОВ

Q4 + полный 2025 год

Введение и методология

Ежедневно сервисы и продукты «Солара» распознают и блокируют десятки тысяч кибератак на тысячи организаций. Информация об угрозах, с которыми сталкиваются наши клиенты, поступает как от организаций-партнеров, так и из наших собственных источников: расследований инцидентов, аналитики вредоносных инструментов, практики Threat Hunting и сети сенсоров сервиса PDNS, который осуществляет мониторинг коммуникации зараженных инфраструктур российских организаций с серверами управления различных вредоносных программ на территории России. Эта информация используется в работе решения для защиты от кибератак через фильтрацию DNS-трафика Solar DNS RADAR. Дополнительно данные с сенсоров PDNS позволяют оценить распространенность угроз в стране.

DNS-серверы используются при интернет-соединении. Каждый раз, когда пользователь или приложение осуществляет попытку соединения с тем или иным веб-ресурсом (за исключением прямых подключений по IP-адресу), браузер делает обращение к DNS-серверу, которых хранит информацию о том, какое доменное имя какому IP-адресу соответствует.

Информация о попытках соединений (резолвах) анализируется с помощью технологии Passive DNS. Она позволяет сравнить список IP-адресов, с которыми устанавливалось соединение, со списком IP-адресов, о которых известно, что они относятся к вредоносным программам и/или атакам.

Если в списке обнаруживаются резолвы к IP-адресам, которые относятся к угрозам, этот случай считается событием, потенциально указывающим на заражение инфраструктуры клиента телеком-оператора, и учитывается в статистике отчета.

В потоке данных, полученных на основе анализа PDNS, мы выделяем несколько типов угроз по их характерным признакам:

- деятельность известных профессиональных хакерских группировок (APT);
- работа инструментов удаленного администрирования (Remote Access Tools, RAT);
- заражение вредоносами-стилерами (ВПО, похищающее конфиденциальную информацию);
- присутствие ботов одного из известных ботнетов;
- заражение вымогателями;
- заражение ВПО для майнинга криптовалют;
- заражение загрузчиками — ВПО, способным устанавливать на атакованный компьютер дополнительные вредоносы;
- переход на фишинговые страницы.

Признаки заражения выявляются в российских организациях, классифицированных по двум критериям: географическое расположение и принадлежность к той или иной сфере экономики, среди которых мы выделяем семь:

- Государственный сектор
- Здравоохранение
- Образование
- Промышленность
- Топливно-энергетические компании
- Финансовая индустрия
- Телекоммуникационная индустрия
- IT-организации.

Отслеживание изменений в ландшафте угроз на основе данных PDNS позволяет прийти к общему пониманию того, какие угрозы представляют наибольшую опасность.

В отчете мы рассматриваем статистику, собранную с сенсоров в четвертом квартале 2025 года, сравниваем ее с результатами третьего квартала, а также — с результатами четвертого квартала 2024 года. Кроме того, подводим краткие итоги за 2025 год.

Информация в отчете является субъективной оценкой ландшафта киберугроз, сделанной на основе доступной Solar 4RAYS информации с сенсоров и ханипотов.

Основные результаты 4-го квартала 2025 года

- Интенсивность заражений различным вредоносным ПО в 4-м квартале после снижения активности в 3-м квартале выросла на 51%. В среднем каждая компания сталкивается со 157 потенциальными заражениями в месяц.
- Интенсивность подобных атак выросла во всех исследуемых индустриях, кроме образования и IT. Больше всего (более чем на 200%, до 1205 срабатываний) она выросла в ТЭК.
- Общее число организаций, в которых было зарегистрировано хотя бы одно событие потенциального заражения, во 4-м квартале сократилось на 160% — до 5305. На это в том числе повлияло снижение бизнес-активности в 4-м квартале, обусловленное наступлением праздничного периода.
- Стилеры — вновь главная угроза. В 4-м квартале их доля выросла на 11 п. п., до 41,7% — и это после снижения числа заражений, которое длилось с лета по конец 3-го квартала. На втором и третьем месте — инструменты APT-группировок и средства удаленного доступа.
- Госсектор, IT, ТЭК, телеком и образование стали отраслями, в которых увеличилась доля событий, связанных с заражением посредством почти всех отслеживаемых типов угроз.

Основные результаты 2025 года

- Всего за год мы зафиксировали **9 326 764** срабатывания в сетях **38 493** организаций. В среднем каждую организацию атаковали **242** раза.

- Стилеры стали самой часто встречающейся угрозой в 2025 году — на них пришлось 36% срабатываний. Индикаторы APT-группировк (27%) — на втором месте. Средства удаленного доступа (19%) — на третьем.

- Индустриями, в которых мы зафиксировали больше всего срабатываний, стали промышленность (29%), здравоохранение (20%) и ТЭК (15%).

Общая статистика

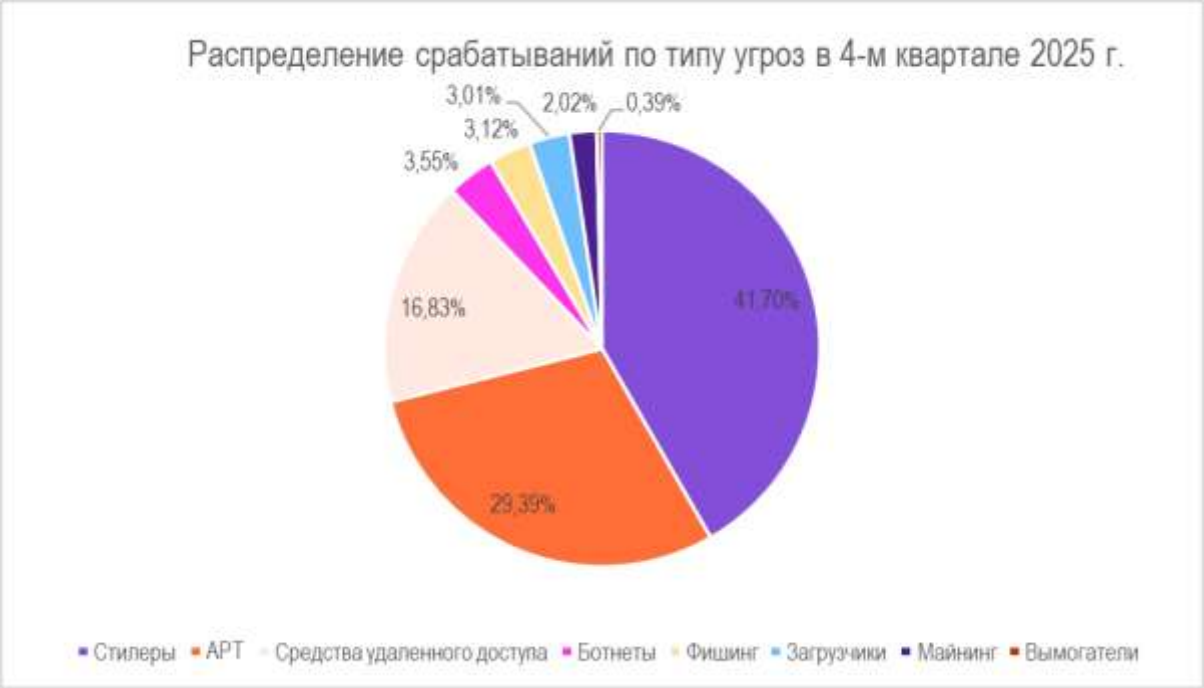
Показатель	3-й кв. 2025	4-й кв. 2025	Изменение	4-й кв. 2024	Изменение квартал к кварталу 2024/2025
Общее число срабатываний	1442976	836709	–72,46%	1210245	–44,64%
Число организаций	13823	5305	–160,57%	29726	–460,34%
Среднее количество атак на организацию	104,3	157,72	+51,22%	40,71	+287,42%

- Общее число срабатываний продолжило снижаться. Если в 3-м квартале оно вернулось на уровень 4-го квартала 2024 года, то в 4-м квартале 2025-го снизилось на 44,6% год к году.
- Количество атакованных организаций также значительно снизилось.
- После снижения в 3-м квартале интенсивность атак (среднее число заражений на одну организацию) увеличилась более чем на 50%. А по сравнению с 4-м кварталом 2024 года этот показатель возрос почти в четыре раза.

Комментарий экспертов Solar 4RAYS:
На общие цифры четвертого квартала оказали влияние сразу два значительных фактора. Во-первых, сезонность. Начиная со второй половины декабря падает как бизнес-активность, так и активность злоумышленников, что отчетливо видно на цифрах. И количество срабатываний, и количество организаций, в сетях которых эти срабатывания произошли, уменьшается. Кстати, похожую картину мы видели и в четвертом квартале 2024 года — тогда падение общего числа срабатываний по сравнению с 3-м кварталом составило 35,2%, а количество организаций снизилось на 15,8%.

Во-вторых, в 4-м квартале мы внесли ряд технических изменений в работу наших PDNS-сенсоров, и поэтому число организаций, от которых мы получаем данные, сократилось. Это повлияло на один из отслеживаемых нами параметров, но репрезентативность данных сохранилась. Рост среднего количества срабатываний означает, что одна организация сталкивается с бОльшим количеством киберугроз, чем раньше, и это свидетельствует о необходимости внедрения комплексных средств защиты. .

Типы угроз и индустрии



- Среди типов угроз наибольшую распространенность в 4-м квартале 2025 года имели стилеры, индикаторы APT-группировок и средства удаленного доступа. Стилеры после снижения во 2-м и 3-м кварталах снова вышли на первое место. А вот RAT «потеряли» 7 процентных пунктов. В сравнении с 4-м кварталом 2024 года доля стилеров удвоилась.

Комментарий экспертов Solar 4RAYS:
Для нового увеличения доли стилеров в общем количестве срабатываний может быть несколько причин. 4-й квартал — традиционно «высокий» сезон для активности финансовых кибератак. Праздничные распродажи, проходящие с ноября по декабрь, сопровождаются, как правило, покупательским ажиотажем — люди заказывают товары в интернете, а этот процесс связан с передачей финансовых сведений. Ежегодно киберпреступники стараются использовать этот период для кражи важной платежной информации — как раз с помощью вредоносного ПО типа стилеров.

Другим объяснением роста может быть «естественная цикличность» ландшафта киберугроз, которая в том числе характеризуется волнообразным распространением того или иного типа вредоносов: период роста числа атак с помощью стилеров сопровождается появлением множества разновидностей подобных программ. ИБ-индустрия реагирует на это усиленным противодействием: быстрым детектированием модификаций вредоносов, блокировкой поддерживающей инфраструктуры и так далее. Противодействие приводит к спаду: атаки становятся менее эффективными, и злоумышленники «берут паузу» на создание новых модификаций ВПО и инфраструктуры под него. В этом случае атак становится меньше на определенный период.

Кроме роста доли атак с помощью стилеров, 4-й квартал характеризует небольшое снижение случаев обнаружения инструментария APT-группировок — 29% срабатываний против 32% в третьем квартале. Это снижение незначительно, профессиональные группировки продолжают активно атаковать. Это происходит в связи с напряженной геополитической обстановкой: российские организации представляют объект повышенного интереса для группировок, работающих в интересах иностранных государств.

Тип угрозы	3-й кв. 2025 г.	4-й кв. 2025 г.	Изменение
Средства удаленного доступа (RAT)	24%	16,83%	–7,17 п. п.
APT	32%	29,39%	–2,61 п. п.
Ботнеты	5%	3,55%	–1,45 п. п.
Стилеры	30%	41,7%	+11,7 п. п.
Майнинг	5%	2,02%	–2,98 п. п.
Загрузчики	2%	3,01%	+1,01 п. п.
Фишинг	1%	3,12%	+2,12 п. п.
Вымогатели	1%	0,39%	–0,61 п. п.

Атакованные сферы экономики

- Доля срабатываний в организациях из сферы здравоохранения в 4-м квартале в сравнении с 3-м выросла сразу на 7 п. п., зато атаки на промышленность потеряли 6 п. п. При этом, если сравнивать год к году, значительных изменений в обеих сферах не наблюдается.
- Обозначившийся в прошлом квартале тренд на увеличение интереса атакующих к предприятиям сферы ТЭК в 4-м квартале продолжился: доля атак на такие предприятия выросла сразу на 16 п. п в сравнении с 3-м кварталом и более чем в три раза год к году.

- По сравнению с 4-м кварталом 2024 года доля атак на образовательные учреждения снизилась в три раза, на 10 п. п., а на госсектор — на 4 п. п., до 12%.

Комментарий экспертов Solar 4RAYS:
Фиксируем продолжающееся давление со стороны злоумышленников на сферу ТЭК. Предприятия этого сектора входят в перечень критически важных для экономики страны и продолжают представлять интерес как для прогосударственных атакующих, так и для киберпреступников, намеревающихся заработать на вымогательстве. Рост атак на здравоохранение в четвертом квартале в сравнении с третьим обусловлен неугасающим интересом атакующих к медицинским данным, которые имеют высокую ценность на черном рынке, а кроме того — незрелостью ИТ-инфраструктуры сферы здравоохранения: из-за стремительной цифровизации адекватные меры безопасности в медицинских учреждениях иногда принимаются со значительной задержкой, из-за чего такие цели могут казаться злоумышленникам «легкими». Обратным (и положительным) примером выглядит ситуация в отрасли образования, где доля зафиксированных срабатываний снизилась с 15% в 4-м квартале 2024 года до 5% в 4-м квартале 2025-го. Это может быть следствием адекватного реагирования IT-команд образовательных учреждений на угрозы. При этом интенсивность (то есть частота срабатываний в среднем на одну организацию) за год возросла на 44% до 23 срабатываний на организацию. Это значительно ниже, чем в организациях из почти любой другой сферы (кроме телекома), но увеличение частоты может свидетельствовать как о повышении детектирующих способностей защитных систем организации, так и о зарождающемся тренде на рост внимания атакующих к образовательным учреждениям.

В целом, как видно из графика ниже, интенсивность атак практически во всех индустриях значительно выросла (иногда более чем на тысячу процентов) в сравнении с 4-м кварталом 2024 года. Это наглядно характеризует заметные изменения ландшафта: российские организации гораздо чаще стали фиксировать атаки.

Среднее количество событий	3-й кв. 2025 г.	4-й кв. 2025 г.	Изменение	4-й кв. 2024 г.	Изменение квартал к кварталу 2024/2025
Индустрия					
Здравоохранение	151	235	+55,63%	80	+194%

Государственный сектор	76	111	+46,05%	27	+311%
Промышленность	115	170	+47,83%	76	+123%
Образование	33	23	–30,03%	16	+44%
ТЭК	398	1205	+202,76%	59	+1942%
Телеком	66	23	–68,25%	81	–71%
Финансы	67	74	+10,45%	19	+289%
IT	308	83	–73,05%	43	+93%

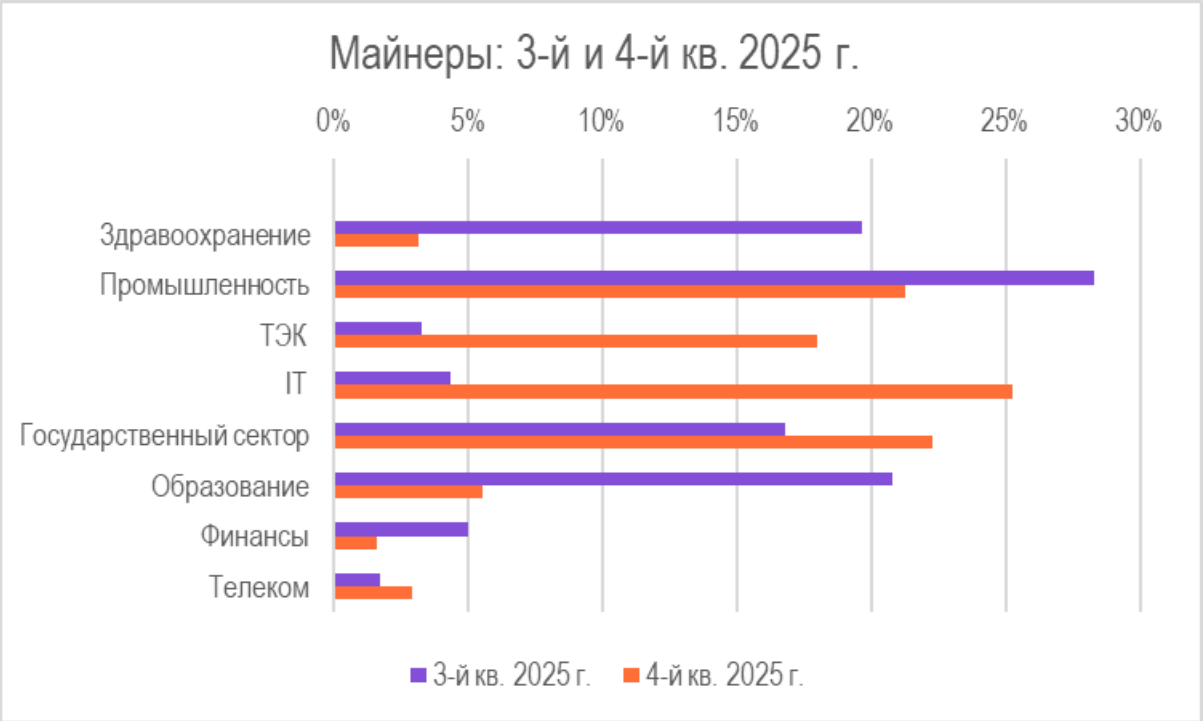
Типы угроз: детали

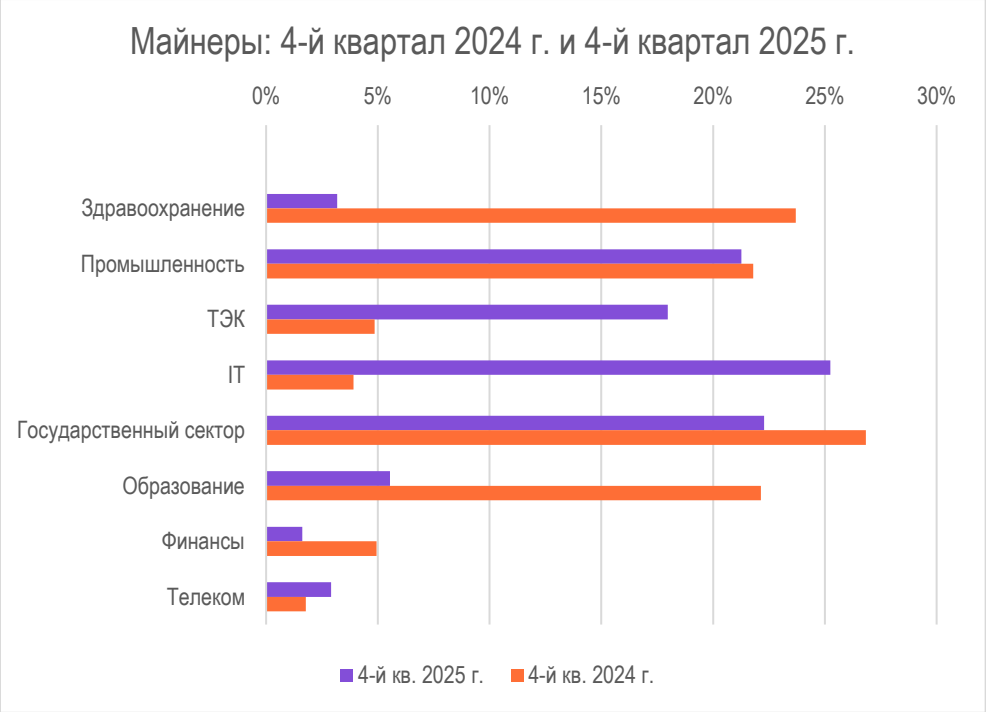
Далее приведем графики, демонстрирующие то, какие киберугрозы представляли наибольшую опасность для каждой индустрии в отдельности, посмотрим, как активность угроз разных типов заражений в 4-м квартале 2025 года изменилась в сравнении с 4-м кварталом 2024 г. и 3-м кварталом 2025-го.

Майнеры

Индустрии, для которых майнеры представляли наибольшую опасность в 4-м квартале:

- IT
- ТЭК
- Телеком.

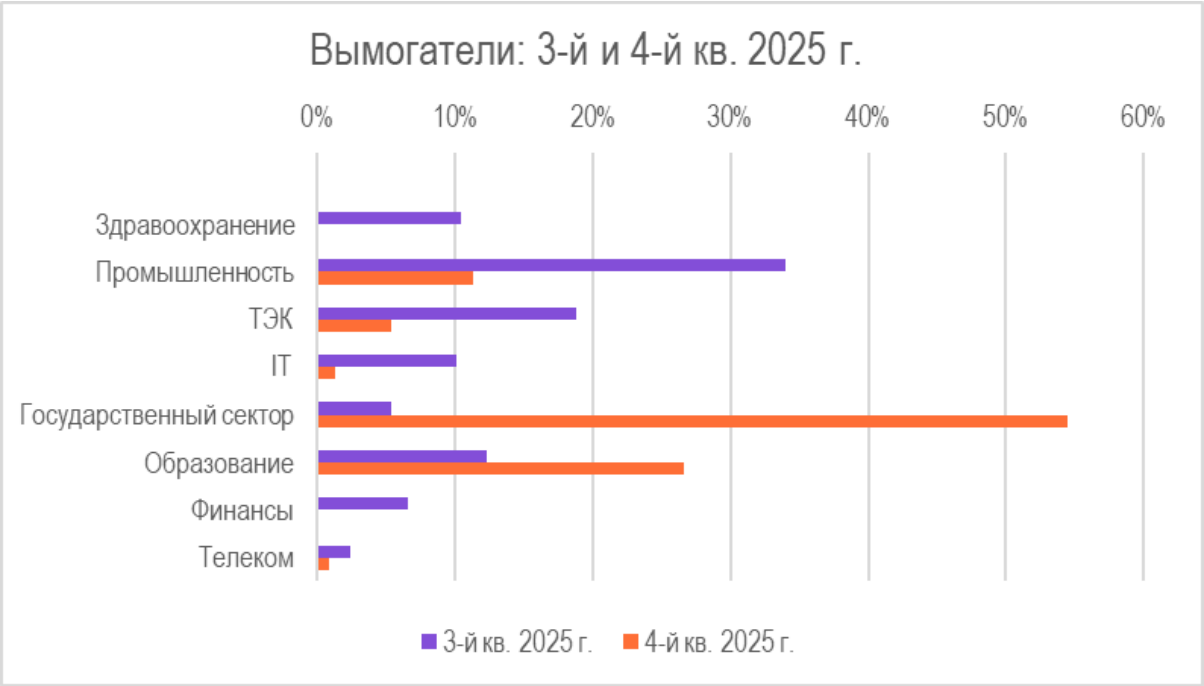


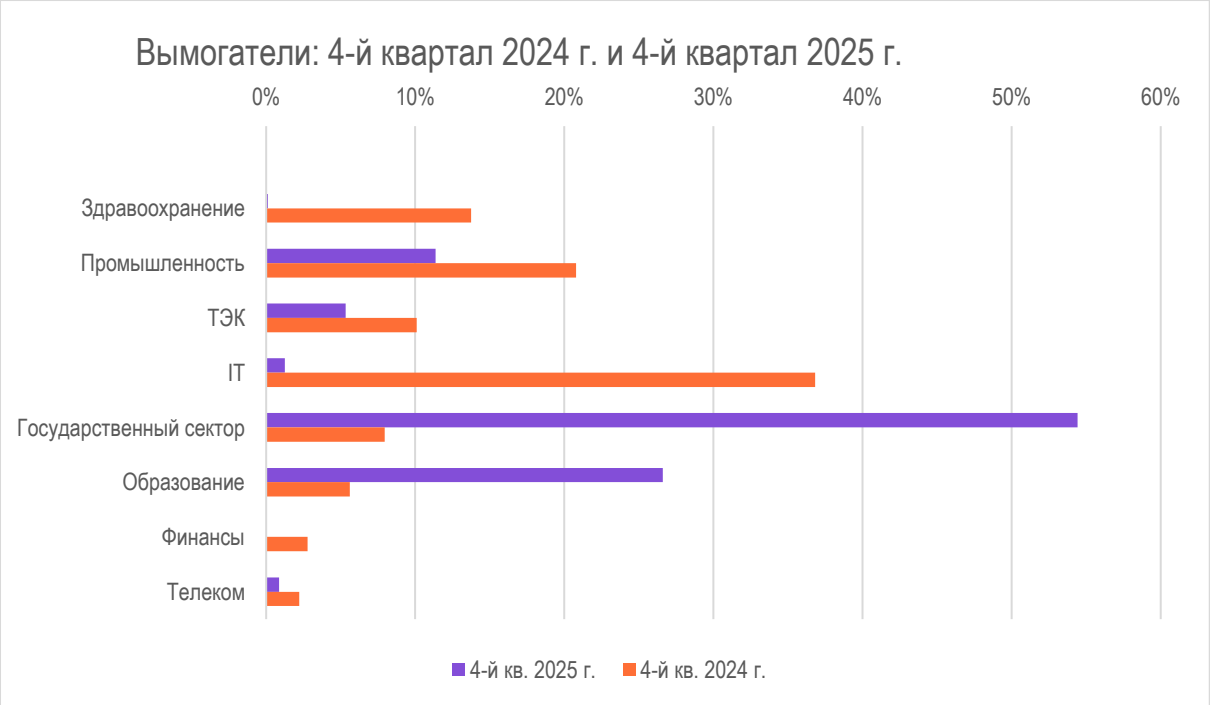

Майнеры: 4-й квартал 2024 г. и 4-й квартал 2025 г.
0%
5%
10%
15%
20%
25%
30%
Здравоохранение
Промышленность
ТЭК
IT
Государственный сектор
Образование
Финансы
Телеком
4-й кв. 2025 г.
4-й кв. 2024 г.

Вымогатели

Индустрии, для которых вымогатели представляли наибольшую опасность в 4-м квартале:

- Государственный сектор
- Образование.

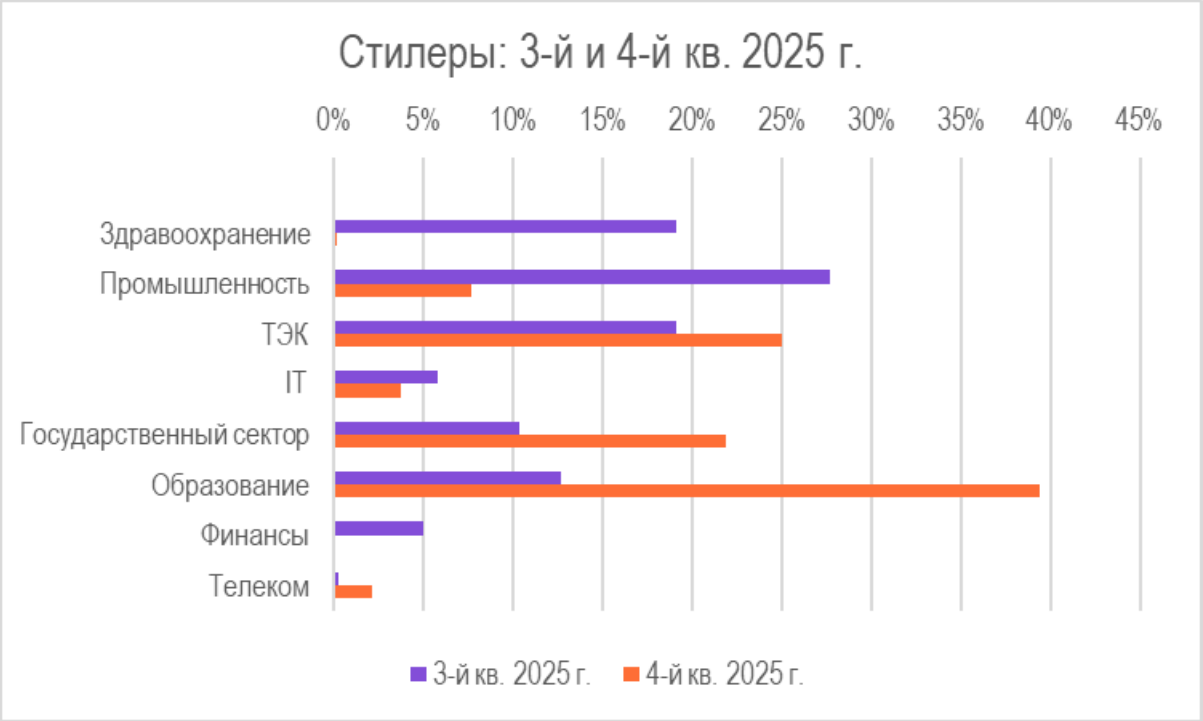


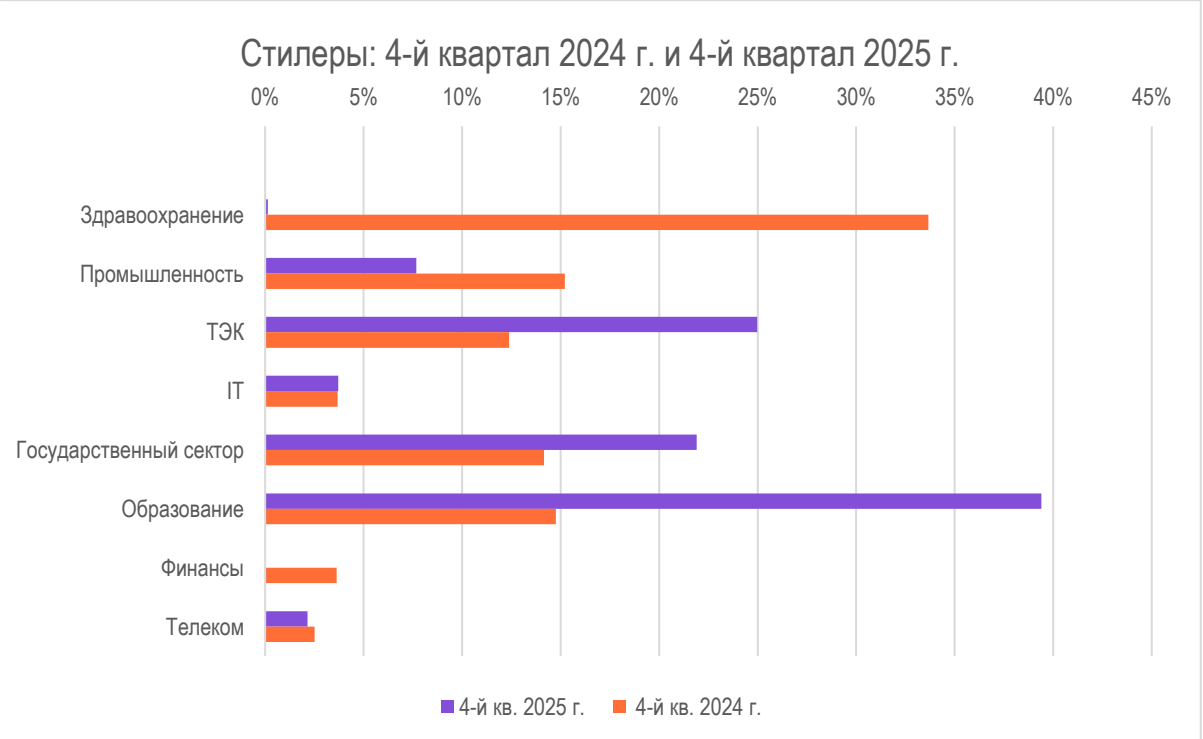


Стилеры

Индустрии, для которых стилеры представляли наибольшую опасность в 4-м квартале:

- Образование
- Государственный сектор
- ТЭК
- Телеком.

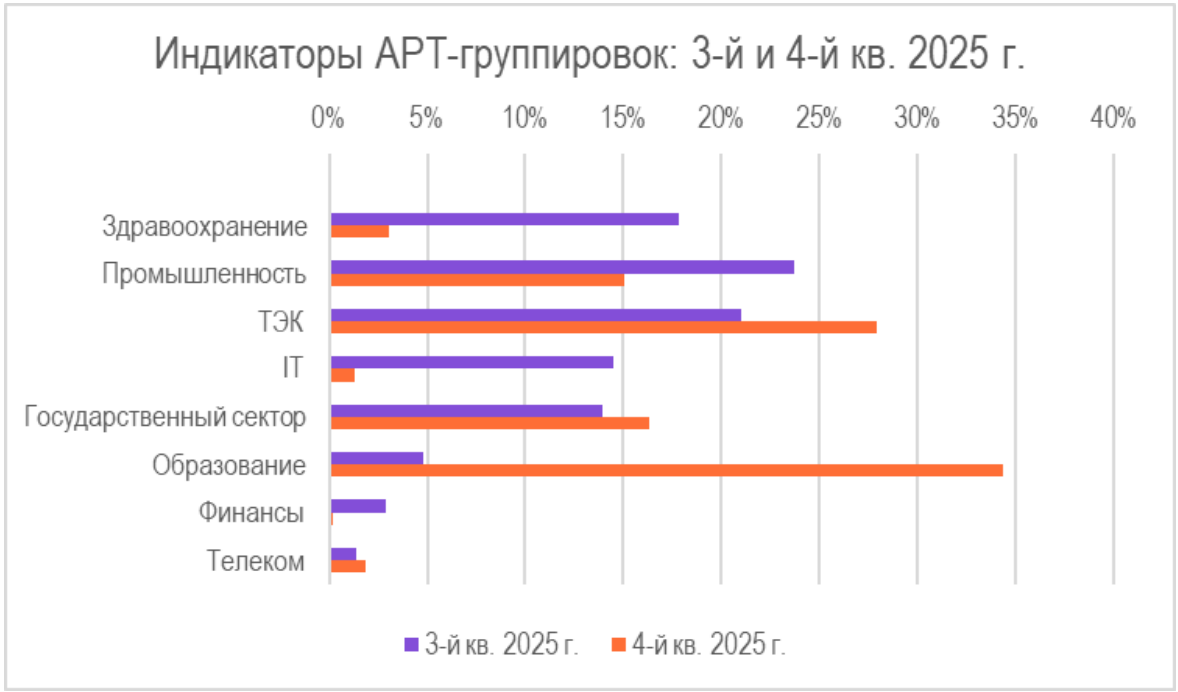


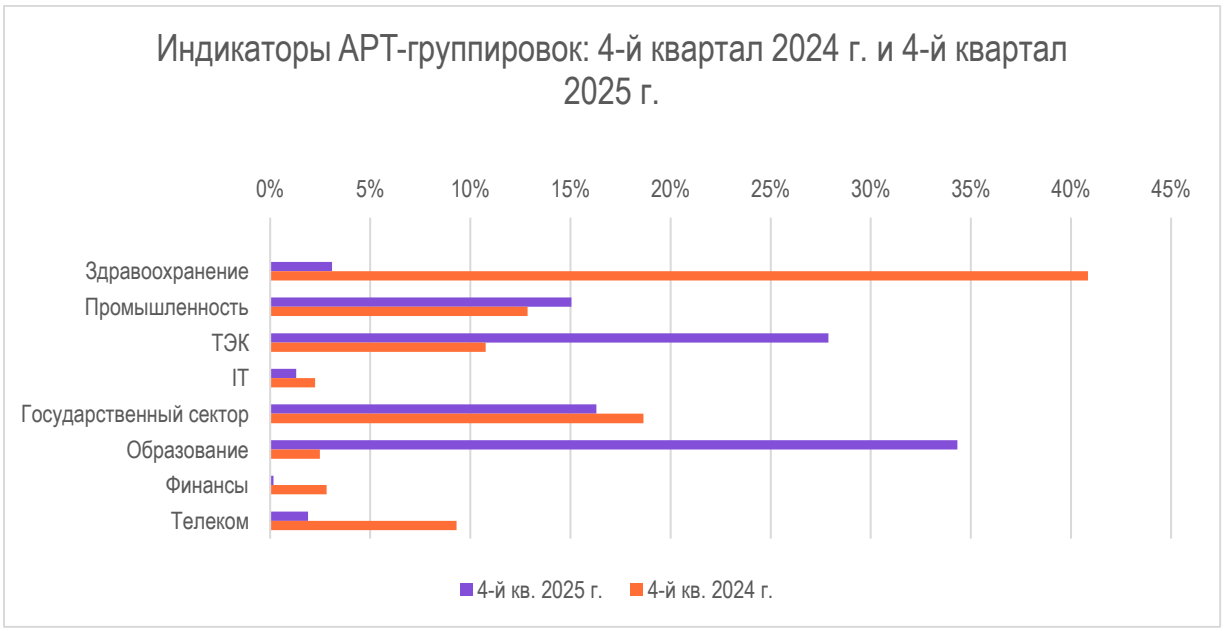


Индикаторы APT-группировок

Индустрии, для которых APT-группировки представляли наибольшую опасность в 4-м квартале:

- Образование
- ТЭК
- Государственный сектор
- Телеком.

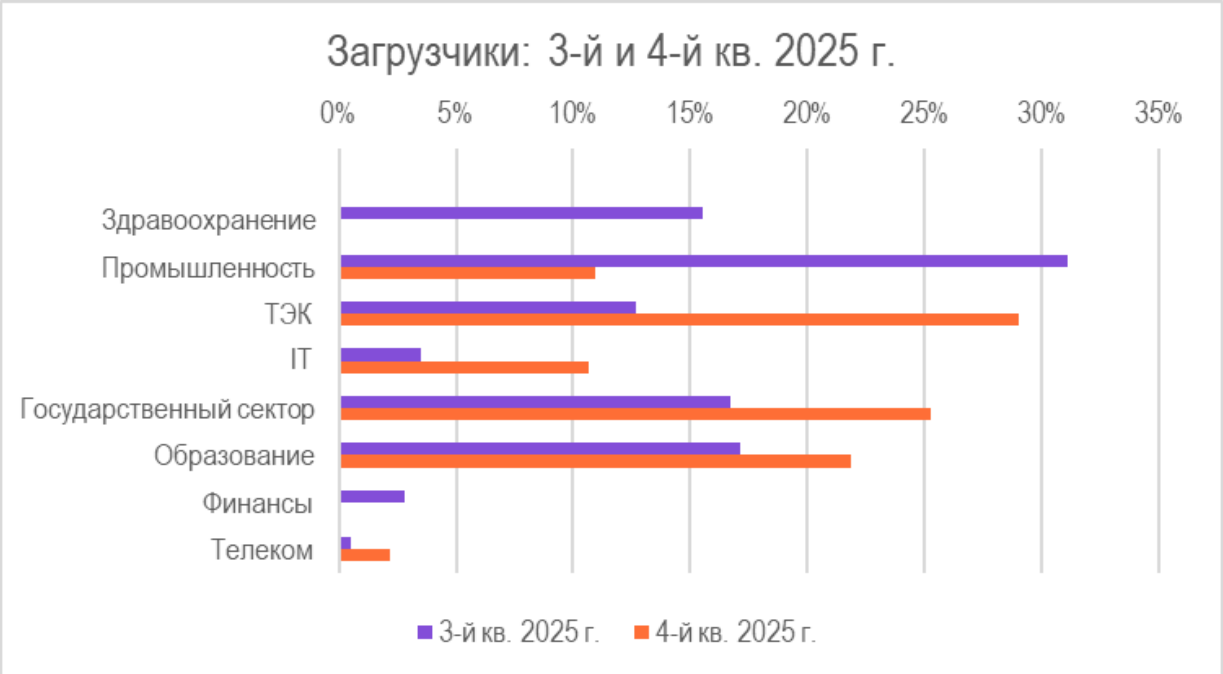


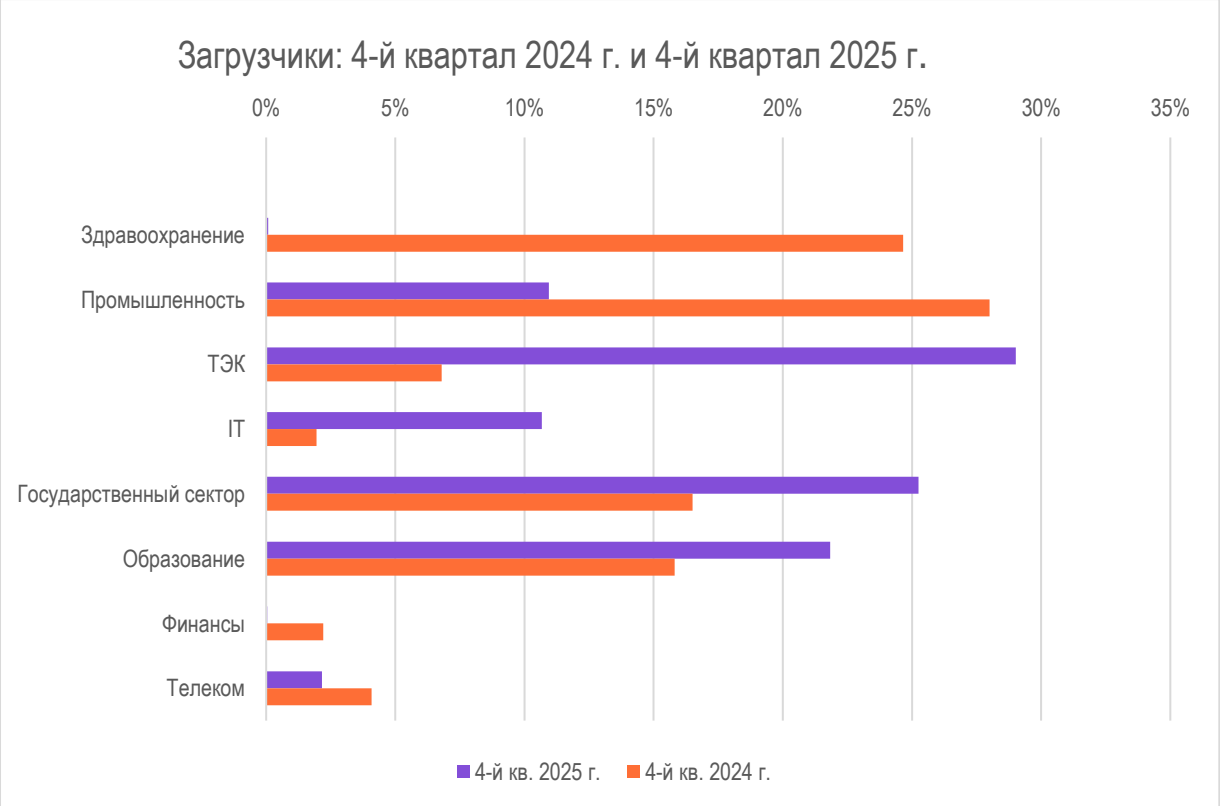


Загрузчики

Индустрии, для которых загрузчики представляли наибольшую опасность в 4-м квартале:

- ТЭК
- IT
- Образование
- Телеком.

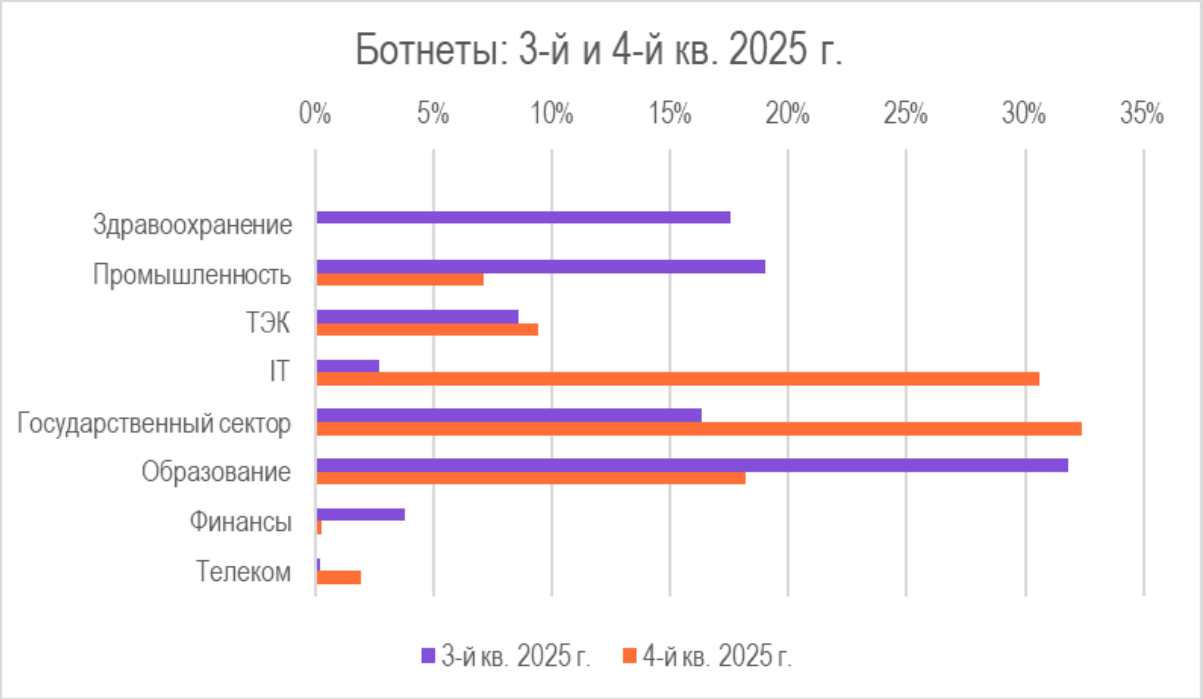


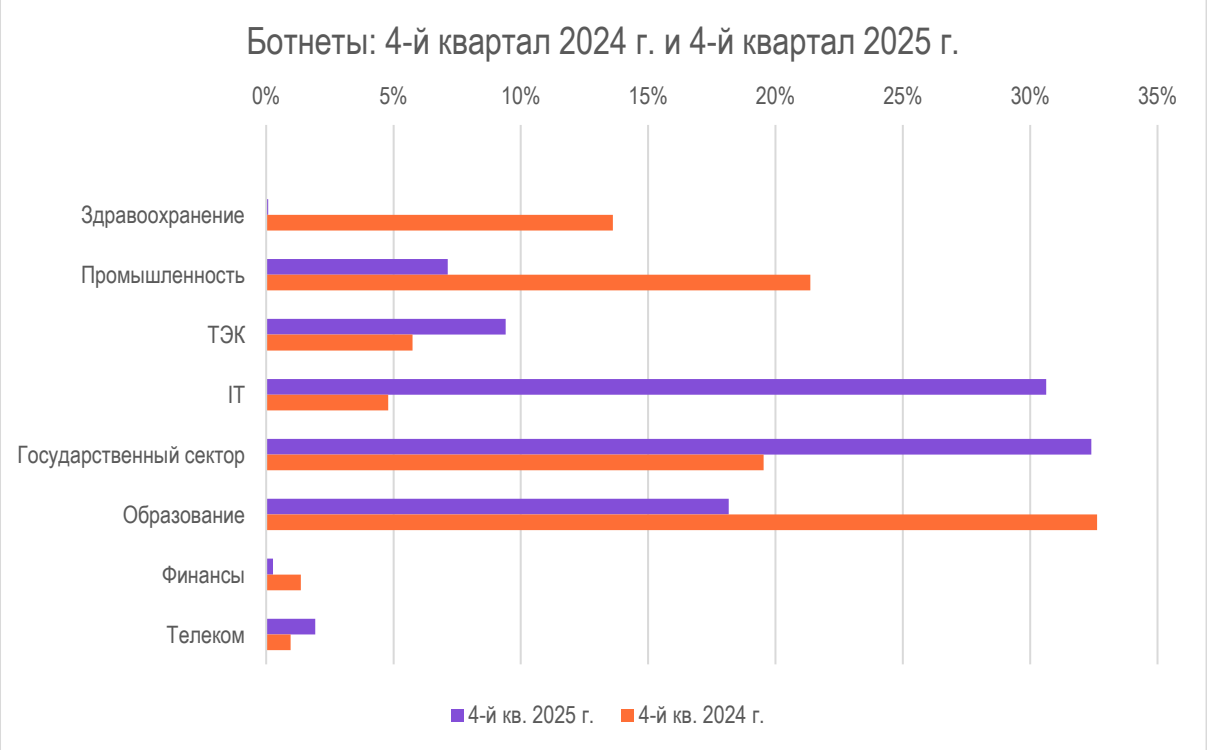


Ботнеты

Индустрии, для которых ботнеты представляли наибольшую опасность в 4-м квартале:

- IT
- Государственный сектор
- Телеком
- ТЭК.

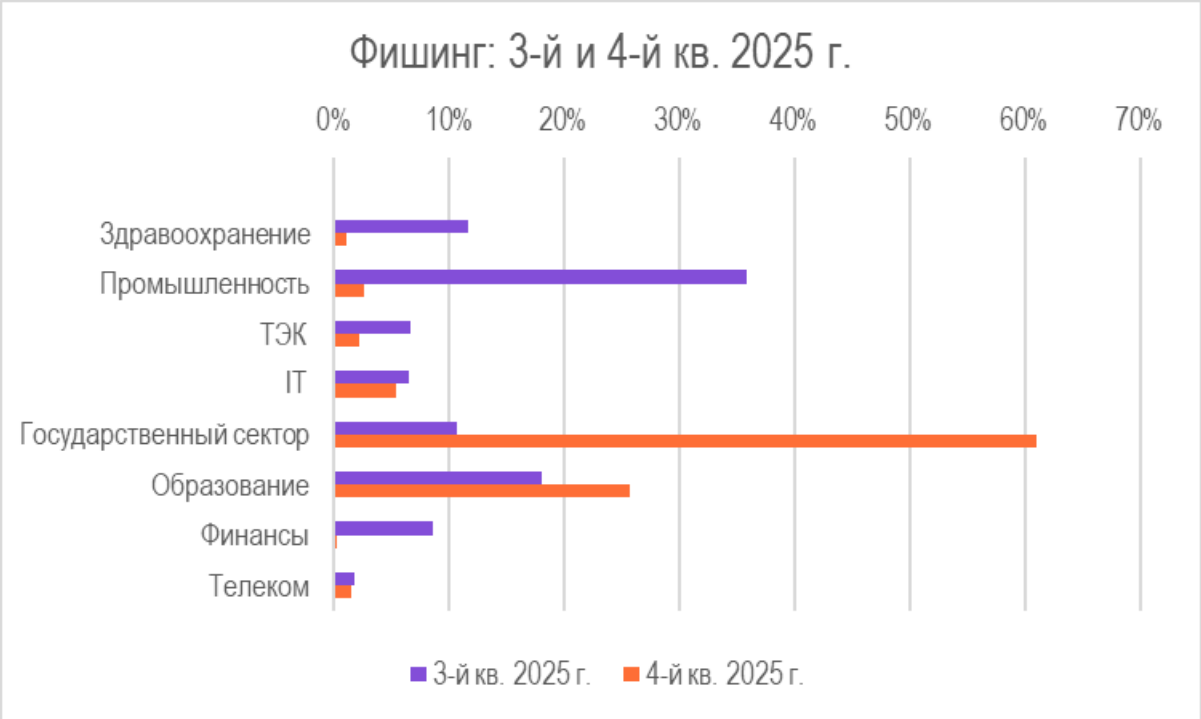


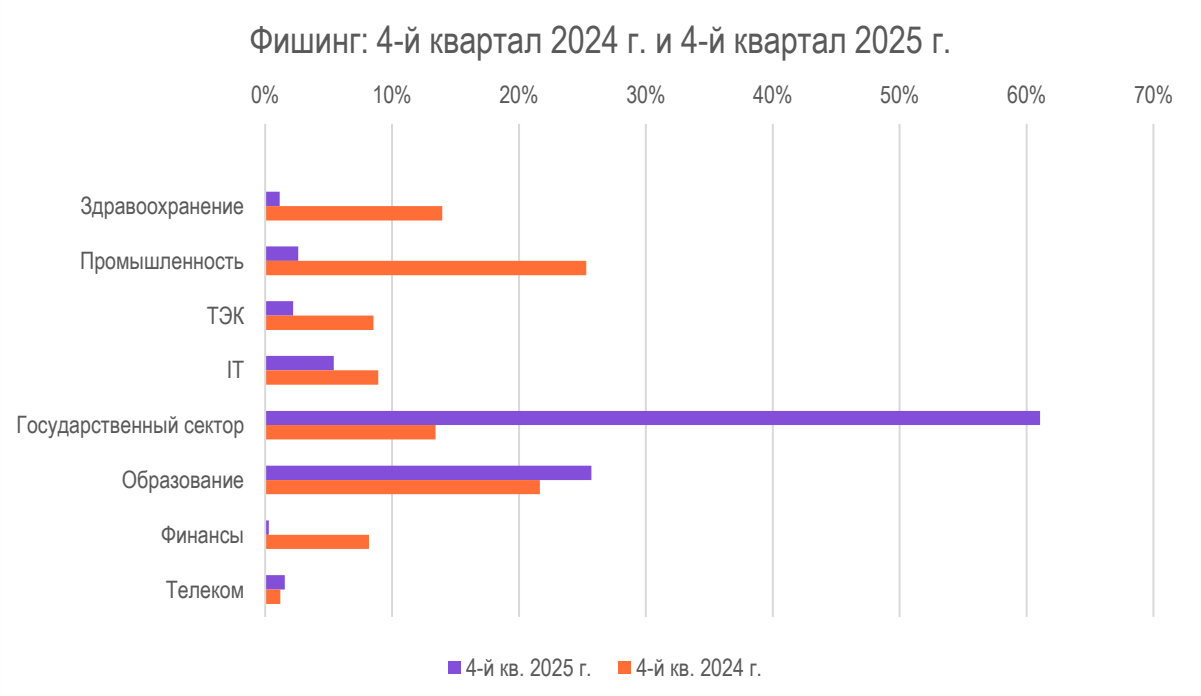


Фишинг

Индустрии, для которых фишинг представлял наибольшую опасность в 4-м квартале:

- Государственный сектор
- Образование.

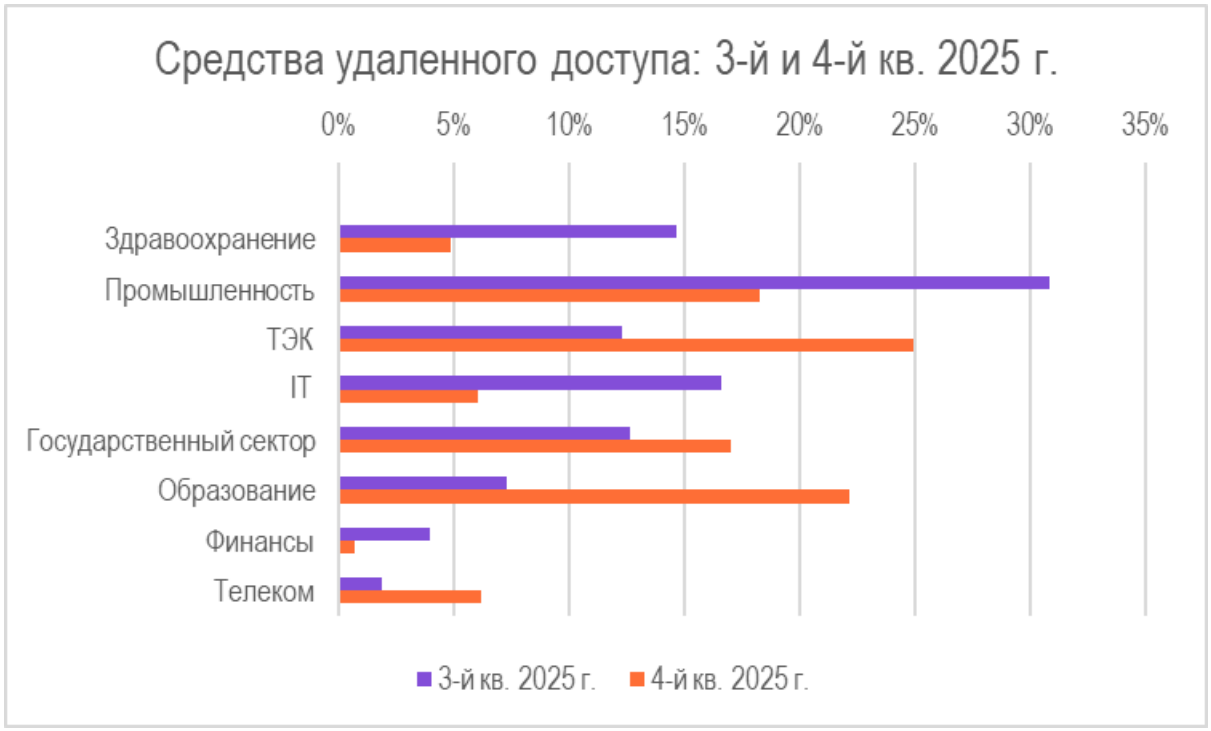


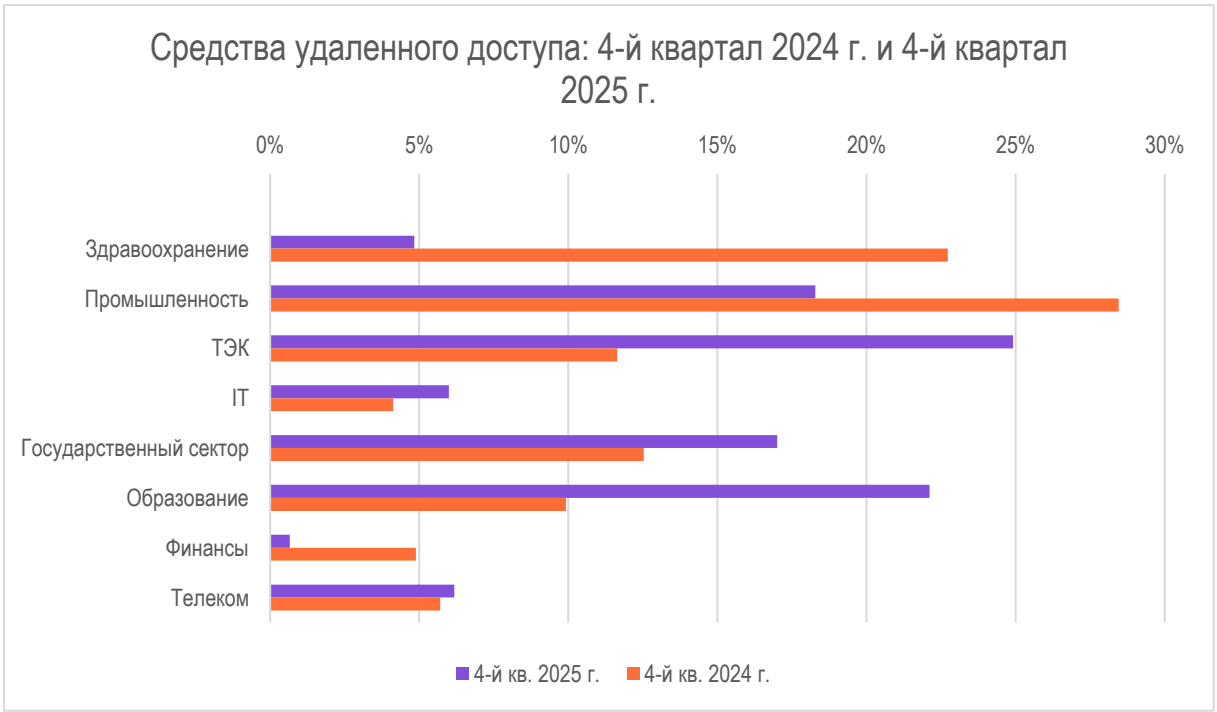


Средства удаленного доступа (RAT)

Индустрии, для которых средства удаленного доступа представляли наибольшую опасность в 4-м квартале:

- Образование
- Телеком
- ТЭК
- Государственный сектор.



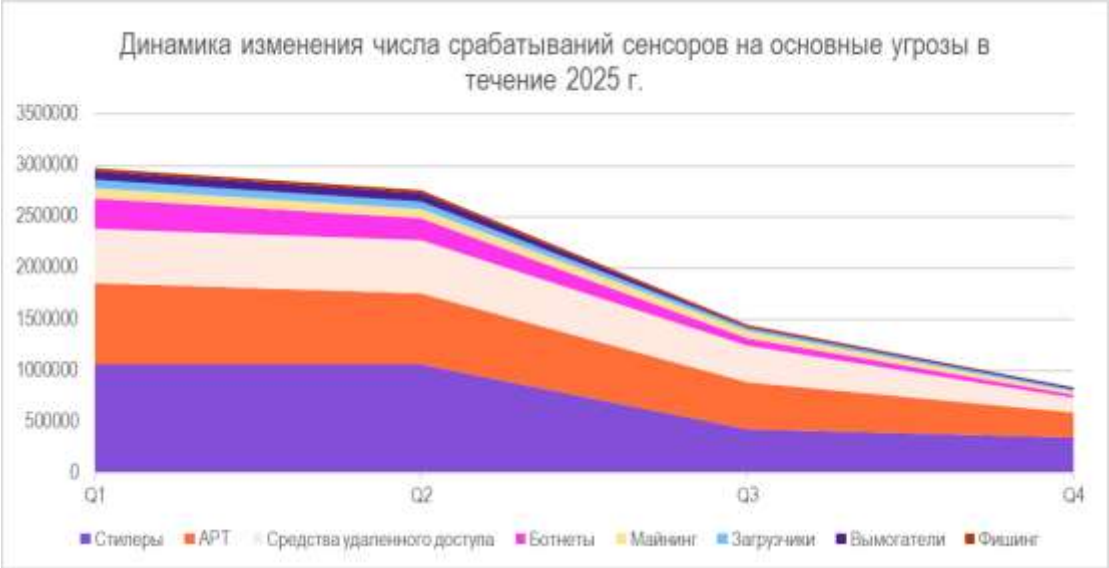


Комментарий экспертов Solar 4RAYS:
Как видно из графиков выше и комментариев к ним, топ индустрий, подвергшихся атакам в 2024–2025 гг., хотя и менялся от угрозы к угрозе, их состав оставался одним и тем же. Госсектор, IT, ТЭК, телеком и образование были в прицеле атакующих в четвертом квартале. Прогнозируем, что в первом квартале наступившего года эта тенденция сохранится, и представителям этих отраслей следует обращать пристальное внимание на защиту.

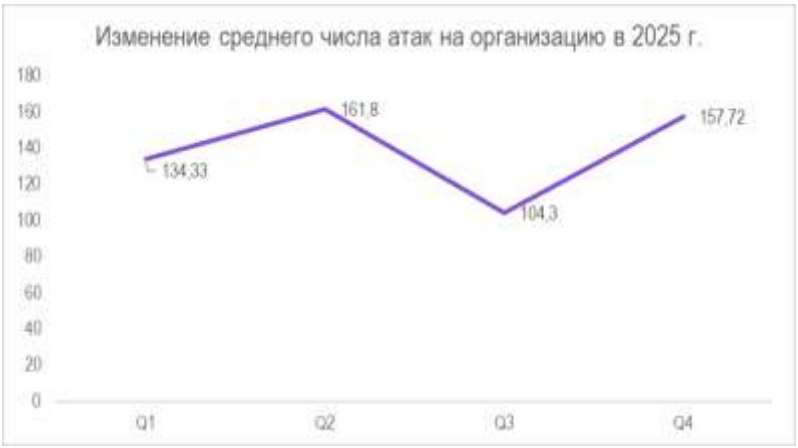
Итоги 2025 года

Весь 2025 год мы ежеквартально отслеживали изменениям в ландшафте массовых киберугроз, и теперь настало время подвести итоги.

Всего за год мы зафиксировали **9 326 764** срабатывания в сетях **38 493** организаций. В течение года наблюдался тренд на снижение общего количества атак, и особенно он стал заметен ко второй половине года. Однако мы предполагаем, что это может быть временным явлением.



В среднем на одну организацию по итогам года пришлось **242** срабатывания. От квартала к кварталу показатель интенсивности менялся волнообразно, а закончился год явным трендом на увеличение интенсивности атак.



Стилеры стали самой часто встречающейся угрозой в 2025 году — на них пришлось 36% срабатываний. Индикаторы APT-группировк (27%) — на втором месте, средства удаленного доступа (19%) — на третьем.

Индустриями, в которых мы зафиксировали больше всего срабатываний, стали промышленность (29%), здравоохранение (20%) и ТЭК (15%).

Комментарий экспертов Solar 4RAYS:
Более 80% угроз, которые мы зафиксировали в сетях российских организаций, — это вредоносные инструменты, направленные на шпионаж и похищение конфиденциальных сведений. С нашей точки зрения, это более чем красноречивая характеристика основного мотива злоумышленников в 2025 году — они охотятся за конфиденциальными сведениями. Интеллектуальная собственность, персональная информация, сведения о состоянии бизнеса или учетные данные для авторизации во внутренних системах — все это либо представляет ценность само по себе (то есть может быть продано на черном рынке в качестве ценных

разведданных), либо открывает возможности для проведения серьезных целевых атак с целью шпионажа, финансовой наживы или деструктивной деятельности.

Фокус на организации, входящие в топ атакованных, вполне соотносится с ключевым мотивом злоумышленников: и промышленность, и в здравоохранение, и организации топливно-энергетического комплекса ежедневно оперируют ценной конфиденциальной информацией, и именно она должна быть основным активом, защите которого стоит уделять внимание российским ИБ-командам.

Заключение и рекомендации

Картина заражений в индустриях, полученная с помощью PDNS, позволяет сделать несколько выводов. Похищение конфиденциальной информации остается основной целью злоумышленников, а интенсивность атак, даже несмотря на снижение их общего количества, растет.

В фокусе атакующих — индустрии, оперирующие большим количеством конфиденциальных сведений. Как мы и предполагали, ТЭК, промышленность и госсектор продолжают быть наиболее подверженными угрозам прежде всего шпионских атак.

Для надежной защиты инфраструктуры организации от кибератак эксперты Solar 4RAYS рекомендуют следующие меры:

- Регулярно сканировать внешний периметр на предмет изменения опубликованных сервисов и наличия в них уязвимостей (Vulnerability Management).
- Публиковать в интернет только действительно необходимые сервисы и осуществлять за ними повышенный контроль. Все интерфейсы управления инфраструктурой и ИБ не должны быть доступны из публичной сети.
- Использовать продвинутые средства защиты (EDR, SIEM) наряду с классическим защитным ПО, чтобы иметь возможность отслеживать события в инфраструктуре и вовремя обнаруживать нежелательные. А кроме того, использовать решения, способные распознавать атаки в DNS-трафике, например Solar DNS RADAR.
- Оперативно обновлять все используемое в инфраструктуре ПО.
- Строго контролировать удаленный доступ в инфраструктуру, особенно для подрядчиков (PAM).
- Предельно ответственно относиться к соблюдению парольных политик, пользоваться сервисами мониторинга утечек учетных записей и вовремя их обновлять. Обеспечивать защиту от автоматизированных атак методом подбора.
- Создавать инфраструктуру бэкапов, следуя принципу «3-2-1», который предполагает наличие не менее трех копий данных, хранение копии как минимум на двух физических носителях разного типа и наличие минимум одной копии за пределами основной инфраструктуры.
- В случае подозрения на атаку не медлить с оценкой компрометации, а лучше — делать ее на регулярной основе.
- Заниматься повышением киберграмотности сотрудников — ведь успешная атака на основе социальной инженерии возможна даже в самой защищенной инфраструктуре.
- Следить за тем, чтобы служба ИБ имела постоянный доступ к последним сведениям о ландшафте киберугроз конкретного региона и индикаторам компрометации (например, через сервисы Threat Intelligence).