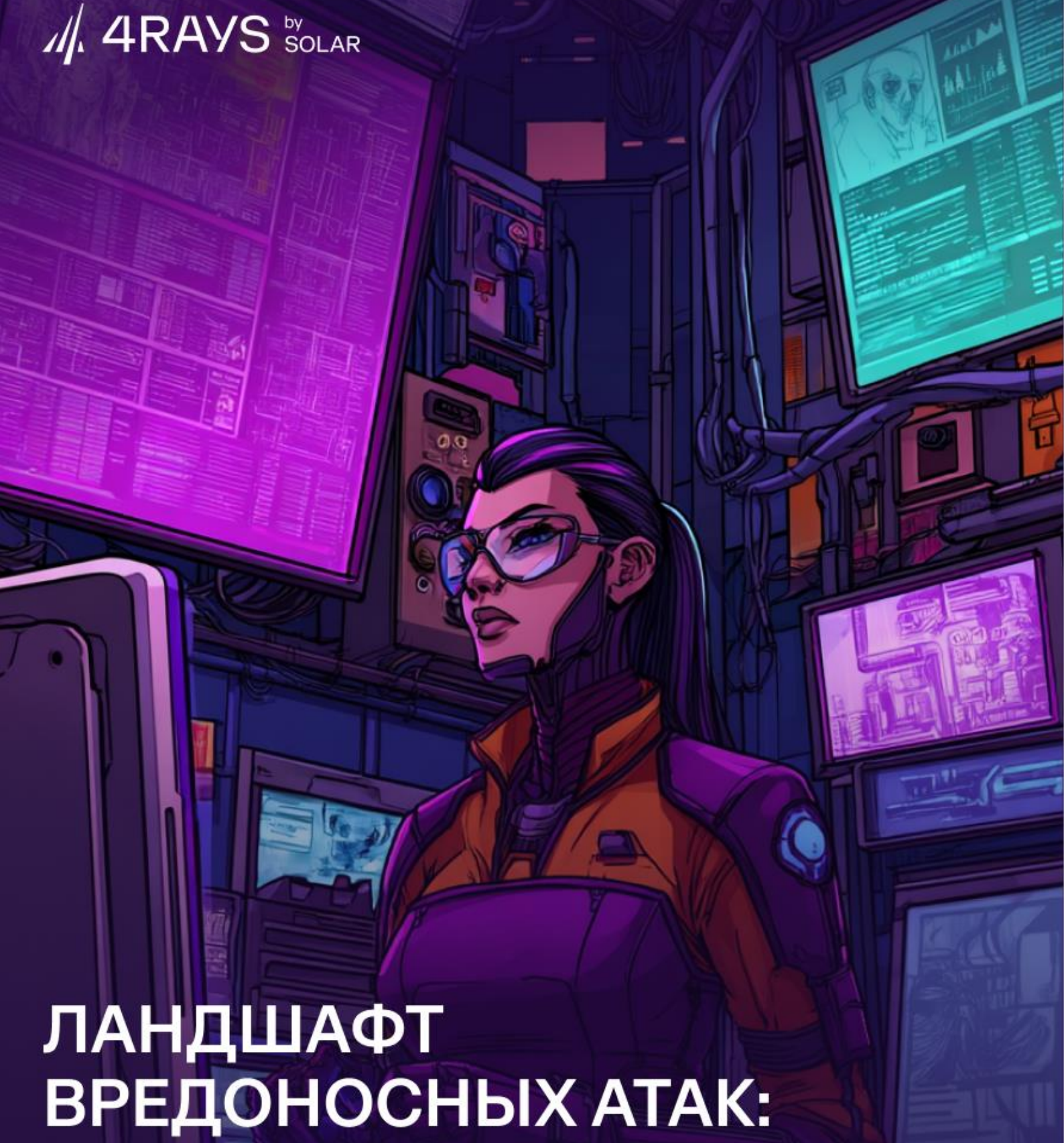
4RAYS by SOLAR



ЛАНДШАФТ ВРЕДОНОСНЫХ АТАК: АНАЛИТИКА С СЕНСОРОВ И ХАНИПОТОВ

Отчет по итогам первого квартала 2025 года

Введение

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, анализа вредоносных инструментов, практики Threat Hunting и сети сенсоров, служащих «приманкой» для злоумышленников.

Центр исследования киберугроз Solar 4RAYS поддерживает глобальную сеть из более чем сотни ханипотов по всему миру. Они круглосуточно действуют в том числе в России, Польше, Франции, Германии, Швейцарии, США, Канаде, Японии и Сингапуре и предоставляют экспертам центра информацию о том, как часто и какие методы атак применяют злоумышленники.

Технически каждый элемент сети ловушек представляет собой сервер с одним из образцов популярного ПО, которое имеет веб-интерфейс. В списке ловушек — роутеры, камеры видеонаблюдения, серверы (VPN, виртуализация, почта и др.) на ОС Windows, Linux и др., реконструкции протоколов (удаленного доступа, SMB и т. д.), эмуляция серверов, подверженных часто используемым злоумышленниками уязвимостям и ряд других ханипотов ПО и оборудования, которые могут стать целью атакующих.

В этом отчете приводятся данные по динамике срабатываний на ловушках в 1-м квартале 2025 года по сравнению с 4-м кварталом 2024 года.

Все срабатывания распределены по типу атаки. Наши ловушки позволяют распознать четыре основных типа:

- CVE (попытка эксплуатации уязвимости).
- Bruteforce (попытка подбора пароля).
- Path Traversal (попытка эксплуатации уязвимости для получения доступа к файлам и директориям за пределами предполагаемой директории веб-сервиса).
- Upload (попытка доставки вредоносной нагрузки на атакованный сервер).

Отслеживание атак на ловушки позволяет фиксировать изменение в поведении злоумышленников и в какой-то мере предсказать их тактики и техники в атаках на ИТ-инфраструктуры реальных организаций.

Методология

Поскольку от квартала к кварталу количество активных ловушек варьируется, в этом отчете мы оперируем нормализованными данными — то есть не абсолютным числом срабатываний ловушек на атаки конкретного типа, а их усредненным значением в пересчете на количество ловушек, доступных под атаки каждого типа.

Отдельно мы рассмотрим данные сервиса PDNS. Он осуществляет мониторинг коммуникаций различных вредоносных программ с серверами управления из зараженных сетей на территории России, что позволяет оценить распространенность угроз в стране.

Данные с сенсоров PDNS

Вторая часть отчета описывает ландшафт угроз на территории России, данные о котором собраны с инфраструктуры PDNS.

DNS-серверы используются при интернет-соединении. Каждый раз, когда пользователь или приложение осуществляет попытку соединения с тем или иным веб-ресурсом, браузер делает обращение на DNS-сервер, который хранит информацию о том, какое доменное имя какому IP-адресу соответствует.

Информация о попытках соединений (резолвах) анализируется с помощью технологии passive DNS. Она сравнивает список IP-адресов и доменов, с которыми устанавливалось соединение, со списком IP-адресов и доменов, 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, которое может указывать 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 признакам:

— деятельности известных профессиональных хакерских группировок (APT);
— работы инструментов удаленного администрирования (Remote Access Tools, RAT);
— заражения вредоносами-стилерами (ВПО, похищающее конфиденциальную информацию);
— присутствия ботов одного из известных ботнетов;
— заражения вымогателями;
— заражения вредоносным ПО для майнинга криптовалют;

— заражения загрузчиками — ВПО, способным устанавливать на атакованный компьютер дополнительные вредоносы;
— перехода на фишинговые страницы.

Российские организации, где выявляются признаки заражения IT-инфраструктуры, классифицируются нами по двум критериям: их географическому положению и принадлежности к сфере экономики. Во второй группе выделяем восемь категорий:

— Государственный сектор.
— Здравоохранение.
— Образование.
— Промышленность.
— Пищевая промышленность.
— Финансовая отрасль.
— Телекоммуникационная отрасль.
— ИТ-организации.

Отслеживание изменений в ландшафте угроз на основе данных PDNS позволяет получить самое общее понимание того, для организаций из каких сфер определенные угрозы представляют наибольшую опасность.

В приложении к отчету мы приведем сводные таблицы, демонстрирующие среднее количество событий на организацию в разных отраслях и индустриях на региональном уровне. Сравнение этих данных с общим средним показателем количества событий по всем организациям позволяет понять, в каких регионах ситуация лучше, а в каких хуже.

Информация в отчете является субъективной оценкой ландшафта киберугроз, сделанной на основе доступной Solar 4RAYS информации с сенсоров и ханипотов. Сведения и выводы в отчете не могут быть основанием для каких-либо решений в области практической информационной безопасности. Для детальных консультаций следует обращаться в Solar 4RAYS.

Основные результаты 1 квартала 2025 года

Ханипоты:

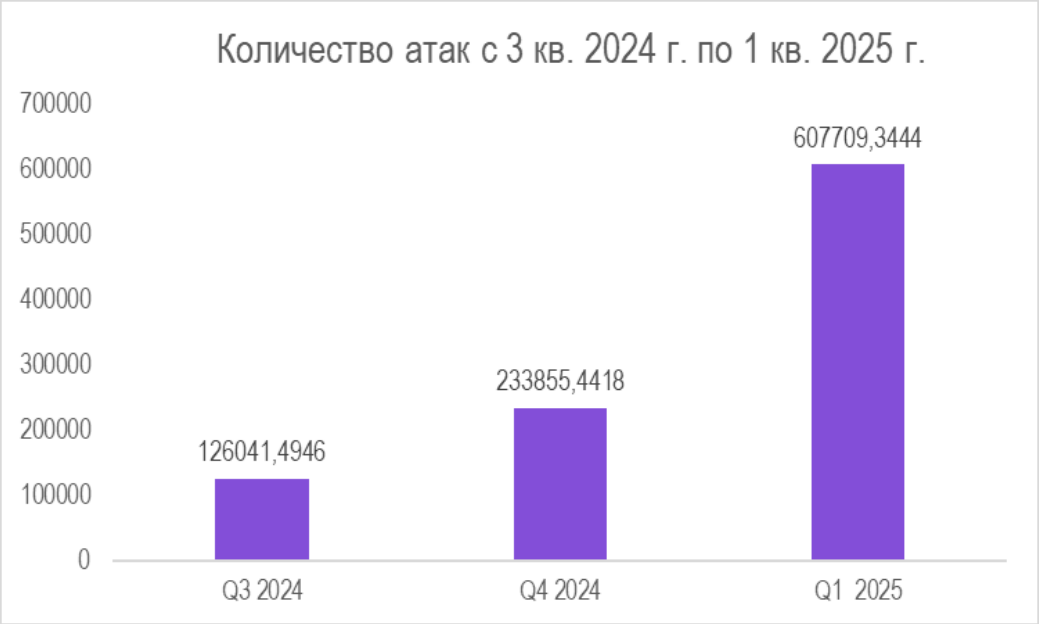
— Общее число зафиксированных ловушками атак составило 607,7 тыс., что на 159,87% больше, чем в последнем квартале 2024 года.
— Значительнее всего выросла доля Bruteforce-атак: относительно атак других типов рост составил 5 процентных пунктов, а в абсолютном выражении — 172,3%. Вероятная причина — злоумышленники активно обновляют базы скомпрометированных аутентификационных данных и используют их как точку входа в опубликованные сервисы организаций.
— США, Китай, Россия и Индия по-прежнему остаются странами, с территории которых на ханипоты было зарегистрировано больше всего атак. В совокупности на них пришлось 51% всех зафиксированных атак.
— Среди атак типа Bruteforce лидируют атаки на SSH и Telnet с показателем в 77%, для сравнения: в 4-м квартале 2024 г. их было всего 13%.
— Более половины атак (56%) пришлось на платформу Kubernetes. На втором месте (13,1%) — Confluence. Кварталом ранее среди лидеров в этой категории были продукты FortiNet и протокол UPnP.

Сенсоры PDNS:

— Общее количество срабатываний, свидетельствующих о возможном заражении вредоносным ПО, в 1-м квартале 2025 года выросло на 145,6% по сравнению с 4-м кварталом 2024 года — с 1,21 млн до 2,97 млн.
— Общее число организаций, в которых было зарегистрировано хотя бы одно событие потенциального заражения сократилось на 34,18% — до 22,1 тыс., а количество событий на организацию, напротив, выросло. Рост числа событий и сокращение количества организаций спровоцировали увеличение среднего показателя заражений на одну организацию. Если в 4-м квартале он составлял 40,71 события, то по итогам 1-го — уже 134,33 события. Заражения в среднем стали выявляться чаще.
— В отличие от двух предыдущих кварталов, в 1-м квартале 2025 года наибольшую угрозу для организаций представляли программы-стилеры. Их доля за квартал увеличилась значительнее других — на 14,96 п.п., до 35,54% всех зафиксированных потенциально вредоносных событий.
— Самый значительный рост показателя среднего числа атак на организацию зафиксирован в промышленной и финансовой сферах, на предприятиях топливно-энергетического комплекса и в IT. Самый низкий из них — в телекоме, госсекторе и сфере образования.

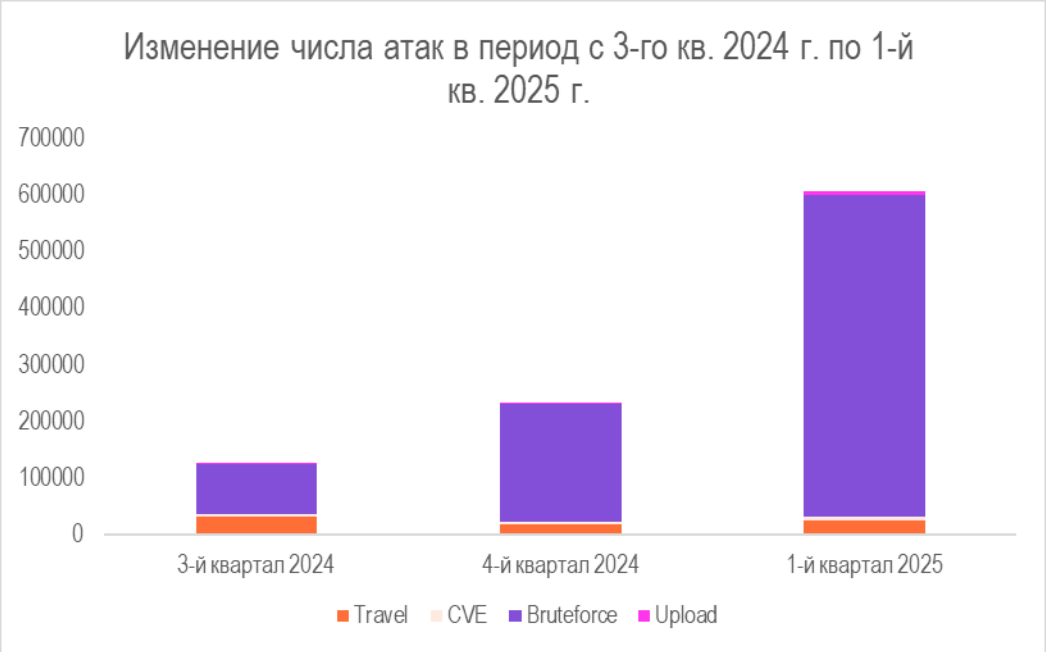
Ловушки-ханипоты: общая статистика и география атак

В первом квартале 2025 года общее количество зафиксированных ловушками атак составило 607,7 тыс., что на 159,87% больше, чем кварталом ранее, когда было обнаружено 233,8 тыс. Примечательно, что количество атак на наши ханипоты растет уже третий квартал к ряду, что отчасти обусловлено постоянным совершенствованием нашей инфраструктуры ханипотов, но также и ростом активности злоумышленников, который в первом квартале оказался особенно значительным.



Тем не менее общее распределение типов атак осталось на прежнем уровне. Чаще всего сенсоры Solar 4RAYS фиксировали Bruteforce-атаки, второе место заняли попытки эксплуатации уязвимостей (CVE), третье — перебор каталогов веб-сайта (Path Traversal), а загрузка и установка полезной нагрузки (Upload) — четвертое.

Доля Bruteforce-атак в 1-м квартале выросла сильнее всего: относительно других типов атак рост составил 5 процентных пунктов, а в абсолютном выражении — и вовсе 172,3%. Мы связываем это изменение с активизацией злоумышленников, которые, очевидно, стремятся обновить свои базы действующих логинов и паролей от доступных из сети инфраструктур.

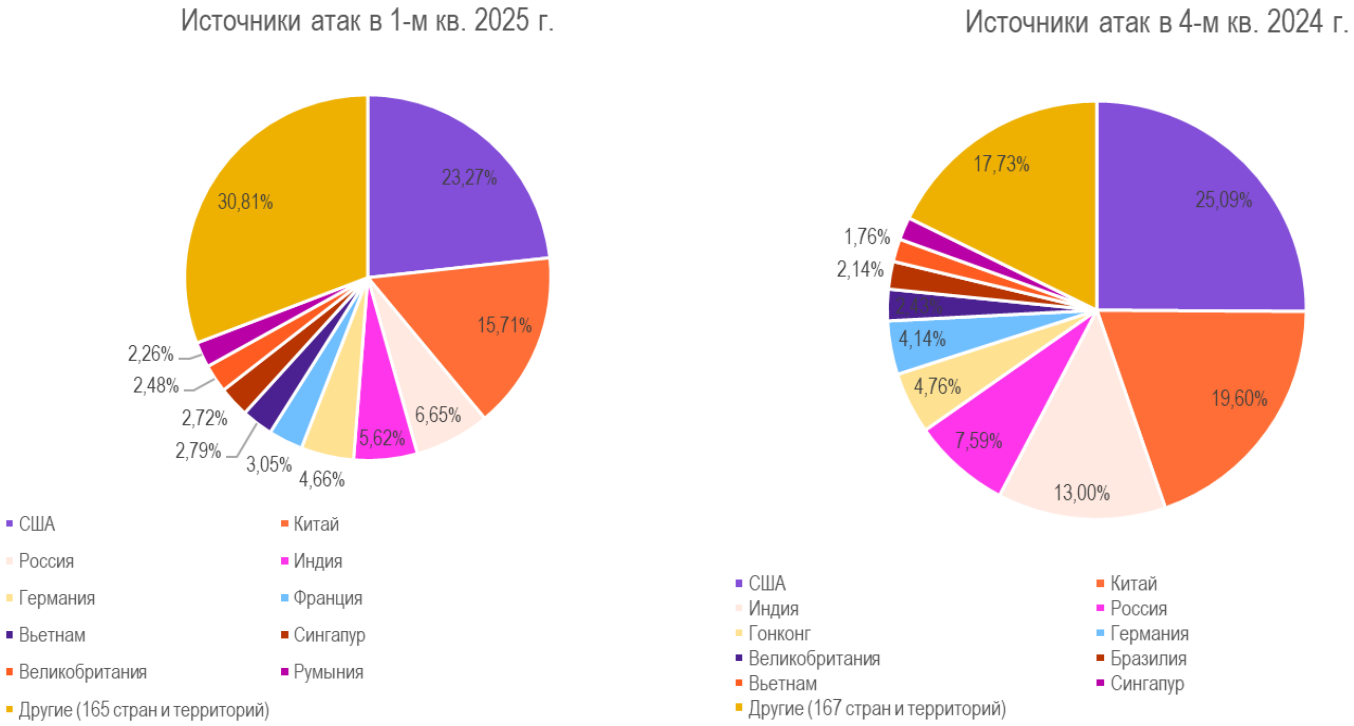


Тип атаки	Q4 2024	Q1 2025	Изменение
BRUTEFORCE	209427,3676	569921,7	+172,13%
TRAVEL	18210,89362	25187,7	+38,31%
CVE	3804,555556	6497,444444	+70,78%
UPLOAD	2412,625	6102,5	+152,94%

Изменение количества атак на ханипоты по типам

География источников атак

В топе стран — источников атак в 1-м квартале изменений мало. США (23%), Китай (16%), Россия (7%) и Индия (5%) остаются теми странами, с территории которых на ханипоты было зарегистрировано больше всего атак.



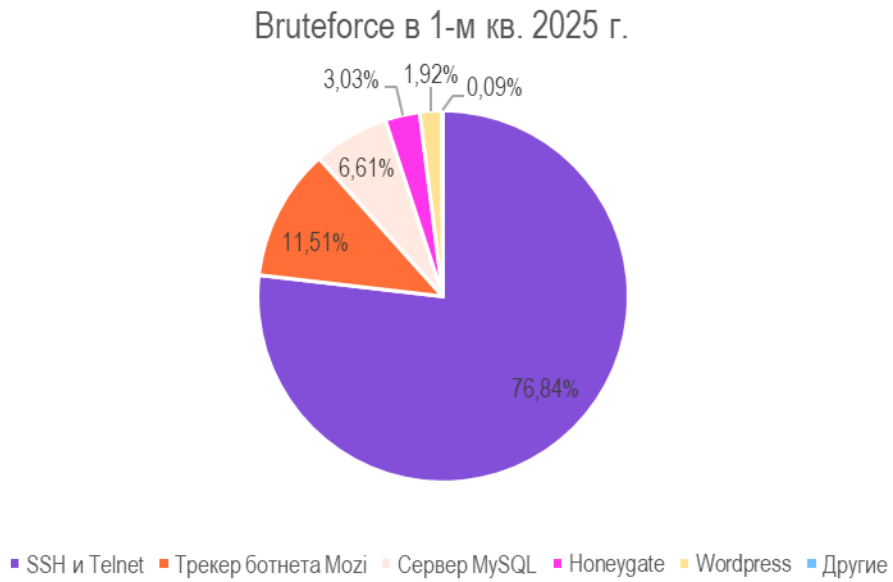
В 4-м квартале картина была несколько иной. Россия занимала 4-е место с 7% атак, а на третьем месте была Индия с 13%. Лидеры — США и Китай — остались на тех же позициях.

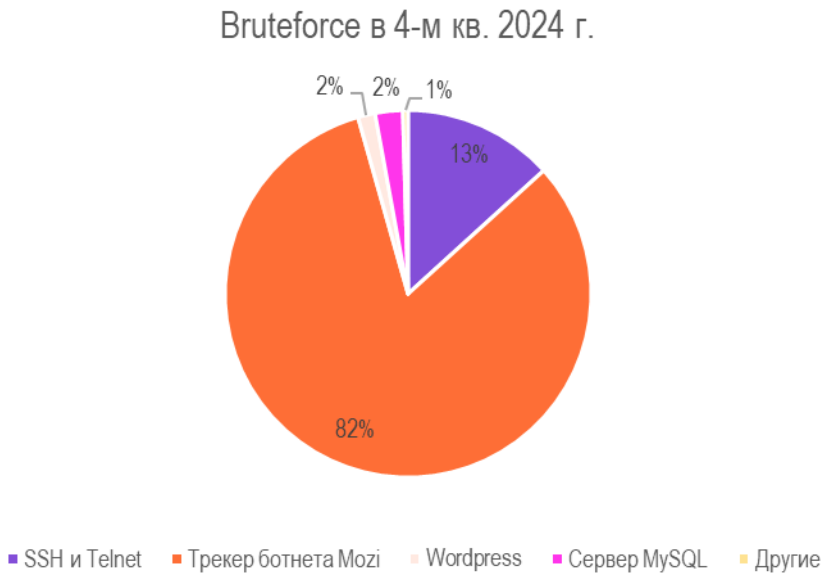
Изменение местоположения источников атак вызвано разными причинами, среди которых изменение географического ландшафта зараженных ПО для автоматизации атак, появление в открытом доступе экплойтов для уязвимостей в ПО, популярном в тех или иных странах, и т. д.

Типы атак

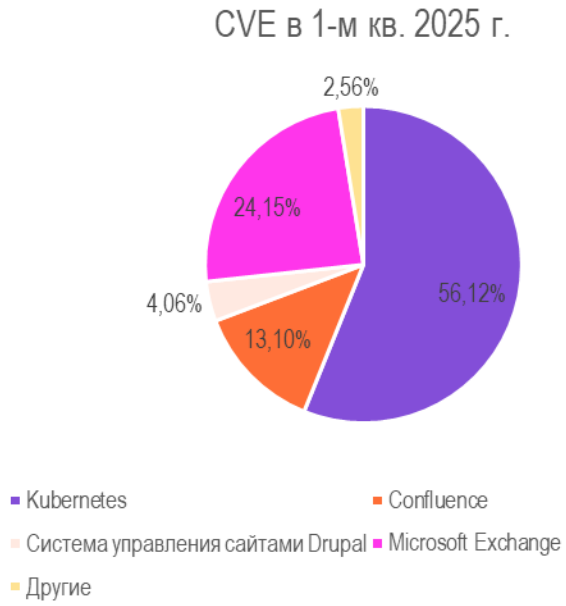
Bruteforce

В 1-м квартале произошла одна значительная перемена: доля атак ботов, унаследовавших полезные нагрузки ботнета Mozi, упала до 11% с 82% в 4-м квартале. Пальму первенства в атаках типа Bruteforce взяли атаки на SSH и Telnet, у которых в 4-м квартале 2024 г. было всего 13%, а в 1-м квартале 2025 г. — уже 77%. Также в абсолютном выражении более чем вдвое сократились атаки на движок Wordpress, и в 1-м квартале он уступил третье место атакам, направленных против серверов MySQL, на которые пришлось 7%.



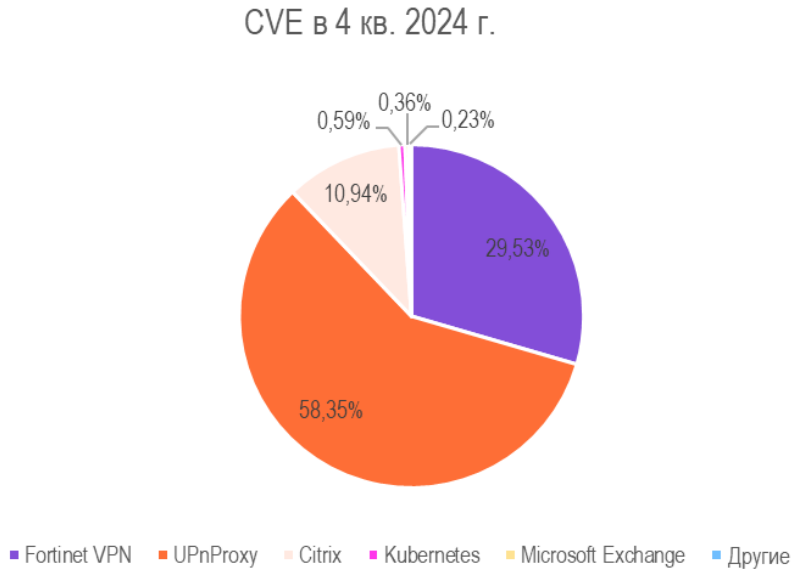


CVE



Значительные изменения произошли в 1-м квартале с автоматизированными попытками эксплуатации уязвимостей. Если в 4-м квартале на первом месте были продукты Fortinet, на втором — атаки против протокола UPnP, а на третьем — продукты Citrix, то в первой четверти 2025 года более половины атак (56%) пришлось на платформу Kubernetes. На втором месте в 1-м квартале 2025 года — Confluence (13,1%). Изменения наглядно демонстрируют смену фокуса злоумышленников, произошедшую в течение квартала. Вероятно, несколько опасных уязвимостей, обнаруженных в продуктах Fortinet в конце прошлого года, получили патчи в большинстве организаций, и атакующие потеряли интерес к этим продуктам.

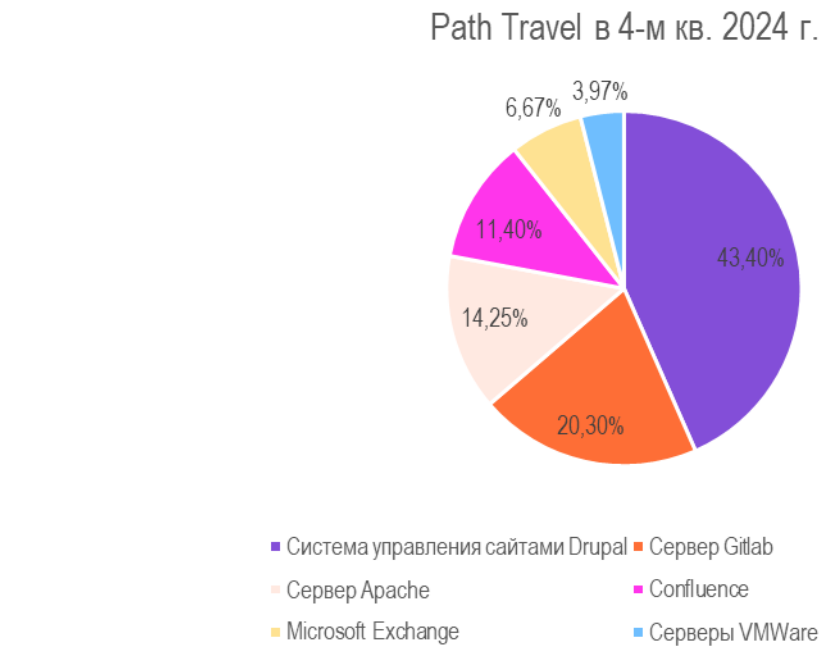
В то же время, по данным мониторинга Solar 4RAYS, в 1-м квартале в Kubernetes обнаружили сразу 5 опасных уязвимостей, что могло привлечь повышенное внимание к этому продукту злоумышленников. Однако довольно быстро для этих уязвимостей вышли обновления, но традиционно организации не спешат их устанавливать, что создает «окно возможностей» для атак.



Path Traversal и Upload

В 1-м квартале значительно сократилась доля атак типа Path Traversal на системы управления сайтами Drupal. Если в последней четверти прошлого года атаки на этот продукт были самыми распространенными (43,4%), то в начале 2025 года этот показатель снизился до 19,7% и на первое место вышли серверы GitLab (32,85%).

Значительно возросла и доля атак на Confluence (с 11,4% до 31,51%).



В атаках типа Upload значительных перемен не наблюдалось. Как и в последней четверти 2024 года, 99% таких атак пришлось на SSH и Telnet.

Сенсоры PDNS: общая статистика

Общее количество срабатываний, свидетельствующих о возможном заражении вредоносным ПО, в 1-м квартале 2025 года выросло на 145,6% по сравнению с 4-м кварталом 2024 года — с 1,21 млн до 2,97 млн.

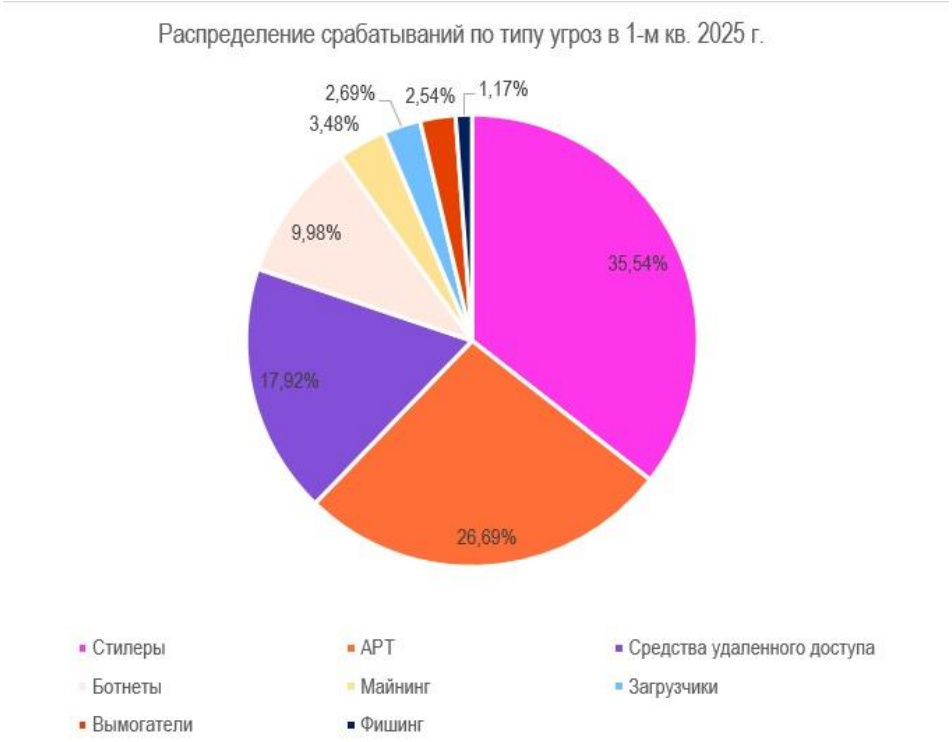
Общее число организаций, в которых было зарегистрировано хотя бы одно событие потенциального заражения сократилось на 34,18% — до 22,1 тыс. Рост числа событий и сокращение количества организаций спровоцировали увеличение среднего показателя заражений на одну организацию: если в 4-м квартале 2024-го он составлял 40,71 события, то по итогам 1-го квартала 2025 года — уже 134,33 события.

Показатель	4 квартал 2024 г.	1 квартал 2025 г.	Изменения
Общее число срабатываний	1210245	2976017	+145,9%
Число организаций	29726	22153	-34,18%
Среднее количество атак на организацию	40,71	134,33	+229,97%

Как мы и предполагали, существенное снижение количества событий, указывающих на потенциальное заражение инфраструктуры, которое мы регистрировали в 4-м квартале, оказалось временным явлением. Скорее всего, оно было связано с общим снижением бизнес-активности в конце ноября — декабре из-за осенних и зимних праздников. Увеличение среднего числа атак может объясняться и возвращением атакующих к активной деятельности, а также с возможным изменением тактики атак — акцент переместился с количества на качество.

Типы угроз

Типы угроз: общие сведения



В отличие от двух предыдущих кварталов, в 1-м квартале 2025 года наибольшую угрозу для организаций представляли программы-стилеры.

Их доля за квартал увеличилась значительнее других — на 14,96 п.п. Изменение может быть связано с высокой активностью некоторых семейств стилеров (Lumma,

DarkWatchman, SnakeKeylogger), зафиксированной в конце 4-го — начале 1-го квартала как сотрудниками Solar 4RAYS, так и другими экспертами по ИБ. Причиной могло стать общее увеличение активности атакующих, вовлеченных в кибершпионаж, в том числе в связи с геополитическими событиями.

Тип угрозы	Q4 2024	Q1 2025	Изменение
Средства удаленного доступа (RAT)	24,41%	17,92%	-6,49 п.п.
APT	23,41%	26,69%	+3,28 п.п.
Ботнеты	20,67%	9,98%	-10,69 п.п.
Стилеры	20,58%	35,54%	+14,96 п.п.
Майнинг	5,79%	3,48%	-2,31 п.п.
Загрузчики	2,54%	2,69%	+0,15 п.п.
Фишинг	2,03%	1,17%	-0,86 п.п.
Вымогатели	0,57%	2,54%	+1,97 п.п.

На индикаторы APT-группировок в 1-м квартале приходилось более четверти зафиксированных событий, что чуть больше, чем кварталом ранее. Значительное снижение доли показали ботнеты (-10,69 п.п.) и RAT (-6,49 п.п.).

Само по себе распределение событий, связанных с разными типами угроз, говорит скорее о характере их сетевой активности (например, программы-вымогатели могут генерировать меньше событий, чем инструментарий APT-группировок), в то время как их динамика от квартала к кварталу указывает на изменение уровня опасности той или иной угрозы. Таким образом, значительно изменилась доля стилеров (их явно стало больше) и ботнетов (а их стало меньше), а остальной ландшафт сохранился примерно в прежнем виде.

Атакованные сферы экономики

Среднее количество событий, свидетельствующих о возможном заражении в пересчете на одну организацию, в 1-м квартале выросло во всех сегментах, но в разных масштабах.

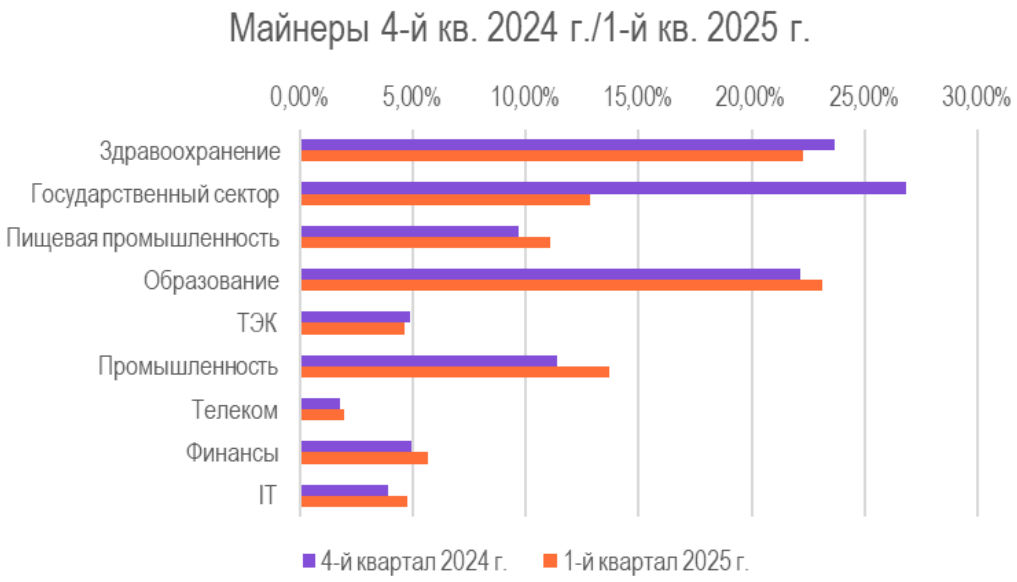
Среднее количество событий	4-й кв. 2024 г.	1 кв. 2025 г.	Изменение
Сфера			
Здравоохранение	80,24	331,79	313,47%
Государственный сектор	27,27	65,55	140,32%
Пищевая промышленность	41,97	178,15	324,45%
Образование	16,45	52,34	218,17%
ТЭК	59,54	313,73	426,85%
Промышленность	34,04	231,8	580,82%
Телеком	81,32	157,68	93,89%
Финансы	19,18	118,216	516,06%
IT	42,91	248,31	478,59%

Самый значительный рост среднего числа событий зафиксирован в промышленности, финансовой сфере, на предприятиях топливно-энергетического комплекса и в IT. При этом самое высокое среднее число потенциально вредоносных событий (в пересчете на одну организацию) отмечается в сферах здравоохранения, ТЭК, IT, промышленности и пищевой промышленности.

Типы угроз: детали

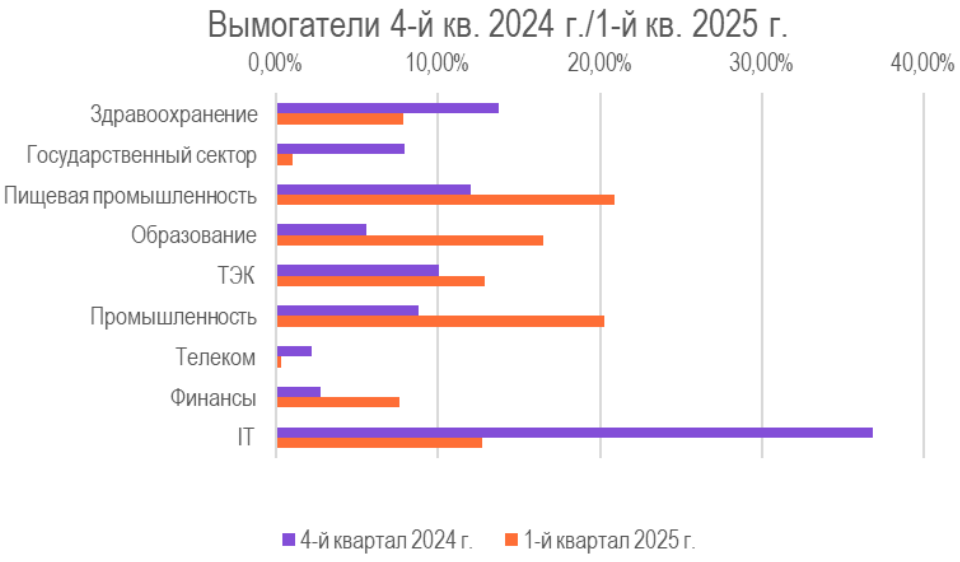
Далее рассмотрим в деталях, какие угрозы чаще встречаются в организациях и на предприятиях из разных отраслей и как ситуация менялась по сравнению с предыдущим кварталом.

Майнеры



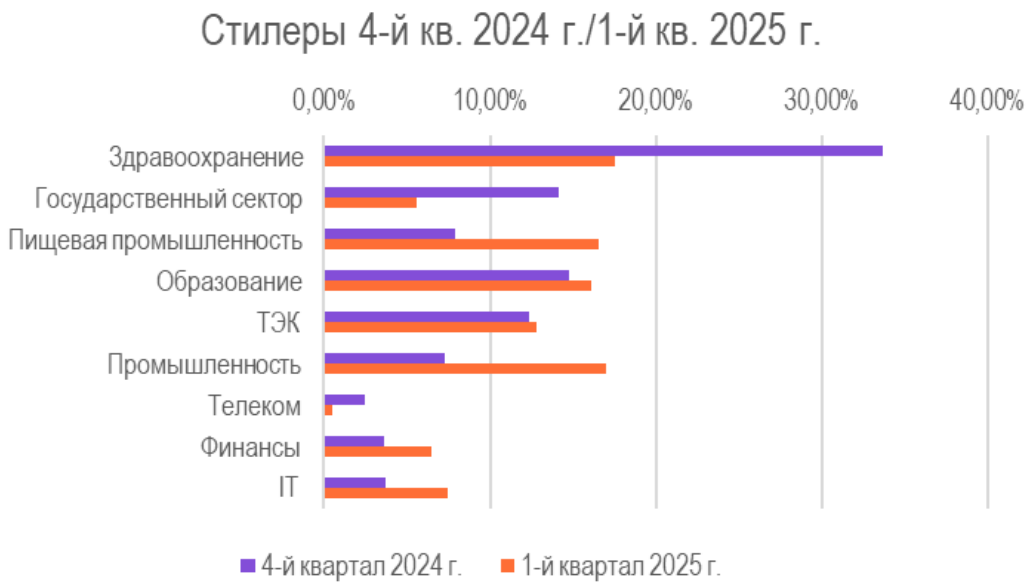
Почти во всех сферах, кроме здравоохранения, госсектора и ТЭК, доля майнеров незначительно выросла. Самое сильное падение мы наблюдаем в организациях государственного сектора, что может быть свидетельством улучшения уровня базовой безопасности — например, более тщательной проверки IT-инфраструктуры на заражения с помощью СЗИ.

Вымогатели



Атакующих интересует не только шпионаж, но и возможность заработка. Значительно выросла доля событий, связанных с заражением инфраструктуры на промышленных предприятиях, в образовательных организациях и организациях топливно-энергетического комплекса. Все это (за исключением образования) отраслевые сегменты, в которых успешное заражение шифровальщиком может привести к остановке важных технологических процессов — одному из самых нежелательных последствий. С этой точки зрения подобные предприятия являются лакомым куском для злоумышленников, специализирующихся на схемах с шифровальщиками, — собранная статистика может служить косвенным тому подтверждением.

Стилеры



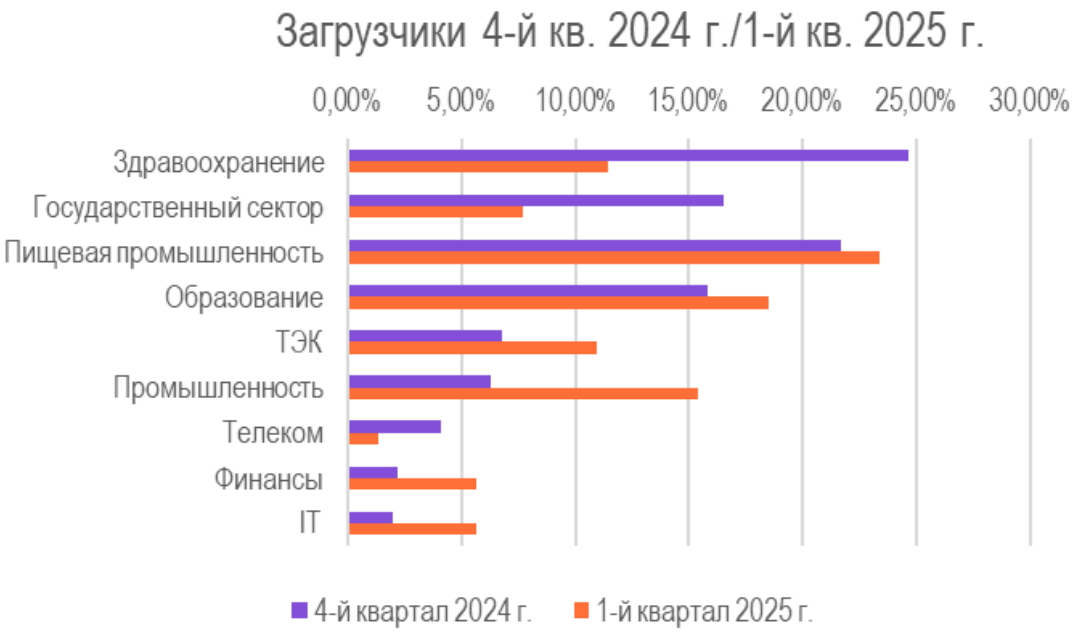
Как отмечалось выше, стилеры в первом квартале показали значительный рост, особенно на предприятиях промышленности, в IT и финансовых организациях. Стилеры позволяют как получить информацию, которую можно позже использовать в атаках на организацию, так и завладеть конфиденциальными данными, которые можно продать на черном рынке. Очевидно, что среди исследуемых организаций всех перечисленных отраслей найдется немало потенциальных целей для злоумышленников, IT-инфраструктуры которых могут содержать большие объемы чувствительных сведений.

APT

Традиционно активность прогосударственных APT-группировок и наемников, которые могут работать как на государственные структуры, так и на частных заказчиков, обнаруживается в каждой исследуемой сфере. В первом квартале эти категории злоумышленников проявили повышенный интерес к промышленности, образованию, ТЭК, финансам и сегменту информационных технологий. IT-отрасль, скорее всего, представляет интерес не столько как источник ценных сведений, сколько как плацдарм для атак через доверительные отношения с компаниями из других секторов, с которыми IT-сегмент часто имеет сетевую связность.

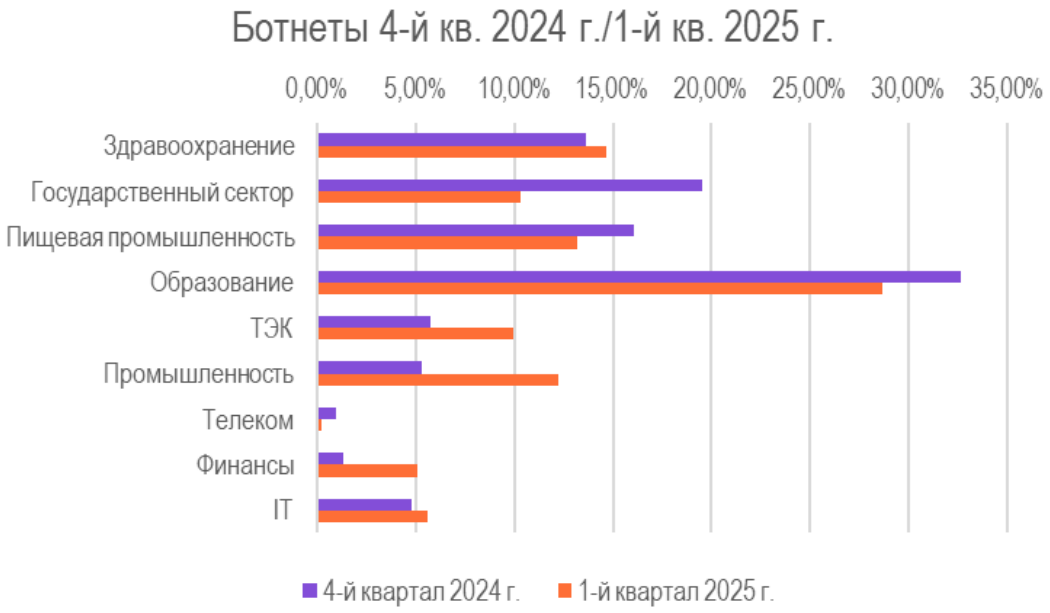
Все прочие отрасли — типичные цели для APT-группировок, и изменение доли событий, связанных со сложными атаками, может свидетельствовать о смене фокуса, новых видах заражения и других изменениях, конкретизировать которые сложно, не зная контекста каждой атаки.

Загрузчики



В атакованных сетях, где была обнаружена какая-либо специфическая полезная нагрузка (майнер, стилер, имплант APT-группировки), обычно содержатся следы присутствия и активности программ-загрузчиков, чья цель состоит как раз в том, чтобы закрепиться в атакованной системе и доставить в нее ВПО, нужное злоумышленникам. Поэтому связь между увеличением числа событий, связанных с загрузчиками, и ростом других событий в одних и тех же отраслях не случайна.

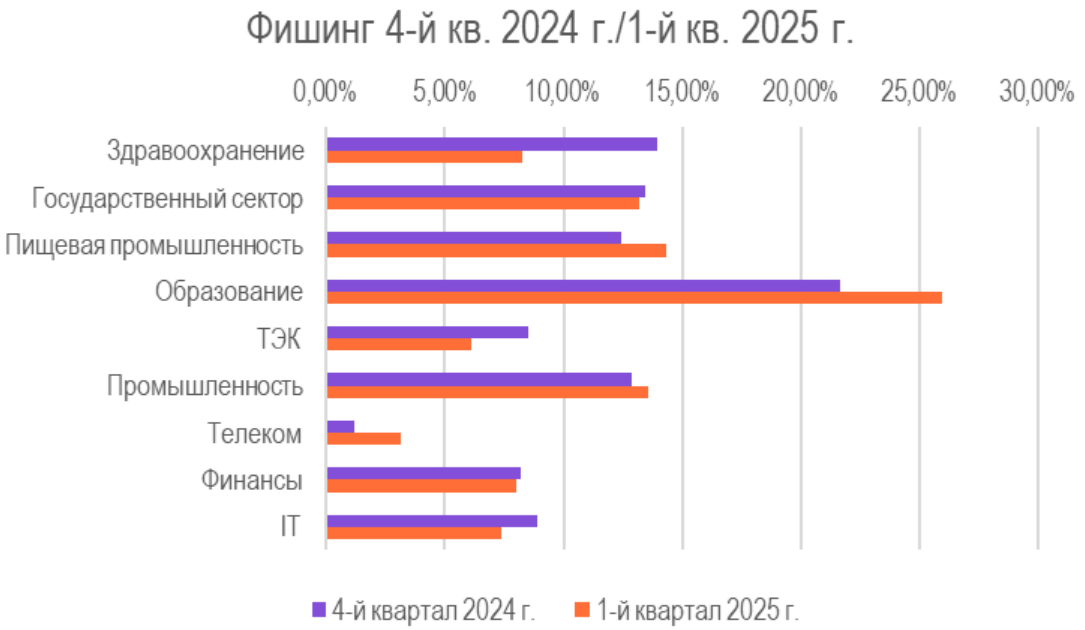
Ботнеты



ТЭК, промышленность (за исключением пищевой), финансы и IT — ключевые сферы, где доля событий, связанных с активностью ботнетов, показала значительный рост. Боты,

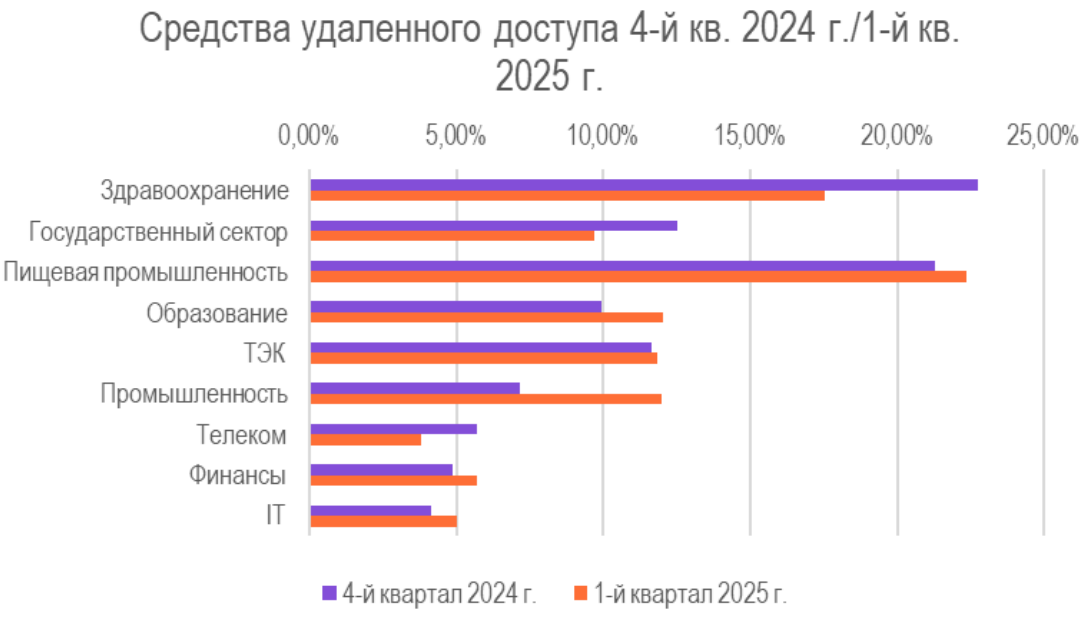
включающие систему в ботнет, обычно появляются на ней автоматически — в результате удачной автоматизированной атаки через какую-нибудь уязвимость или работы загрузчика. Изменение доли на графике выше скорее означает, что в IT-инфраструктурах организаций некоторых отраслей в 1-м квартале присутствовало значительное количество уязвимых к атакам систем.

Фишинг



Небольшой рост фишинговых атак в организациях системы образования в 1-м квартале может быть связан с фактором сезонности: например, в вузах во время зимних сессий по сравнению с концом года может наблюдаться всплеск фишинговой активности.

Средства удаленного доступа (RAT)



Значительный рост доли событий, связанных с использованием средств удаленного доступа в 1-м квартале, зафиксирован только в предприятиях промышленности. Скорее всего, это свидетельство общего тренда, в рамках которого промышленность стала одной из индустриальных отраслей, в которых признаки исследуемых угроз встречались в первом квартале 2025 года значительно чаще, чем в предыдущем.

Заключение и рекомендации

Угрозы, зафиксированные на ловушках, позволяют говорить о том, на что следует обращать внимание сотрудникам ИБ-команд для обеспечения безопасности своих инфраструктур. Атаки типа Bruteforce остаются ключевой массовой угрозой для SSH и Telnet. Фокус злоумышленников на Kubernetes в атаках через уязвимости стал яркой тенденцией 1-го квартала и, с нашей точки зрения, является маркером того, на что следует обращать внимание корпоративным службам ИБ.

Картина заражений IT-инфраструктур в указанных сферах деятельности, полученная с помощью PDNS, позволяет сделать несколько выводов.

1. Основное, что изменилось, — резко увеличилось число атак стилеров, которые стали значимой угрозой практически для всех отраслей.
2. Самый высокий средний показатель количества событий в здравоохранении, ТЭК, IT, промышленности говорит о том, что IT-инфраструктуры в таких организациях представляют повышенный интерес для атакующих, что создает необходимость пристального внимания к защите таких сетей.

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

- ✓ Регулярно сканировать внешний периметр на предмет изменения опубликованных сервисов и наличия в них уязвимостей.
- ✓ Публиковать в интернете 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.
- ✓ Оперативно обновлять все используемое в инфраструктуре ПО.

- ✓ Строго контролировать удаленный доступ в инфраструктуру, особенно для подрядчиков.
- ✓ 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 одной копии за пределами основной инфраструктуры.
- ✓ В случае подозрения на атаку следует немедленно провести оценку компрометации, а лучше — проводить ее на регулярной основе.
- ✓ Повышать уровень 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.

Для раннего обнаружения киберугроз и своевременного реагирования нужно собирать данные кибербразведки (Threat Intelligence) начиная с ручного поиска, OpenSource и уведомлений регуляторов, до продвинутых сервисов поставки потоков данных (фидов).

Solar TI Feeds — поток данных об актуальных киберугрозах в реальном времени. Если вы заинтересованы в непрерывном получении разведданных об актуальных киберугрозах, свяжитесь с нами, чтобы подключить пилот сервиса.

Приложение: региональные данные

В данном приложении представлена информация о среднем количестве событий, указывающих на потенциальное заражение в отслеживаемых отраслях на региональном уровне. В каждой таблице — десять регионов с наиболее высоким показателем.

Средний показатель по всем отраслям и регионам в 1-м квартале составил 134,33 события. Если в каком-то регионе показатель значительно превышает это значение, это может означать повышенный интерес атакующих к конкретной сфере и возможную необходимость принятия мер в области ИБ.

Пищевая промышленность

Регион	1-й кв. 2025 г.
Республика Коми	3790
Кабардино-Балкарская Республика	2209
Тюменская область	1390
Санкт-Петербург	1187
Республика Марий Эл	340
Вологодская область	267
Ростовская область	247
Чувашская Республика	169
Кировская область	99,69
Удмуртская Республика	89,29
Остальные регионы	40,57

IT

Регион	1-й кв. 2025 г.
Пензенская область	4480
Республика Татарстан	714
Саратовская область	280
Калининградская область	216
Мурманская область	106
Тюменская область	104
Республика Мордовия	73,83
Ульяновская область	33,81
Оренбургская область	26,94
Остальные регионы	22,71
Нижегородская область	17,83

Государственный сектор

Регион	1-й кв. 2025 г.
Кировская область	268
Удмуртская Республика	242
Новосибирская область	98,74
Архангельская область	197
Республика Марий Эл	131
Ульяновская область	93
Краснодарский край	59,51
Ростовская область	42,63
Самарская область	39,25
Ставропольский край	66,5
Остальные регионы	31,16

ТЭК	Регион	1-й кв. 2025 г.
	Карачаево-Черкесская Республика	11 050
	Республика Карелия	5550
	Ямало-Ненецкий автономный округ	1308
	Ханты-Мансийский автономный округ — Югра	934
	Самарская область	648
	Тульская область	645
	Пензенская область	390
	Удмуртская Республика	315
	Тюменская область	117
	Краснодарский край	83,37
	Остальные регионы	16,5

Промышленность

Регион	1-й кв. 2025 г.
Ямало-Ненецкий автономный округ	21 920
Санкт-Петербург	3803
Челябинская область	955
Ставропольский край	921
Свердловская область	767
Чувашская Республика	591
Кировская область	529
Саратовская область	289
Нижегородская область	201
Удмуртская Республика	102
Остальные регионы	45,63

Образование

Регион	1-й кв. 2025 г.
Санкт-Петербург	2393
Омская область	135
Республика Саха (Якутия)	64,53
Удмуртская Республика	53,78
Республика Марий Эл	45,96
Оренбургская область	40,74
Нижегородская область	39,54
Ставропольский край	33,7
Архангельская область	33,6
Новосибирская область	28,7
Остальные регионы	18,38

Здравоохранение

Регион	1-й кв. 2025 г.
Удмуртская Республика	4683
Республика Мордовия	891
Чувашская Республика	459
Калининградская область	457
Мурманская область	354
Омская область	328
Краснодарский край	195
Тюменская область	183
Нижегородская область	154
Пензенская область	43,62
Остальные регионы	23,3

Финансы

Регион	1-й кв. 2025 г.
Санкт-Петербург	9068
Ульяновская область	1081
Свердловская область	326
Республика Татарстан	226
Удмуртская Республика	184
Нижегородская область	125
Кировская область	71,5
Новосибирская область	56,82
Оренбургская область	51,35
Краснодарский край	28,09
Остальные регионы	18,72

Телекоммуникации

Регион	1-й кв. 2025 г.
Архангельская область	3292
Пензенская область	570
Курганская область	227
Магаданская область	183
Республика Мордовия	127
Санкт-Петербург	74,57
Республика Татарстан	60,16
Республика Саха (Якутия)	59,66
Ульяновская область	48
Чувашская Республика	38,46
Остальные регионы	9,41