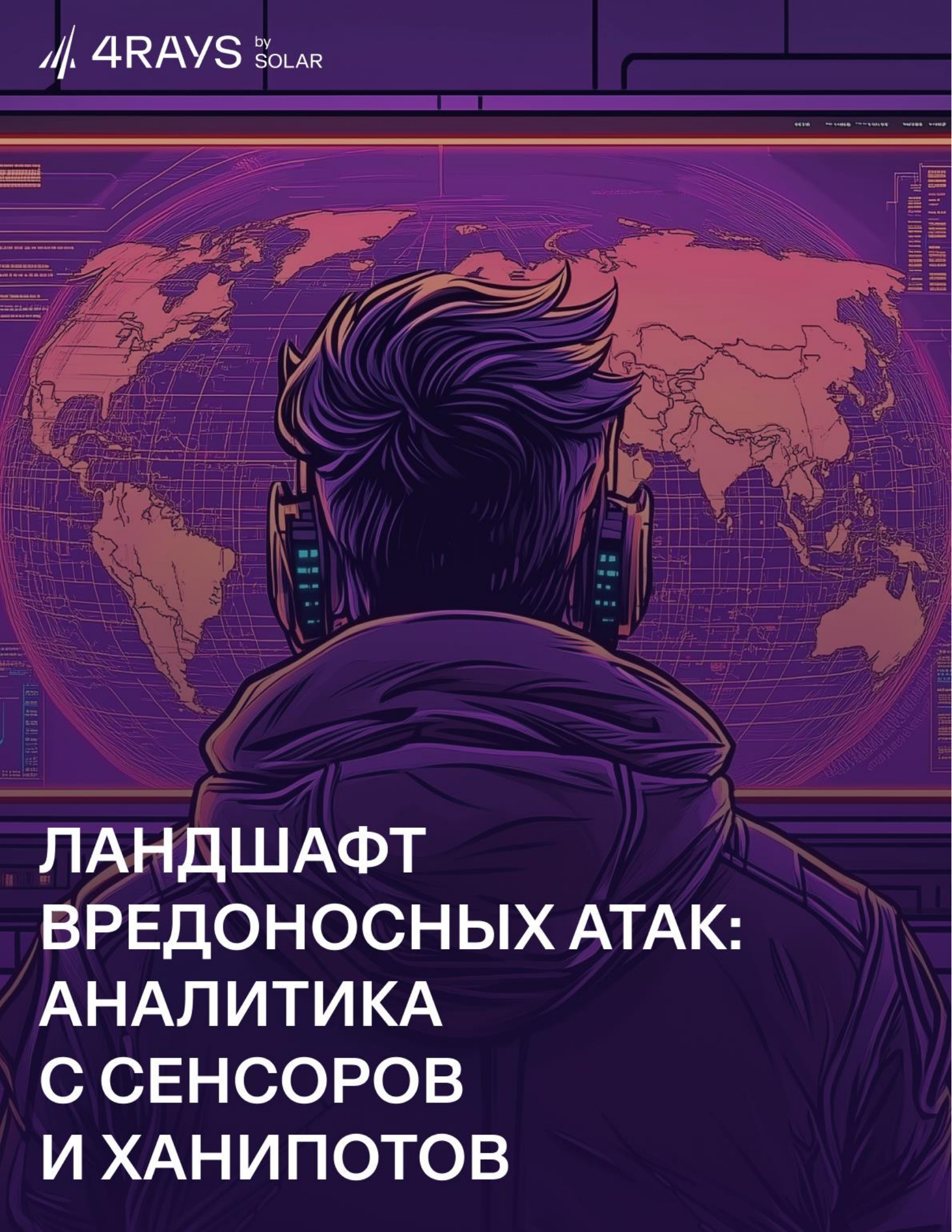
4RAYS by SOLAR



ЛАНДШАФТ ВРЕДОНОСНЫХ АТАК: АНАЛИТИКА С СЕНСОРОВ И ХАНИПОТОВ

Оглавление

Введение

Центр исследования киберугроз Solar 4RAYS ГК «Солар» поддерживает глобальную сеть из более чем сотни сенсоров, разбросанных по всему миру. Они круглосуточно действуют в России, Польше, Франции, Германии, Швейцарии, США, Канаде, Японии, Сингапуре и других странах, предоставляя экспертам компании информацию о том, какие методы атак и как часто применяют злоумышленники.

В отчете представлена аналитика, собранная с сети сенсоров и ханипотов (ловушек) в 3 квартале 2024 года, а также ее сравнение с аналогичным периодом прошлого года.

Полученные данные позволяют фиксировать изменение в поведении злоумышленников и в какой-то мере предсказать их тактики и техники в атаках на ИТ-инфраструктуры реальных организаций. Ловушки распознают четыре основных типа атак:

- 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).

Также в отчете представлена информация о зафиксированной активности вредоносного программного обеспечения в различных отраслях и регионах РФ, что позволяет оценить распространенность киберугроз в стране.

Методология

Поскольку от квартала к кварталу количество активных ловушек варьируется, в этом отчёте мы оперируем нормализованными данными - то есть не абсолютным числом срабатываний ловушек на конкретный тип атак, а их усредненным числом в пересчёте на количество доступных ловушек под каждый тип атак. Пример: абсолютное число срабатываний ловушек на атаки типа Upload в третьем квартале составило 3667. Эти данные получены с 11 ловушек. Таким образом, нормализованное значение составило 333,36 атаки.

Основные результаты

- Самым распространенным типом атак на ловушки в 3 квартале 2024 года оставался Bruteforce, но его доля сократилась в сравнении с тем же периодом 2023 года. А почти четверть всех зафиксированных атак пришлась на Path Traversal – их доля за год возросла;

- Индия, Литва, Китай, США и Франция - источники наибольшего числа атак в отчетном периоде. В 2023 году это список выглядел так: Китай, США, Индия, Россия;

- Большая часть атак типа Bruteforce была сгенерирована ботнетами, подхватившими полезные нагрузки уничтоженного в минувшем году ботнета Mozi;

- Целью большинства атак, нацеленных на эксплуатацию уязвимостей, оказался протокол UPnP;

- Path Traversal-атаки в основном были направлены на продукт для управления сайтами Drupal, серверы Gitlab и Confluence;

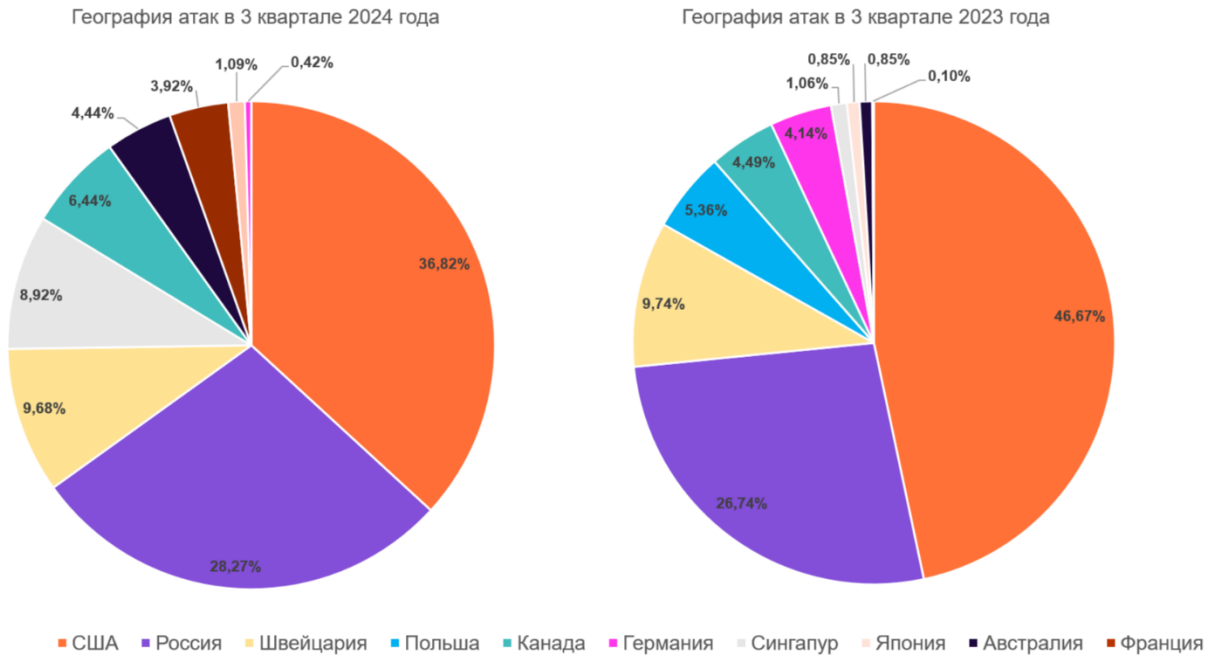
- Здравоохранение, государственные органы и пищевая промышленность - три сферы, где было зафиксировано больше всего событий, указывающих на заражение ВПО;

- Средства удаленного доступа, APT-группировки, ботнеты и стиллеры - самые распространенные угрозы для российских предприятий из различных отраслей;

- Нижегородская и Самарская области, а также Удмуртская Республика лидируют среди регионов с наибольшим числом событий, указывающих на заражение инфраструктуры вредоносным ПО.

Общая статистика и география атак на ловушки

Количество атак (зафиксированных попыток взлома ловушки) в 3 квартале 2024 года составило **126 тыс.** На США пришлось 36,82% всех срабатываний, еще 28,27% - на Россию. Остальные атаки распределились между другими странам, в которых расположены ловушки: Канада, Швейцария, Сингапур, Австралия, Япония, Германия, Франция.

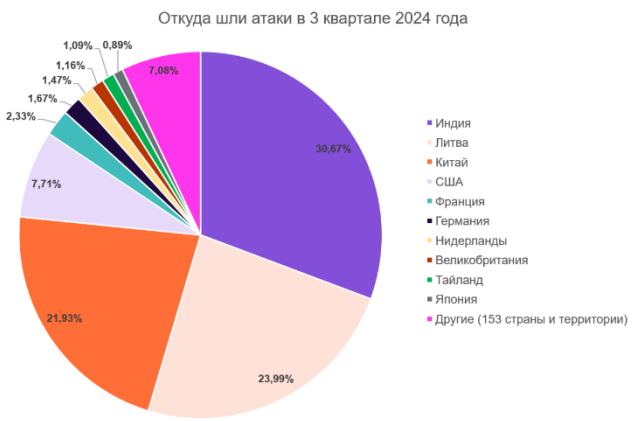


Распределение зафиксированных атак отражает прежде всего географическую распределенность наших ловушек и является скорее техническим параметром, показывающим, в каких странах мы имеем более развитую инфраструктуру ловушек: чем выше доля атак, тем более разнообразны типы ловушек, представленные в стране.

Источники атак

Показательным параметром является регион, из которого на ловушки осуществлялись атаки, поскольку он демонстрирует, где располагались вредоносы, пытающиеся атаковать ловушки. Географическая картина в этом разрезе за год значительно изменилась.

В отчетном периоде источниками более 90% зафиксированных атак оказались 10 стран, включая Индию, Литву, Китай, США, Францию и Германию. В 3 квартале 2023 года в топ-5 входили Китай, США, Индия, Россия и Ливан, а на топ-10 стран приходилось чуть менее 70% всех зафиксированных атак.



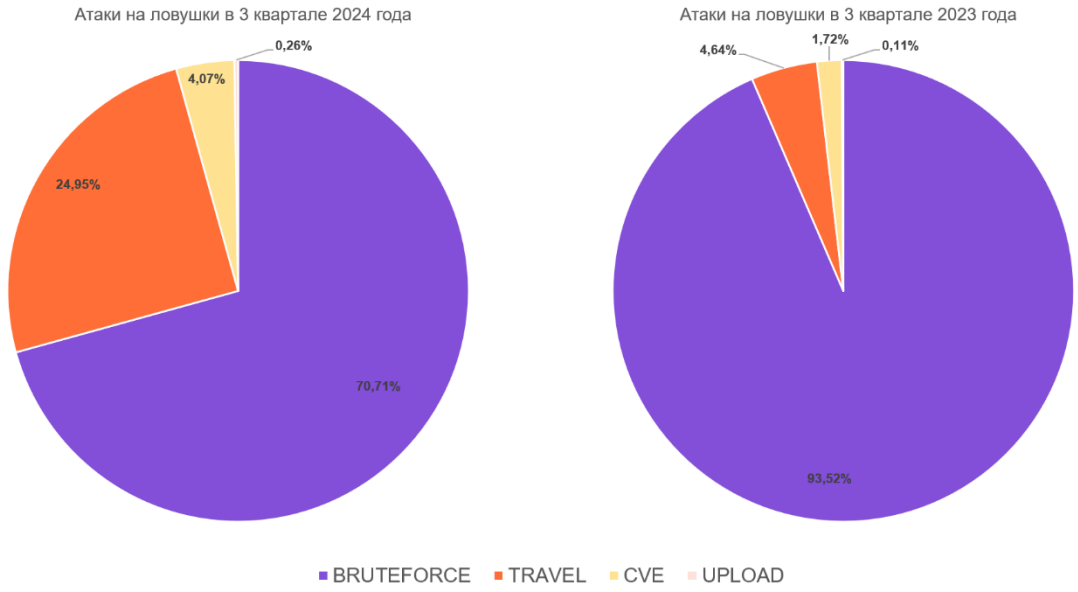
У таких перемен может быть множество причин, и определить их только из статистики невозможно. Примечательно, что в топе стран-источников атак неизменно остаются Индия, Китай, США, Нидерланды и Германия. Одна из причин: распространенность в этих регионах определенного ПО (обычно - масса доступных из сети серверов) и оборудования (например, непропатченные роутеры и т.п.), которые часто становятся “базой” для ботнетов.

Регион атаки	Доля в 3 квартале 2023 года	Доля в 3 квартале 2024 года	Изменение
Китай	20,95%	21,93%	+0,98 п.п.
Индия	10,88%	30,67%	+9,72 п.п.
США	11,07%	7,71%	-3,36 п.п.
Нидерланды	2,73%	1,47%	-1,26 п.п.
Германия	1,97%	1,67%	-0,3 п.п.
Ливан	4,65%	0,04%	-4,61 п.п.
Вьетнам	4,14%	0,18%	-3,96 п.п.
Мексика	2,11%	0,26%	-1,85 п.п.
Тайланд	0,96%	1,09%	+0,13 п.п.
Литва	0,29%	23,99%	+23,7 п.п.
Великобритания	0,47%	1,16%	+0,69 п.п.
Япония	0,61%	0,89%	+0,28 п.п.

Россия	8,96%	0,03%	-8,93 п.п.
Бразилия	1,83%	0,28%	-1,55 п.п.
Франция	1,08%	2,33%	+1,25 п.п.
Другие	30,71%	7,08%	-23,63 п.п.

Типы атак

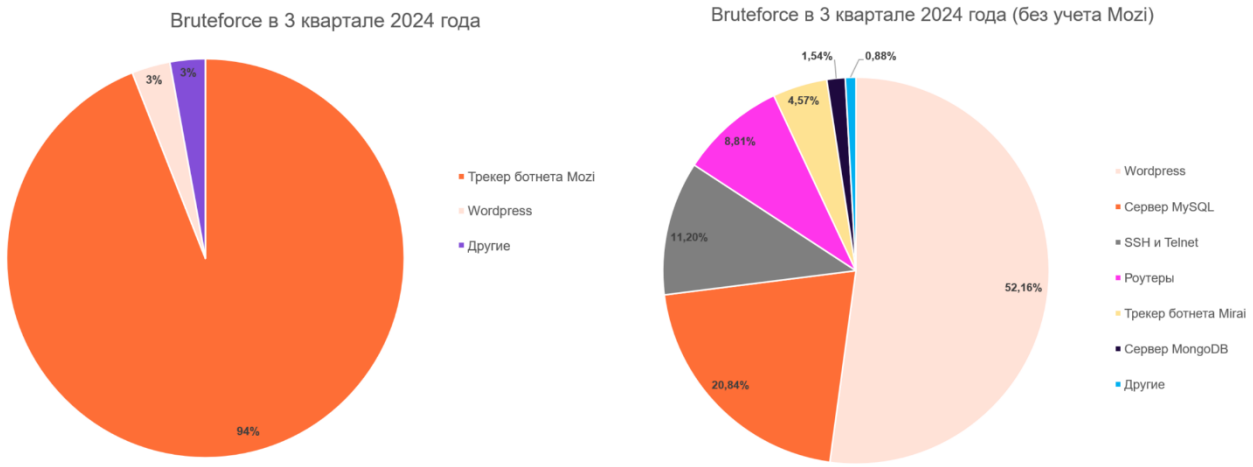
В этом разделе рассмотрим то, как четыре типа атак (Bruteforce, CVE, Path Traversal и Upload) распределились по конкретным ловушкам.



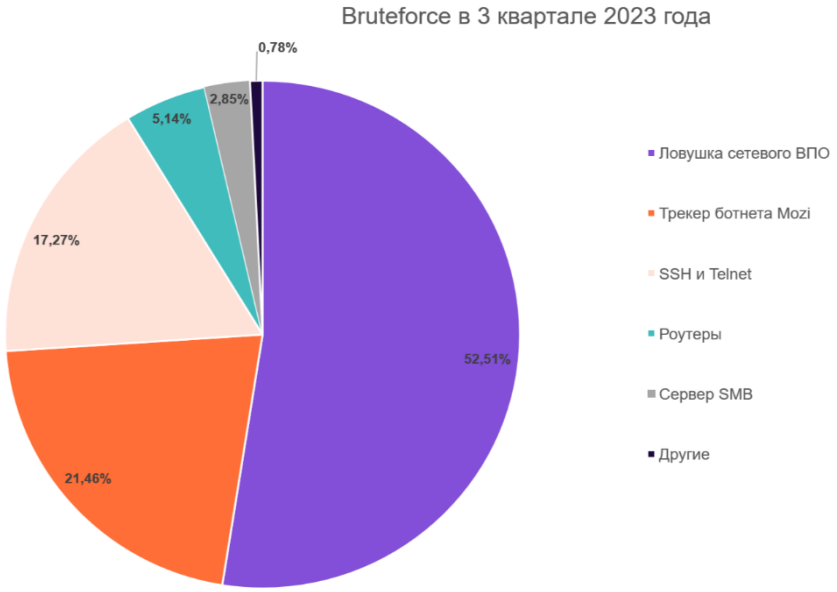
Абсолютное большинство срабатываний в отчетном периоде пришлось на атаки типа Bruteforce. Тем не менее их доля за год сократилась с 93,5% до 70,7%. Доля атак типа Path Traversal, наоборот, увеличилась: с 4,64% до 24,95%. Вероятно, злоумышленники проявляют больший интерес к атакам типа Path Traversal, поскольку потенциально они (удачная эксплуатация уязвимости в сетевом окружении цели) дают больше возможностей, чем просто подбор учетных данных для входа.

Bruteforce

В 3 квартале 2024 года атаки этого типа были зафиксированы на 64 различных ловушках. 94% зафиксированных попыток подбора пароля пришлось на трекер DDoS-ботнета Mozi (обычно атакует IoT-устройства). В конце 2023 года СМИ писали об отключении ботнета, но, как видно из статистики, год спустя он работает (а вернее, другой ботнет – Androxgh0st – может распространять полезные нагрузки, характерные для Mozi). Если исключить ботнет Mozi, то больше половины атак в отчетном периоде пришлось на подбор пароля к серверам Wordpress, MySQL, а также протоколам SSH и Telnet.



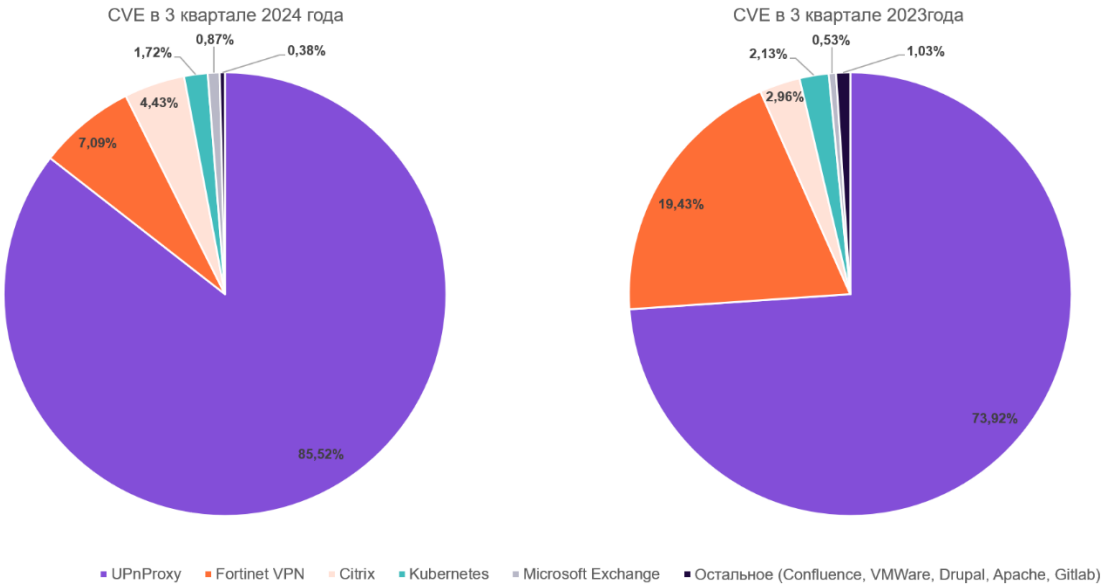
Годом ранее ситуация была иной: более половины атак фиксировалось на ловушке сетевого ВПО (имитирует различные сетевые протоколы, включая SMB, FTP, MySQL, SIP и т.д.), а трекер ботнета Mozi занимал второе место. В топе также были атаки на роутеры.



Главное изменение за год (кроме возвращения ботнета Mozi) — это рост числа атак на Wordpress. На этом “движке” работает множество сайтов, и злоумышленники пытаются массово получить доступ к ним.

Эксплуатация уязвимостей

Большая часть автоматизированных попыток эксплуатации какой-либо уязвимости в 3 квартале пришлась на атаки UPnProxy против протокола UPnP. Она позволяет автоматически создавать правила переадресации портов на устройстве.

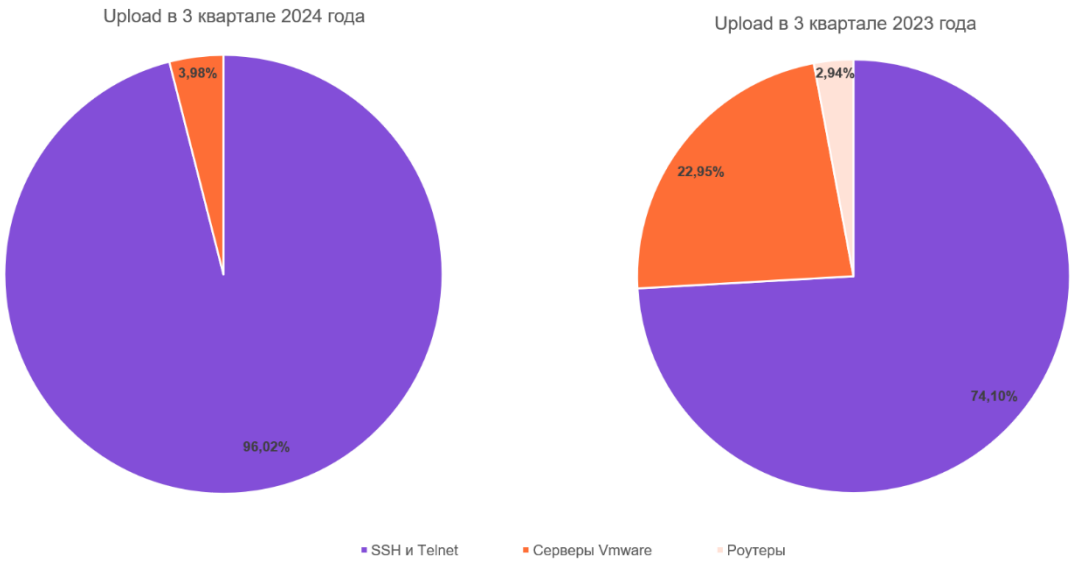


Злоумышленникам уязвимость помогает создавать прокси и таким образом скрывать свою вредоносную активность.

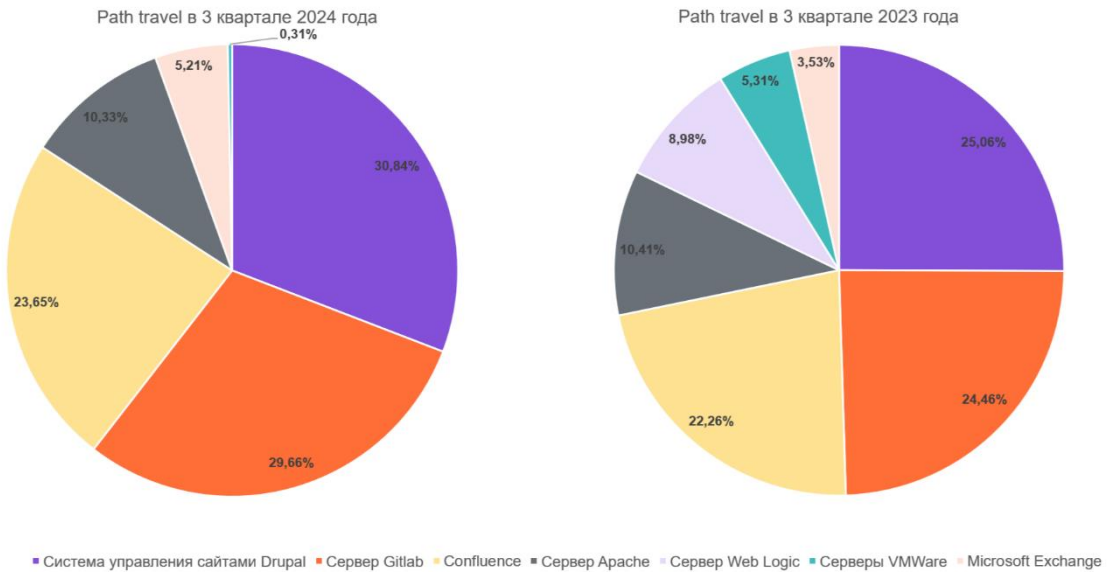
В целом за год ситуация с атаками типа CVE почти не изменилась. Помимо UPnP атакующие пытались проэкплуатировать уязвимости в Fortinet VPN, продуктах Citrix, платформе Kubernetes, почтовом сервере Microsoft Exchange и др. Это объясняется распространенностью указанных продуктов в корпоративных инфраструктурах.

Path Traversal и Upload

Среди целей атак типа Path Traversal — система Drupal, серверы Gitlab, Confluence, Apache и Microsoft Exchange. Это весьма распространенные продукты для различных целей, которые часто настроены небезопасно и доступны из сети. По этой причине они становятся частой жертвой различного вредоносного ПО. За год распределение между наиболее атакуемыми целями принципиально не поменялось. Единственное – исчезли атаки, направленные на Oracle Web Logic.



Если говорить об атаках типа Upload, то в этом году попытки загрузить полезную нагрузку фиксировались только на ловушках, имитирующих ресурсы, доступные по SSH и Telnet, а также серверы Vmware. Год назад мы фиксировали также попытки загрузить полезную нагрузку на ловушки, имитирующие прошивки роутеров, но в 2024 году они перестали привлекать злоумышленников.

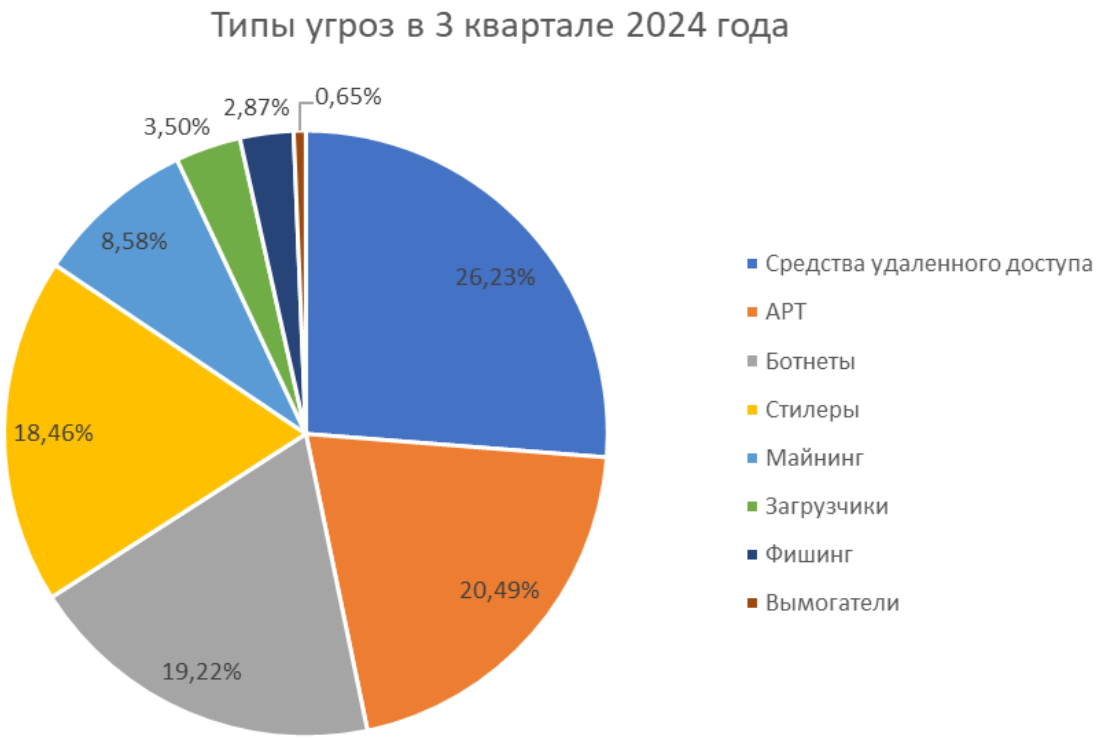


Статистика по заражению ВПО

Данные с сети сенсоров позволяют выделить индикаторы компрометации, относящиеся к разным типам угроз (вредоносное ПО конкретного типа). Эти данные позволяют экспертам Solar 4RAYS выявлять: ВПО для майнинга криптовалют, программы-вымогатели (шифровальщики), стиллеры, сложные киберугрозы (APT), загрузчики (ВПО для загрузки другого ВПО), ботнеты, фишинг и средства удаленного доступа (Remote Access Tools, RAT).

Распространенные угрозы и самые зараженные индустрии

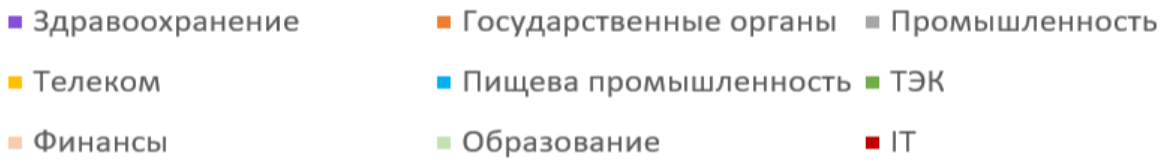
Всего в отчетном периоде эксперты Solar 4RAYS зафиксировали 1,6 млн резолвов вредоносного ПО из предприятий в более чем 60 субъектах РФ.

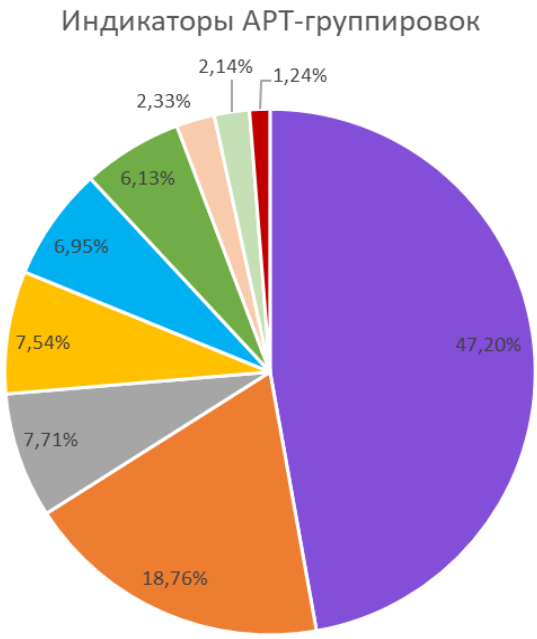


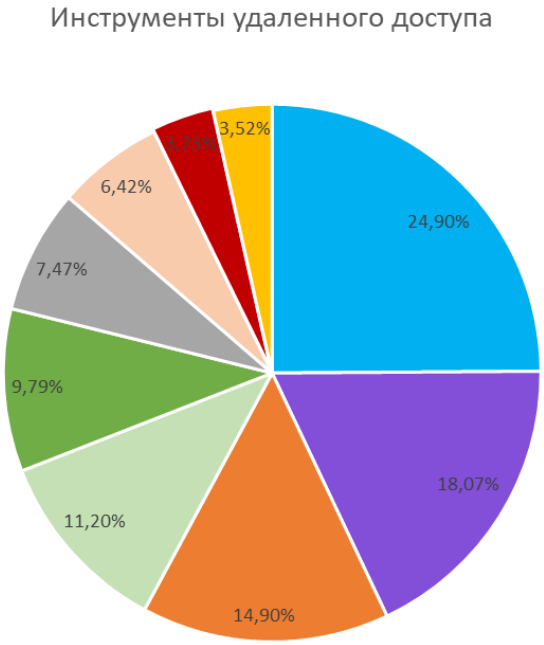
Чаще всего в 3 квартале эксперты фиксировали коммуникацию средств удаленного доступа (RAT), которые активно используют в целевых атаках. На втором месте – срабатывания на индикаторы известных APT-группировок.

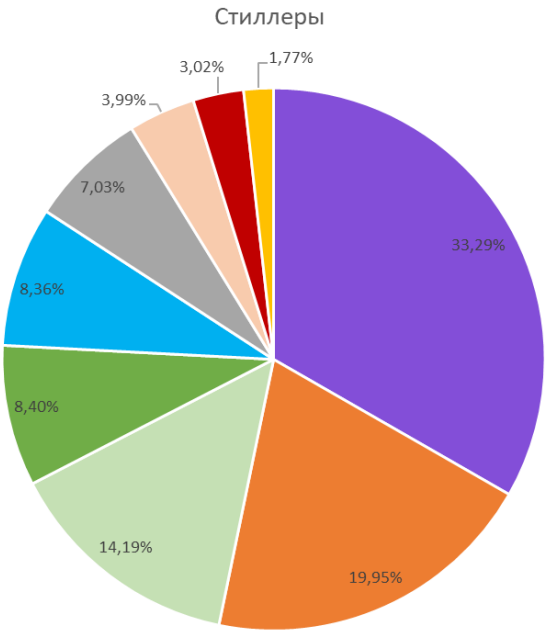
Четверть всех зафиксированных сработок пришлась на организации здравоохранения, еще 18% – на госорганы и 16% – на предприятия пищевой промышленности. Отчасти такой результат связан с повышенным интересом атакующих к конфиденциальной информации, которая часто содержится в инфраструктурах госорганов и медицинских организаций. Отчасти – не всегда высоким уровнем информационной безопасности в некоторых сетях из наиболее затронутых индустрий. Рассмотрим более детально, какие угрозы в какой индустрии встречаются чаще.

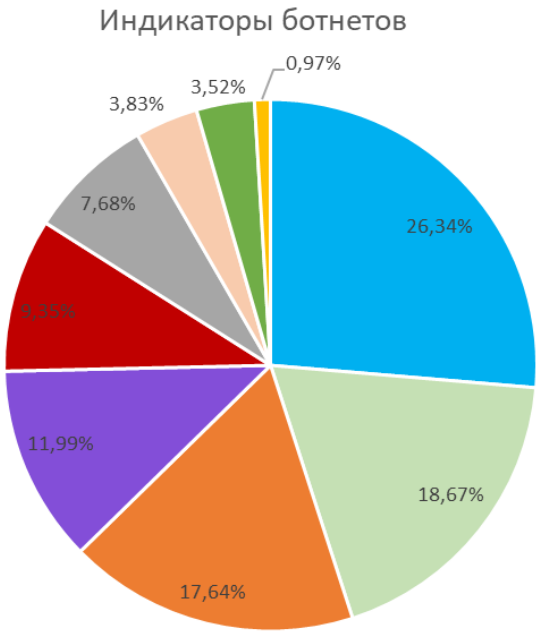
Типы угроз и индустрии



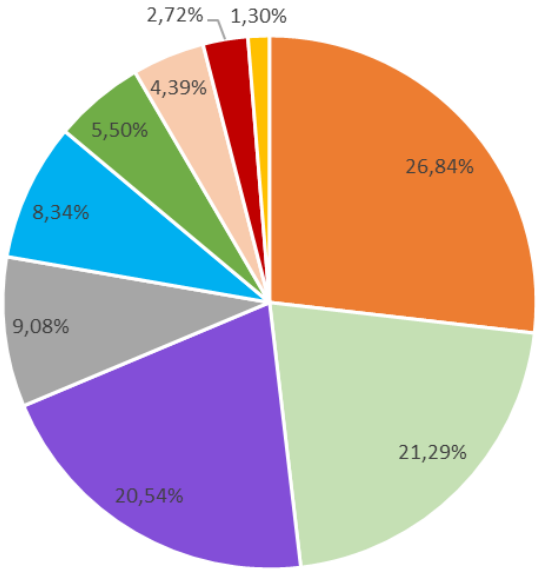




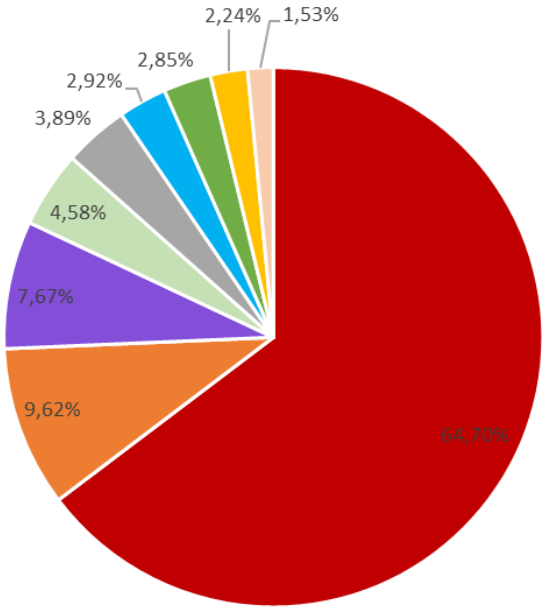




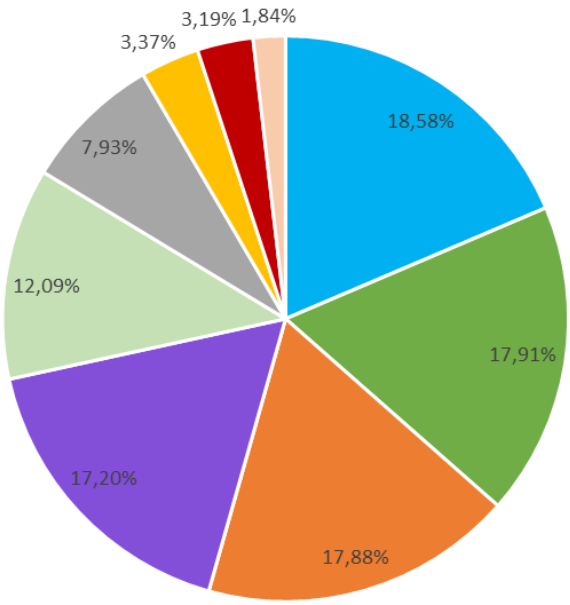
ВПО для майнинга криптовалют



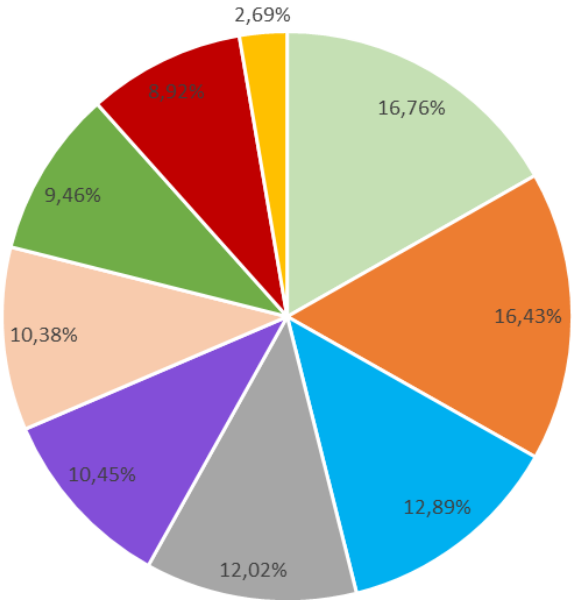
Программы-вымогатели



Загрузчики



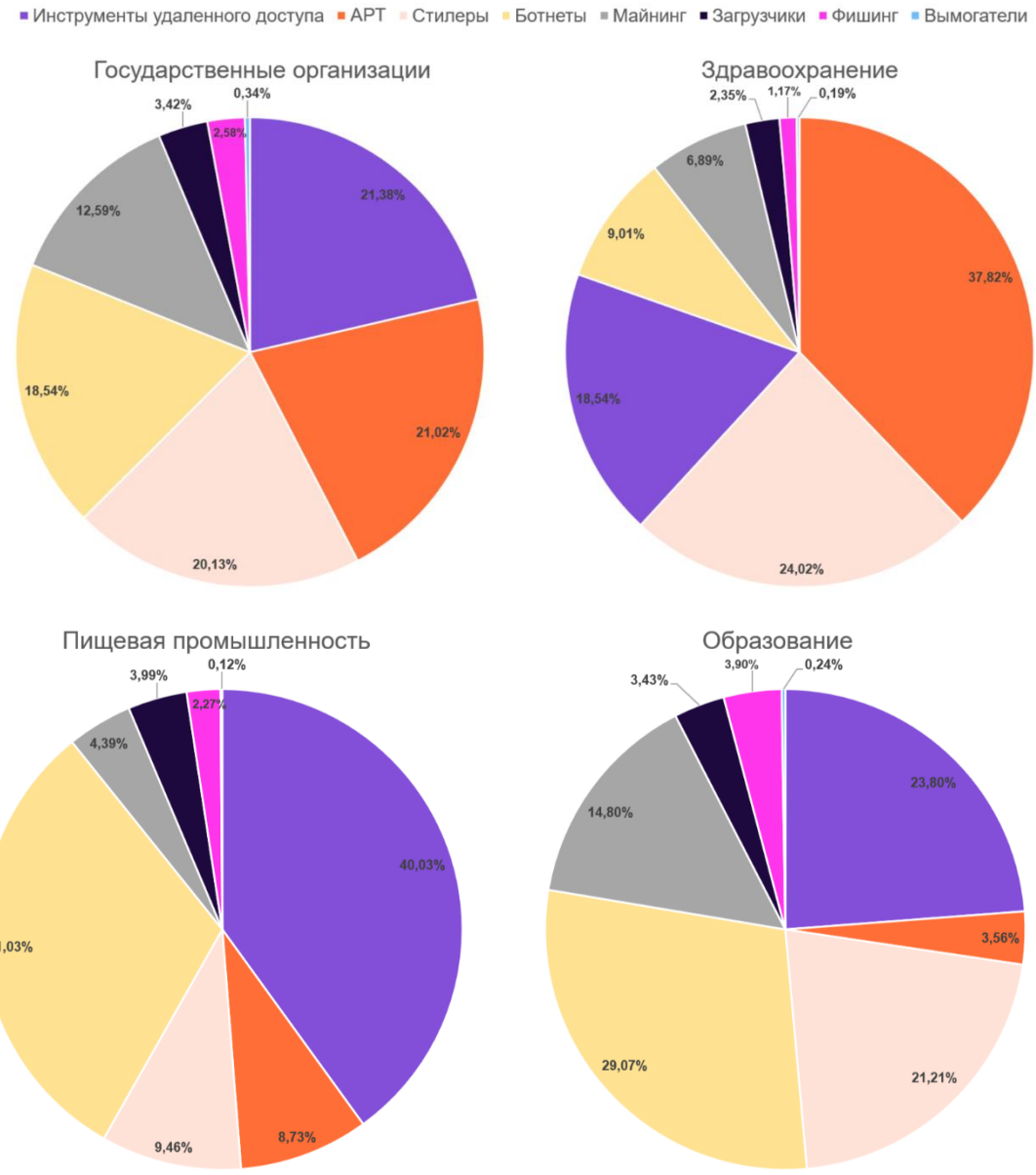
Фишинг



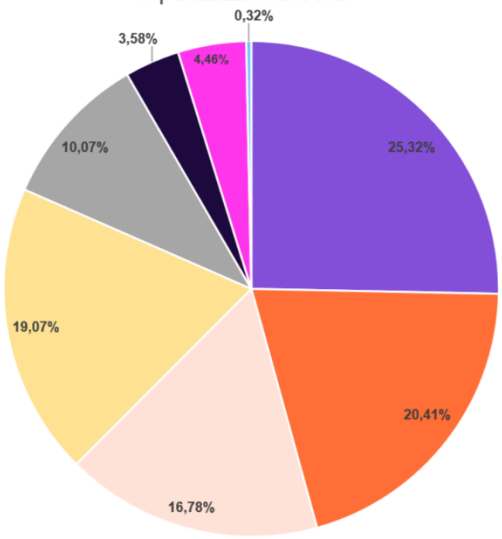
Индустрии и регионы

Показательной характеристикой ландшафта киберугроз является то, каким образом распределились угрозы в каждой конкретной индустрии, а также какие регионы подвержены угрозам в большей степени. Чтобы узнать ответ на этот вопрос, эксперты Solar 4RAYS проанализировали данные о количестве резолвов в разных регионах РФ в разрезе индустрий и количество таких событий в разрезе – по типу угрозы в конкретной индустрии. Забегая вперед, скажем, что общий итог анализа таков: инструменты удаленного доступа, APT-группировки, стиллеры и ботнеты – наиболее распространенные угрозы для организаций вне зависимости от отрасли. А вот распределение угроз от региона к региону меняется.

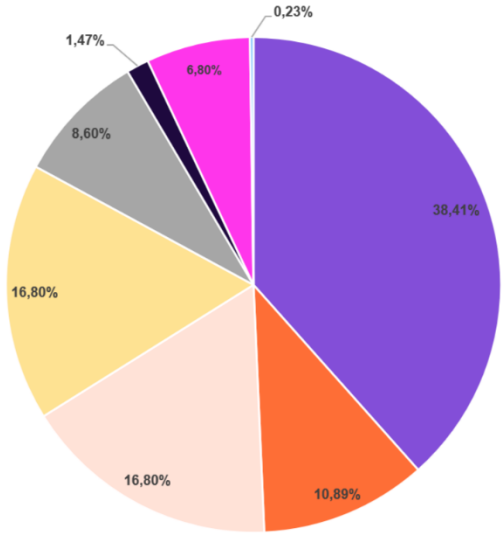
Распределение различных типов угроз по отраслям



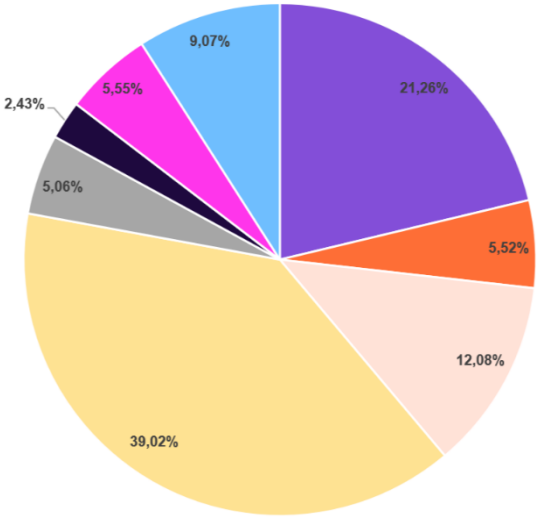
Промышленность



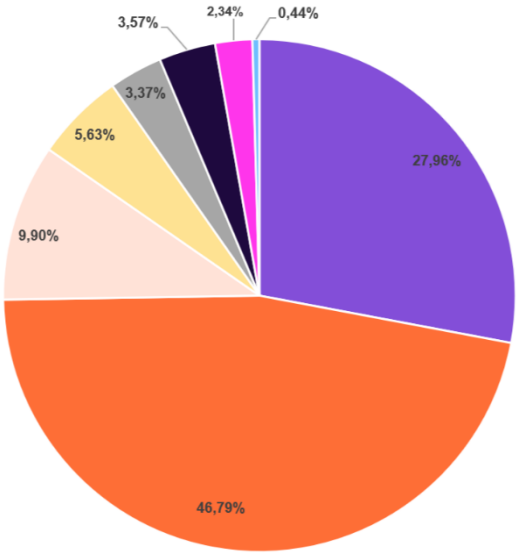
Финансовые организации



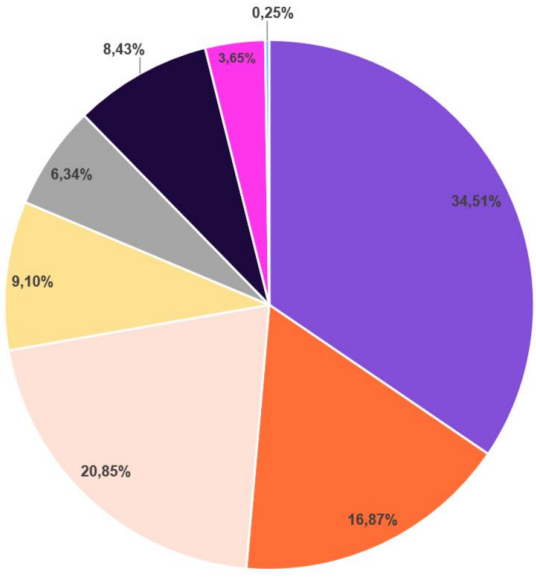
ИТ-компании



Телеком

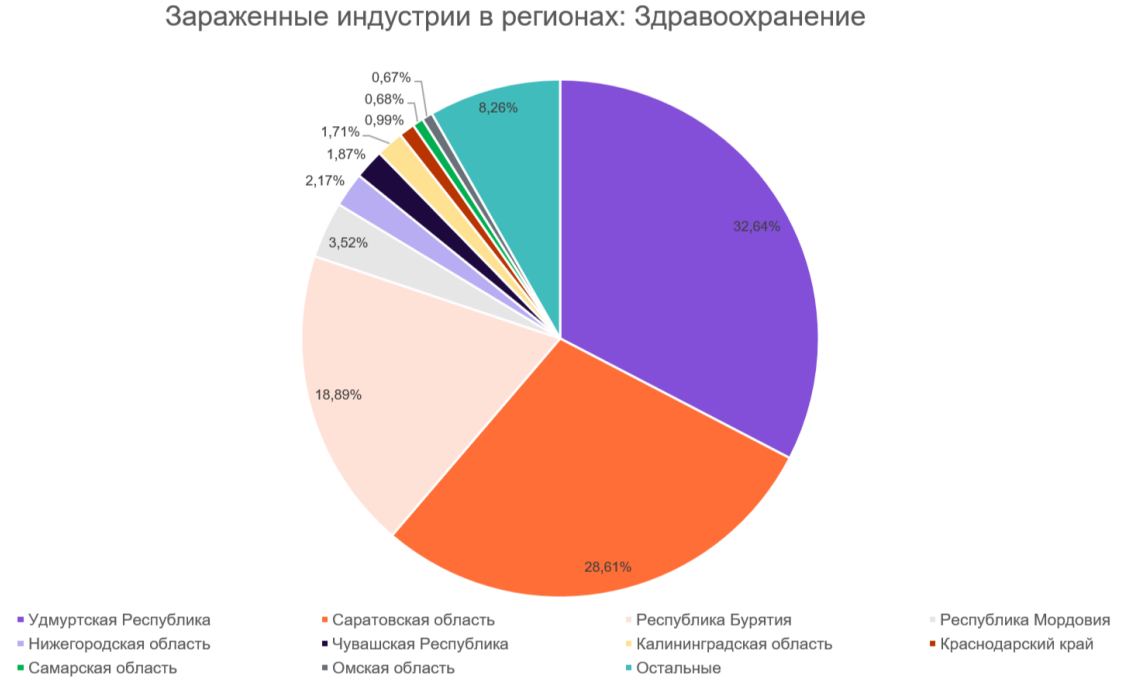


ТЭК



Распределение угроз по регионам и индустриям

Главными угрозами для государственных органов стали инструменты удаленного доступа, APT-группировки и стиллеры. В совокупности эти угрозы сгенерировали более 60% всех событий. А среди регионов в этой сфере в третьем квартале лидировали Республика Саха (50% событий), Удмуртская республика и Нижегородская область



В сфере здравоохранения хуже всего дела обстояли в учреждениях Удмуртской республики, Саратовской области и Республики Бурятия. На эти три региона пришлось около 80% всех событий, указывающих на возможное заражение в сфере.

Чаще всего события, указывающие на потенциальное заражение, фиксировались в сетях пищевых предприятий на территории Нижегородской области, Чувашской республики и Санкт-Петербурга.

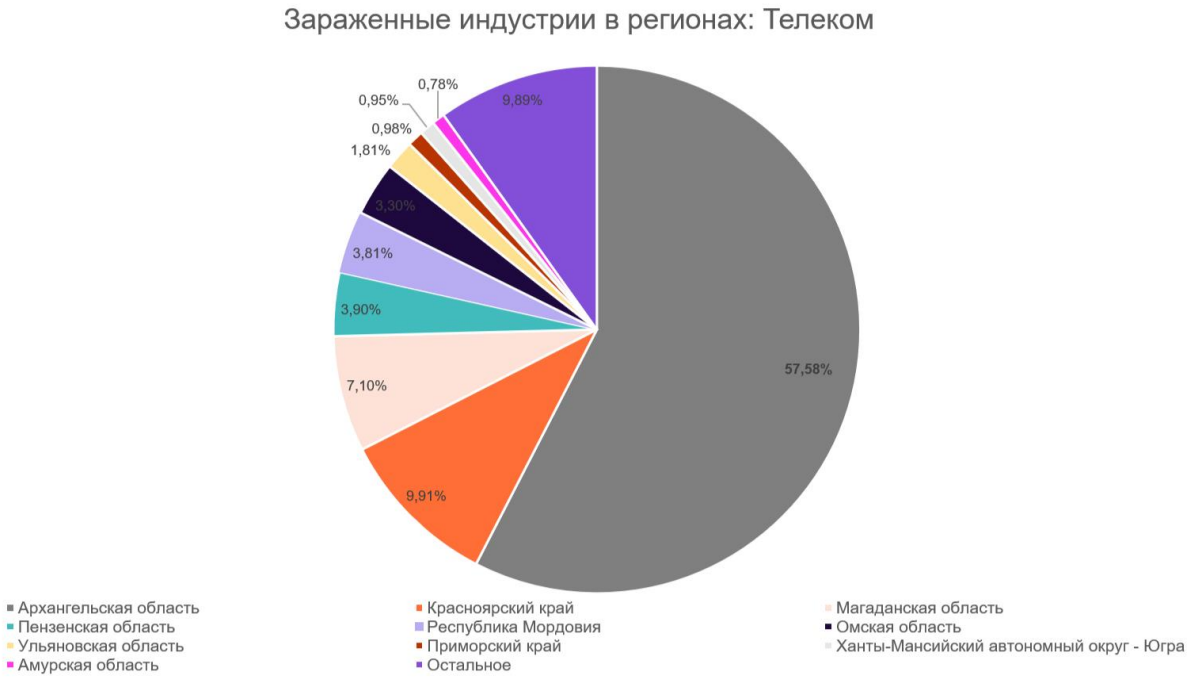
Чаще других признаки заражения демонстрировали ИТ-компании из Самарской, Пензенской и Саратовской областей.

В сфере топливно-энергетического комплекса активнее всего признаки заражения фиксировались в сетях предприятий Ханты-Мансийского автономного округа, Карачаево-Черкесской республики и Краснодарского края.

Образовательные учреждения Республики Саха, Волгоградской и Омская областей чаще учреждений из других регионов демонстрировали признаки заражения. Хотя львиная доля зафиксированных вредоносных событий пришлась на организации Республики Саха, а остальные участники “тройки лидеров” показали значительно менее масштабный процент.

Промышленные предприятия Чувашии, Нижегородской и Самарской областей демонстрировали признаки заражения чаще, чем предприятия других регионов, хотя в данном случае следует отметить, что доля признаков заражения в первой десятке регионов распределилась относительно равномерно – в диапазоне от 3 до 6%.

В финансовой сфере чаще всего признаки заражения демонстрировали организации из Удмуртской Республики, Ульяновской области, и Санкт-Петербурга.



“Лидеры” в телекоммуникационной сфере - Архангельская область, Краснодарский край и Магаданская область. Также следует отметить, что наряду со сферой здравоохранения, телеком – это индустрия, в которой признаки присутствия APT-группировок находятся на первом месте в списке угроз.

Регионы-лидеры

Ниже представлена сводная таблица регионов-лидеров по количеству индустрий с признаками заражения вредоносным ПО. В топ-3 входят: Нижегородская и Самарская области, а также Удмуртская Республика. В третьем квартале организации из большинства исследуемых индустрий в этих регионах продемонстрировали значительные признаки заражения.

Цветом выделены случаи, когда в организации из региона оказывались в первой тройке в “индустриальных” срезах (цифра в скобках - место региона в конкретном срезе по индустрии). Нижегородская область и Удмуртская Республика оказались двумя регионами с наибольшим числом таких результатов.

Другими словами, организации почти всех индустрий в данных регионах содержат признаки заражения ВПО и часто - в значительных количествах.

	Кол-во индустрий	ИТ	Госорганы	ТЭК	Образование	Промышленность	Здравоохранение	Финансы	Телеком	Пищевая промышленность
Нижегородская область	8	2% (9)	2,43 % (3)	5,73% (4)	1,82% (5)	11,5% (2)	2,17% (5)	4,15 % (7)		20,25% (1)
Самарская область	7	26,05 % (1)	2,12 % (5)	2,29% (4)	4,17% (10)	7,48% (3)	0,98% (9)			4,22% (7)
Удмуртская республика	7		11,35 % (2)	5,17% (5)	1,72% (6)	4,33% (9)	32,64% (1)	18,39% (1)		4,98% (6)
Кировская область	5	3,61% (6)	1,72 % (7)			6,08% (4)		2,74 % (9)		3,12% (10)
Омская область	4	4,48% (4)			2,76% (3)		0,67%(10)		3,3 % (6)	
Республика Мордовия	4	3,13% (8)					3,52% (4)	5,93 % (4)	3,81 % (5)	
г. Санкт-Петербург	4				2,22% (4)	3,86% (10)		3,04 % (3)		6,26% (3)
Пензенская область	3	21,92 % (2)		4,4 % (8)					3,9 % (4)	

Саратовская область	3	10,06 % (3)				5,63% (5)	28,61% (2)			
Красноярский край	3	2,71% (10)	1,74 % (6)						9,91 % (2)	
Ульяновская область	3		2,29 % (4)					10,66% (2)	1,81 % (7)	
Чувашия	3					11,65% (1)	1,87% (6)			9% (2)

Заключение и рекомендации

Угрозы, зафиксированные на ловушках, позволяют сделать выводы о том, на что следует обращать внимание сотрудникам ИБ-команд при обеспечении безопасности вверенных им инфраструктур. Рост доли атак типа Path Traversal может указывать на то, что злоумышленники активно ищут доступные извне элементы ИТ-инфраструктуры, а значит, специалистам стоит внимательное заниматься их настройкой.

Среди попыток эксплуатации уязвимостей лидируют UPnP, продукты Fortinet и Citrix, что тоже указывает на то, какое именно ПО нужно обращать пристальное внимание, когда речь заходит о патч-менеджменте и других мерах по предотвращению эксплуатации уязвимостей.

Картина заражений в регионах и индустриях, полученная с помощью сети сенсоров, также позволяет сделать несколько выводов. Например, среди наиболее распространенных угроз в организациях вне зависимости от индустрии – популярное ВПО (за исключением индикаторов действий APT-группировок), которое обычно успешно детектируется стандартными средствами защиты информационных систем.

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

- регулярно сканировать свой внешний периметр на предмет изменения опубликованных сервисов и наличия в них уязвимостей;
- 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;
- 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;
- обеспечить 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 её 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;