4RAYS by SOLAR

ЛАНДШАФТ ВРЕДОНОСНЫХ АТАК: АНАЛИТИКА С СЕНСОРОВ И ХАНИПОТОВ

Отчёт по итогам
4 квартала 2024 г.

Введение и методология

Ежедневно сервисы и продукты “Солара” распознают и блокируют десятки тысяч кибератак на сотни организаций. Информация об угрозах, с которыми сталкиваются наши клиенты, поступает как от организаций-партнёров, так и из 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, разбросанных 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, какие методы атак и как часто 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 (удалённого доступа, SMB и т.д.), автоматизированные системы управления технологическим процессом (АСУ ТП), 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 4 квартале 2024 года и их сравнение с 3 кварталом 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 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. Например: 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.

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

Данные с сенсоров PDNS

Вторая часть отчета описывает ландшафт угроз на территории России. Данные для неё 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, которых хранит информацию о том, какое доменное имя какому IP-адресу соответствует.

Информация о поптыках соединений (резолвах) анализируется с помощью технологии passive DNS. Она сравнивает 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, 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:

- признаки деятельности известных профессиональных хакерских группировок (APT)
- признаки работы инструментов удаленного администрирования (Remote Access Tools, RAT)
- признаки заражения вредоносами-стилерами (ВПО, похищающее конфиденциальную информацию)
- признаки присутствия ботов одного из известных ботнетов
- признаки заражения вымогателями
- признаки заражения ВПО для майнинга криптовалют
- признаки заражения загрузчикам – ВПО, способное устанавливать на атакованный компьютер дополнительные вредоносы.
- признаки перехода на фишинговые страницы.

Признаки заражения выявляются в российских организациях, классифицированных по двум признакам: географическое расположение и принадлежность к той или иной сфере экономики. Всего мы выделяем восемь сфер:

- Государственный сектор
- Здравоохранение
- Образование

- Промышленность
- Пищевая промышленность
- Финансовая индустрия
- Телекоммуникационная индустрия
- ИТ-организации

Отслеживание изменений в ландшафте угроз на основе данных PDNS позволяет получить примерное представление о том, какие угрозы представляют наибольшую опасность для организаций из каких сфер и регионов.

Основные результаты

Ханипоты:

- Количество атак на ловушки Solar 4RAYS в четвёртом квартале 2024 года выросло до 233,8 тыс., что более чем на 85% больше, чем в третьем квартале.

- В основном рост случился из-за значительного увеличения зафиксированных попыток взлома учетных записей методом “грубой силы” (bruteforce): на 135% больше, чем кварталом ранее.

- США, Китай, Индия и Россия в четвертом квартале 2024 года стали главными источникам вредоносной активности, зафиксированной ловушками. В совокупности на эти страны пришлось 65% атак. По сравнению с третьим кварталом более других возрос “вклад” в общее число атак со стороны США (+ 17 процентных пунктов) и России (+7,5 п.п.).

- Большая часть атак типа bruteforce была нацелена на включение атакованных компьютеров в ботнет Mozi, а также на протоколы SSH и Telnet.

- Как и кварталом ранее, большая часть автоматизированных попыток эксплуатации какой-либо уязвимости в четвертом квартале пришлось на атаки UPnProxy потиво протокола UPnP. Однако их доля сократилась с 86% ддо 58%. Техника UPnProxy позволяет автоматически создавать правила переадресации портов на устройстве. При этом за квартал значительно выросла доля атак на продукты Fortinet - с 7% до 30%.

Сенсоры PDNS:

- Общее количество срабатываний, свидетельствующих о возможном заражении вредоносным ПО, в четвертом квартале 2024 года упало на 35,2% – с 1,6 млн до 1,2 млн.

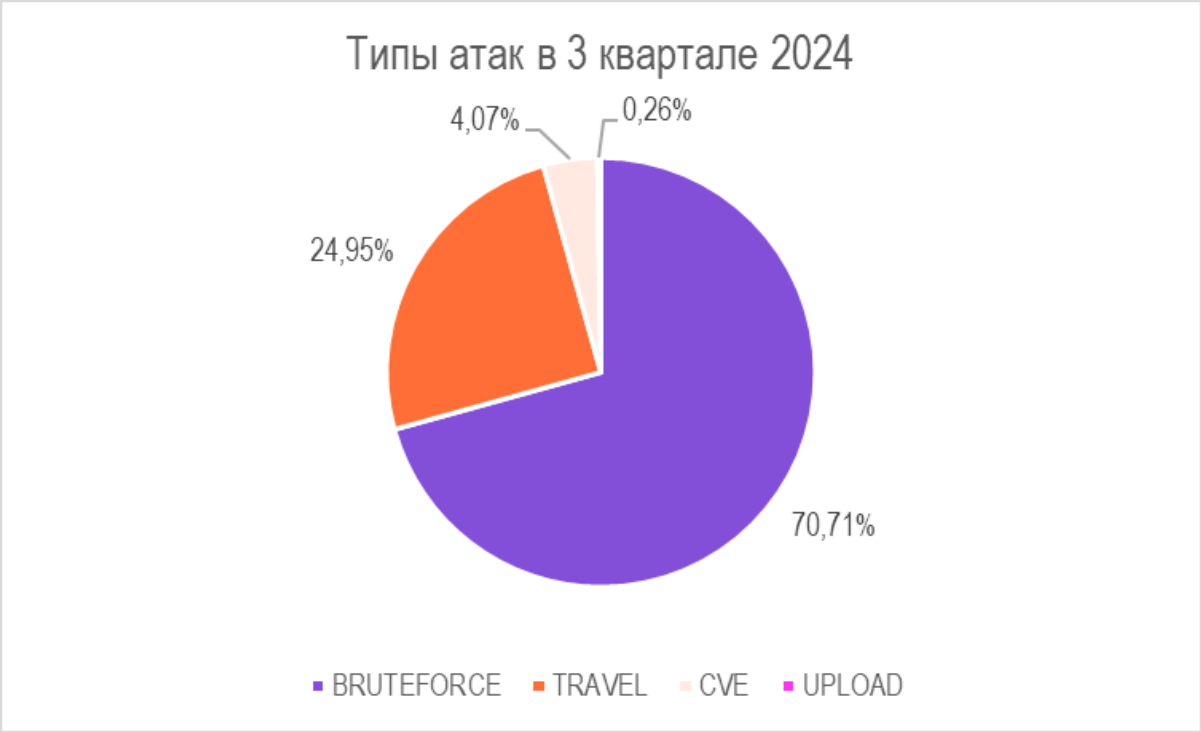
- За квартал сократилось и число атакованных организаций – на 15,86% (с 34 тыс. до 29 тыс). Таким образом, в среднем на одну компанию в четвертом квартале 2024 года пришлось 40,71 срабатывания, в то время как кварталом ранее показатель равнялся 47,5 срабатываниям.

- Средства удаленного администрирования (RAT), APT, ботнеты и стиллеры – угрозы, признаки заражения которыми, встречались в организациях чаще всего в 4 квартале.

- Телекоммуникации, здравоохранение, ТЭК, IT и пищевая промышленность лидировали в четвертом квартале по среднему количеству срабатываний на одну организацию.

Ловушки-ханипоты: общая статистика и география атак

Количество атак, зафиксированных ловушками в 4 квартале, составило 233,8 тыс., что на 85,5% больше, чем кварталом ранее. Наибольший “вклад” в этот рост внесли атаки типа Bruteforce (+134,9%). В то же время количество атак Path Traversal и CVE значительно упало – на 72,7% и 34,9% соответственно. В процентном соотношении доли атак распределились следующим образом



Тип атаки	**Количество атак в 3 кв. 2024 г.**	**Количество атак в 4 кв. 2024 г.**	Изменение
BRUTEFORCE	89126,60317	209427,3676	+134,98%
TRAVEL	31449,51111	18210,89362	- 72,70%
CVE	5132,016667	3804,555556	- 34,89%
UPLOAD	333,3636364	2412,625	+623,72%

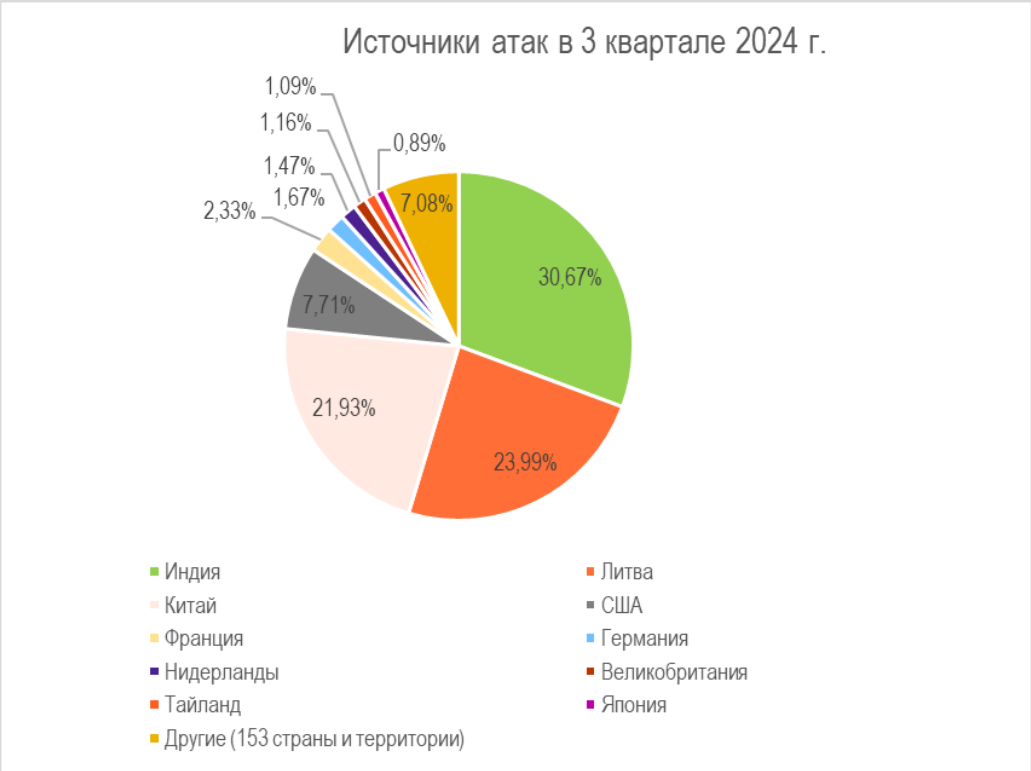
География целей атак

В четвертом квартале ловушки, расположенные на территории России, вышли на первое место по доле атак – на них зафиксировано 22,61% всех попыток (против 28,27% в третьем квартале). США, которые возглавляли ТОП наиболее атакуемых стран в 3 квартале, переместился на второе место (в доля упала с 36,82% до 17,72%).

Доля ловушек в иных странах также возросла. Если в 3 квартале на них приходилось 34,9%, то в 4-м – всего 59,67% атак. Значительно выросла доля атак на ловушки на территории Германии - с 0,42% - до 14,95%.

Откуда шли атаки

США, Китай, Индия и Россия в 4 квартале 2024 года стали главными источникам вредоносной активности, зафиксированной ловушками. В совокупности на эти страны пришлось 65,13% атак.



В третьем квартале Индия была на первом месте с 30,67% атак, а “компанию” ей (в порядке убывания долей) составляли Литва (23,99%), Китай (21,93%) и США (7,71%).

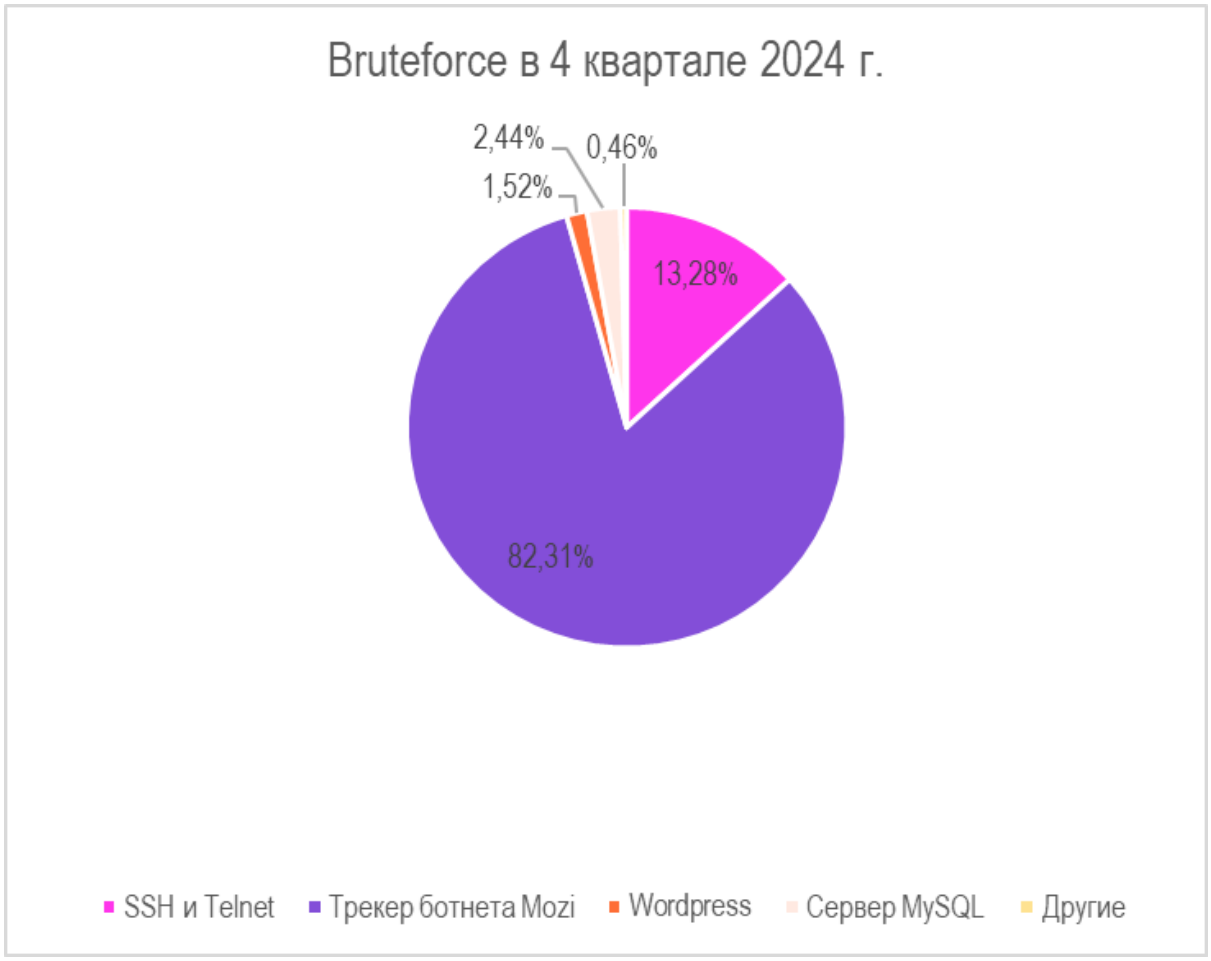
Страна	Доля атак в 3 квартале	Доля атак в 4 квартале	Изменения
США	7,71%	25,03%	+17,32 п.п.
Китай	21,93%	19,55%	-2,38 п.п.
Индия	30,67%	12,97%	-17,7 п.п.
Россия	0,03%	7,58%	+7,55 п.п.
Гонконг	0,04%	4,75%	+4,71 п.п.
Германия	1,67%	4,13%	+2,46 п.п.
Великобритания	1,16%	2,42%	+1,26 п.п.
Франция	2,33%	0,24%	-2,09 п.п.
Бразилия	0,28%	2,13%	+1,85 п.п.
Вьетнам	0,18%	1,76%	+1,58 п.п.
Литва	23,99%	0	-23,99 п.п.
Нидерланды	1,47%	1,07%	-0,4 п.п.
Тайланд	1,09%	0,09%	-1 п.п.
Япония	0,89%	1,21%	+0,32 п.п.
Другие	7,08%	19,44%	+12,36 п.п.

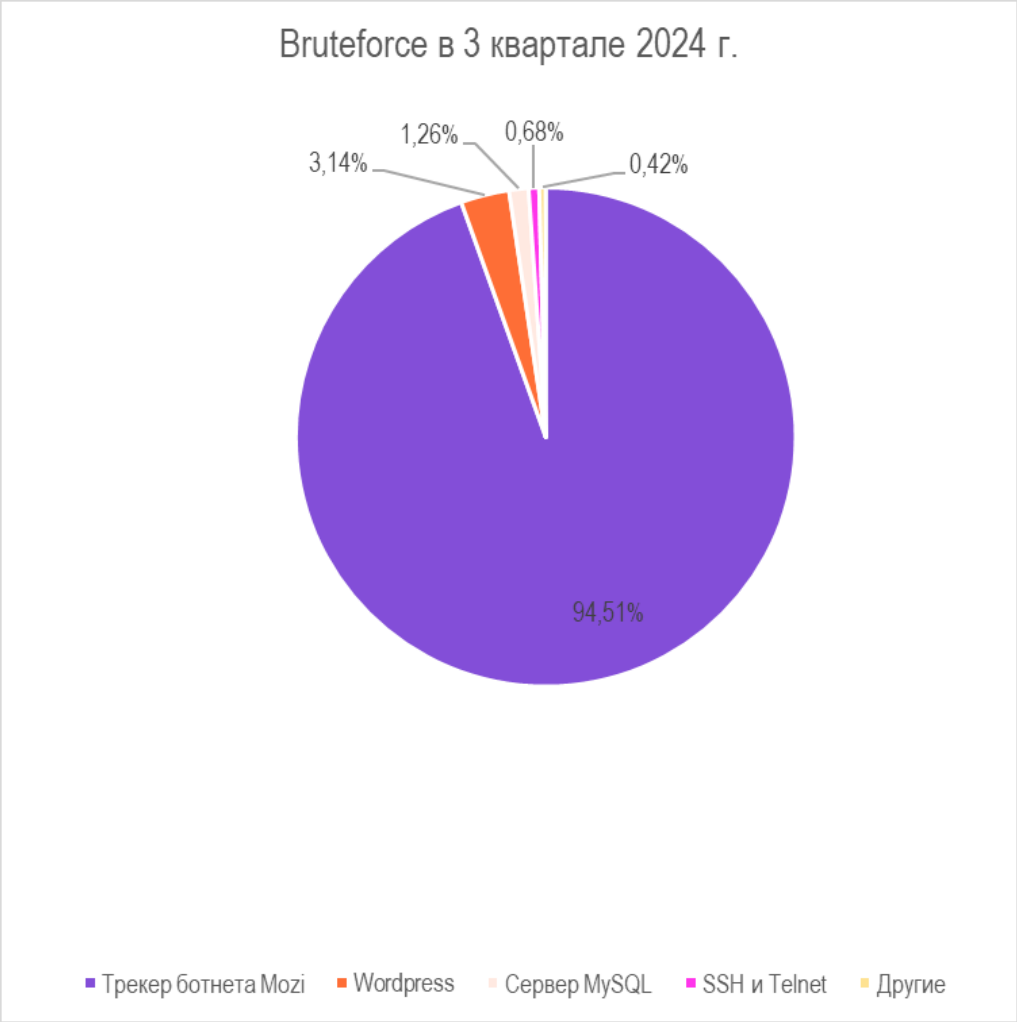
У изменения в географии целей и источников нет конкретной причины. Это результат влияния нескольких факторов, среди которых изменение географического ландшафта заражённых ПО для автоматизации атак, появление в открытом доступе экплойтов для уязвимостей в ПО, популярном в тех или иных странах, и т.д.

Типы атак

Bruteforce

Хотя в течение квартала мы видели атаки на 12 разновидностей ПО, львиная их доля в 4 квартале пришлась пришлась на случаи попыток заражения ПО, связанного с ботнетом Mozi, а также на атаки против протоколов SSH и Telnet. В третьем квартале на ботнет Mozi и вовсе пришлось более 94% зафиксированных попыток подбора паролей. Именно рост числа атак на SSH и Telnet, которые в случае успеха предоставляют злоумышленникам удалённый доступ в атакованную инфраструктуру, стал основным фактором, повлиявшим на рост доли Bruteforce-атак на фоне других типов.

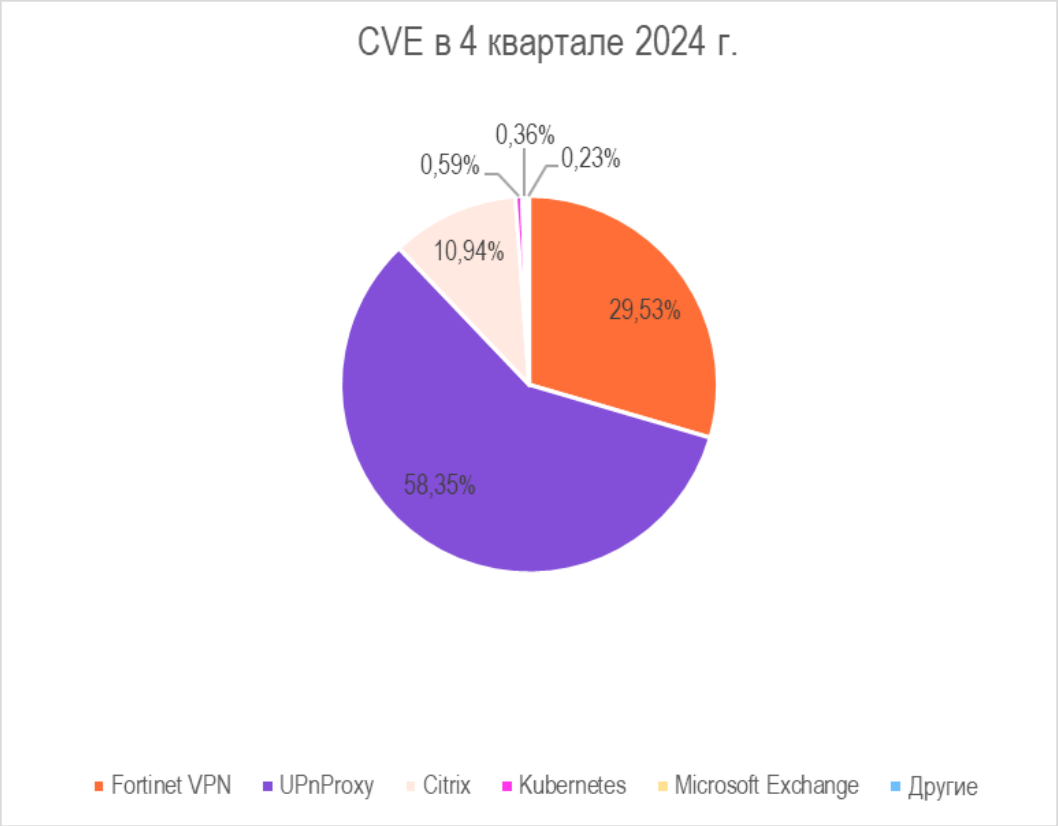

Bruteforce в 4 квартале 2024 г.
2,44%
0,46%
1,52%
13,28%
82,31%
SSH и Telnet
Трекер ботнета Mozi
Wordpress
Сервер MySQL
Другие

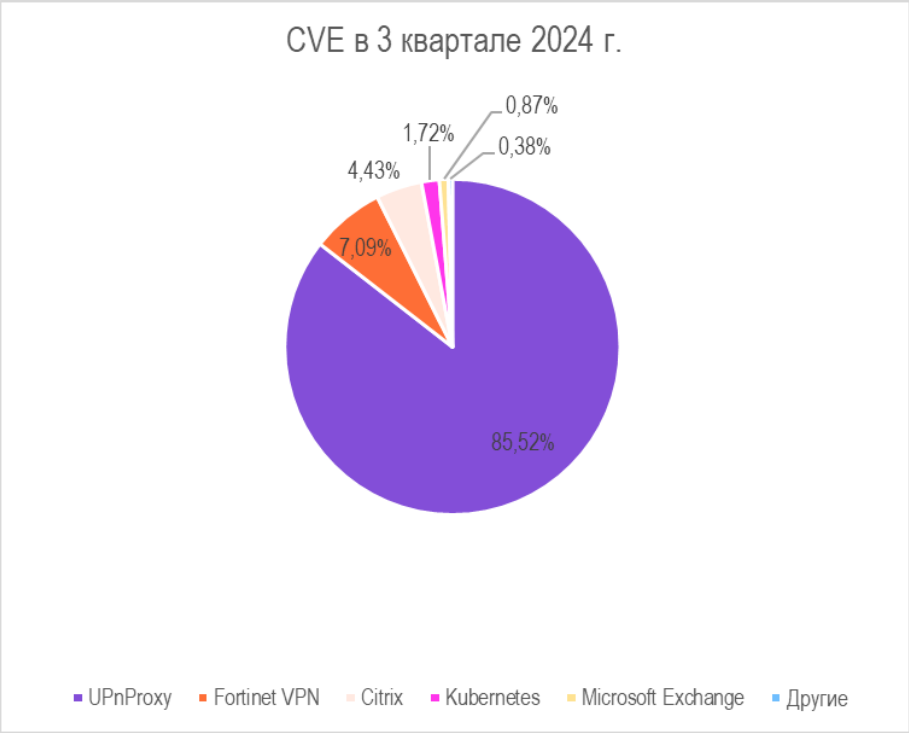


CVE

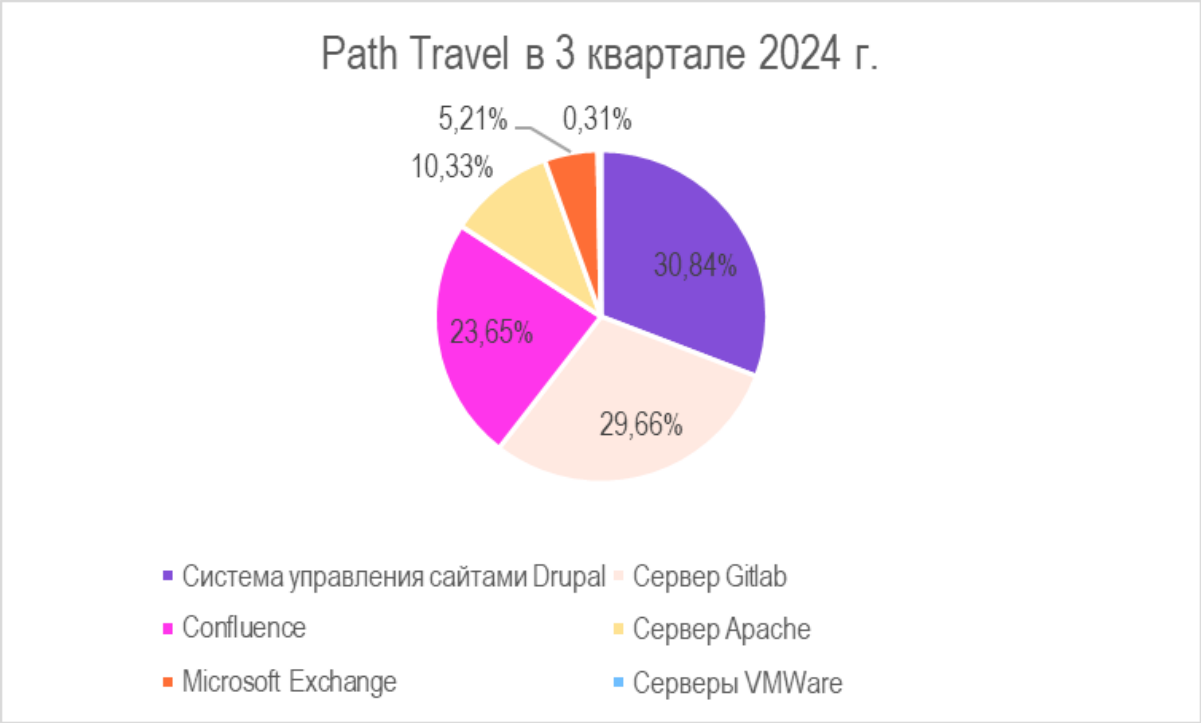
Большая часть автоматизированных попыток эксплуатации какой-либо уязвимости в 4 квартале пришлась на атаки UPnProxy против протокола UPnP - доля составила 58,35%. Атака позволяет автоматически создавать правила переадресации портов на устройстве. Однако доля таких атак значительно сократилась (в 3 квартале на них приходилось 85,52%).

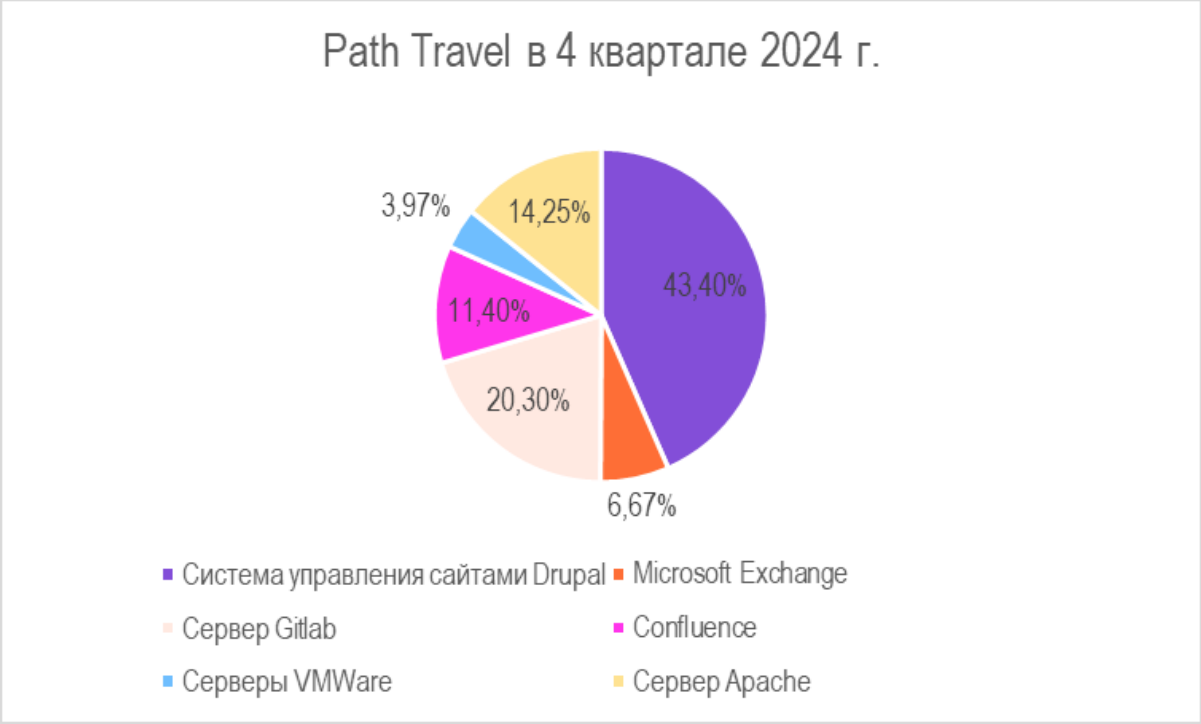
В то же время за квартал увеличилась доля атак на продукты Fortinet (29,53% в 4 квартале против 7,09% в 3-м). В абсолютном выражении атаки на Fortinet тоже выросли – более, чем в 3 раза (с 15 тыс до 49 тыс. атак). Очевидно, это связано с появлением двух уязвимостей нулевого дня в FortiClient VPN, о которых стало известно в ноябре 2024 года. Злоумышленники часто пытаются воспользоваться периодом, когда об уязвимости уже известно, но большинство компаний не успели пока установить нужные обновления.





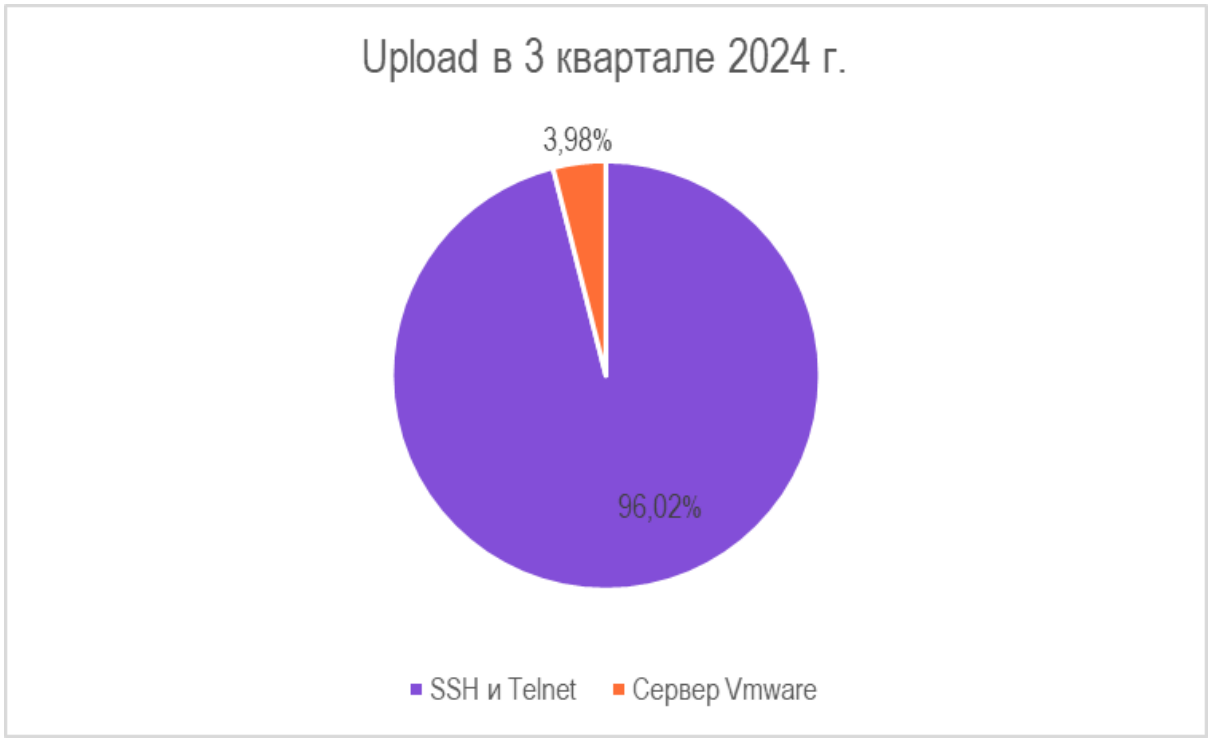
Path Traversal и Upload

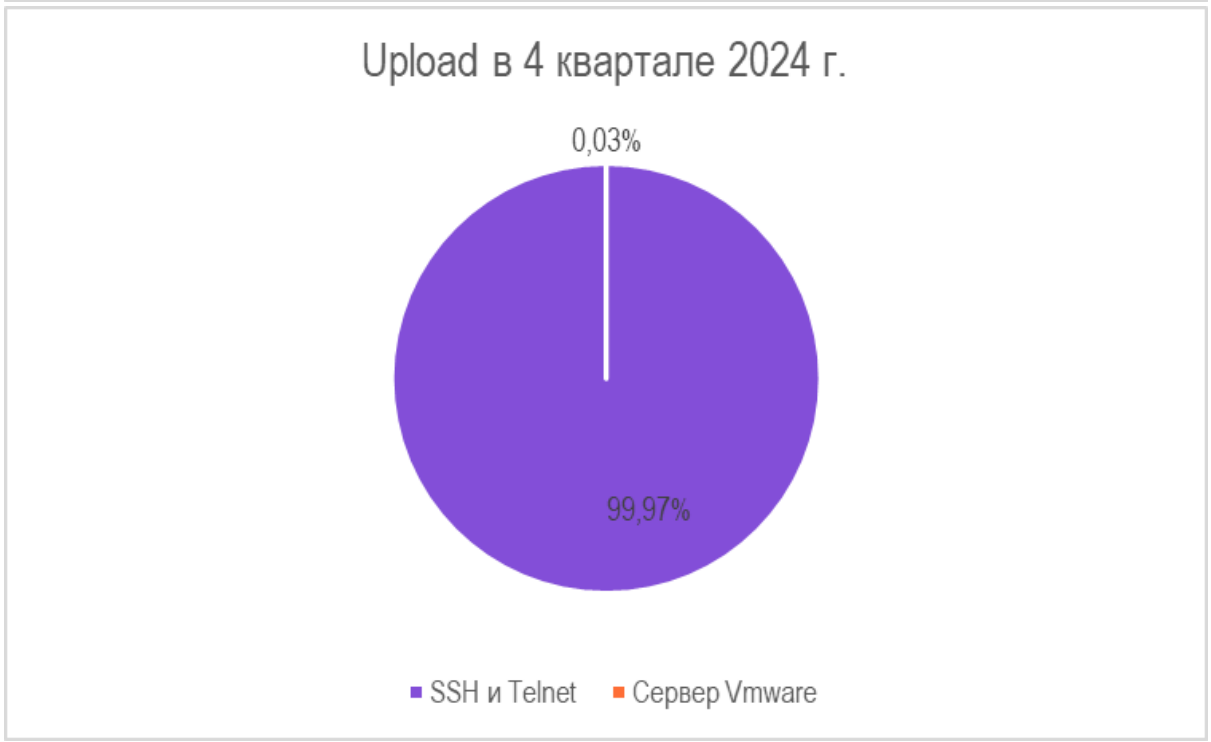




Распределение атак типа Path Traversal за квартал не претерпело значительных изменений: чаще всего злоумышленники применяют этот тип атак против системы управления сайтами Drupal, серверов GitLab и Confluence. В 4 квартале доля атак на Drupal заметно выросла, а на GitLab и Confluence – наоборот сократилась. Также атакам стали чаще подвергаться серверы Apache.

В случае с атаками типа Upload главной целью атакующих два квартала подряд оставались протоколы SSH и Telnet.


Upload в 3 квартале 2024 г.
3,98%
96,02%
SSH и Telnet
Сервер Vmware


Upload в 4 квартале 2024 г.
0,03%
99,97%
SSH и Telnet
Сервер Vmware

Сенсоры PDNS: общая статистика

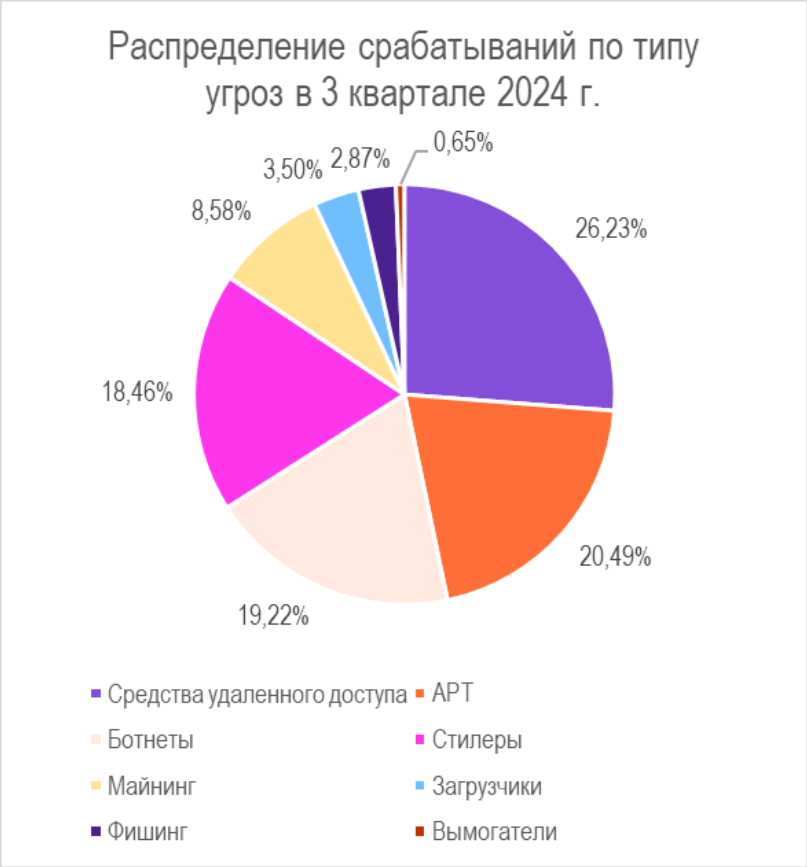
Общее количество срабатываний, свидетельствующих о возможном заражении вредоносным ПО, в 4-м квартале 2024 года сократилось на 35,2%: с 1,6 млн до 1,2 млн. Также на 15,8% сократилось число атакованных организаций:с 34 тыс до 29 тыс. Таким образом, в среднем на одну компанию в 4-м квартале 2024 года приходилось 40,71 срабатывания, в то время как кварталом ранее показатель равнялся 47,5.

Показатель	3 квартал	4 квартал	Изменения
Общее число срабатываний	1636207	1210245	- 35,20%
Число организаций	34442	29726	- 15,86%
Среднее количество атак на организацию	47,5	40,71	- 16,68%

Такая динамика может быть следствием нескольких причин. Во-первых, в конце года бизнес-активность, как правило, идёт на спад, а вслед за ней и активность злоумышленников. Во-вторых, на динамику срабатываний могут влиять меры безопасности, принимаемые в организациях – например, устранение заражения вредоносным ПО.

Типы угроз и индустрии

Типы угроз: общие сведения



Наибольшую угрозу организациям, как и в предыдущем квартале, составили средства удаленного доступа (RAT), индикаторы присутствия APT-группировок, вредоносный код ботнетов и стиллеры – программы, похищающие конфиденциальные сведения. В четвертом квартале доля APT, ботнетов и стилеров незначительно выросла, а доля RAT – наоборот сократилась.

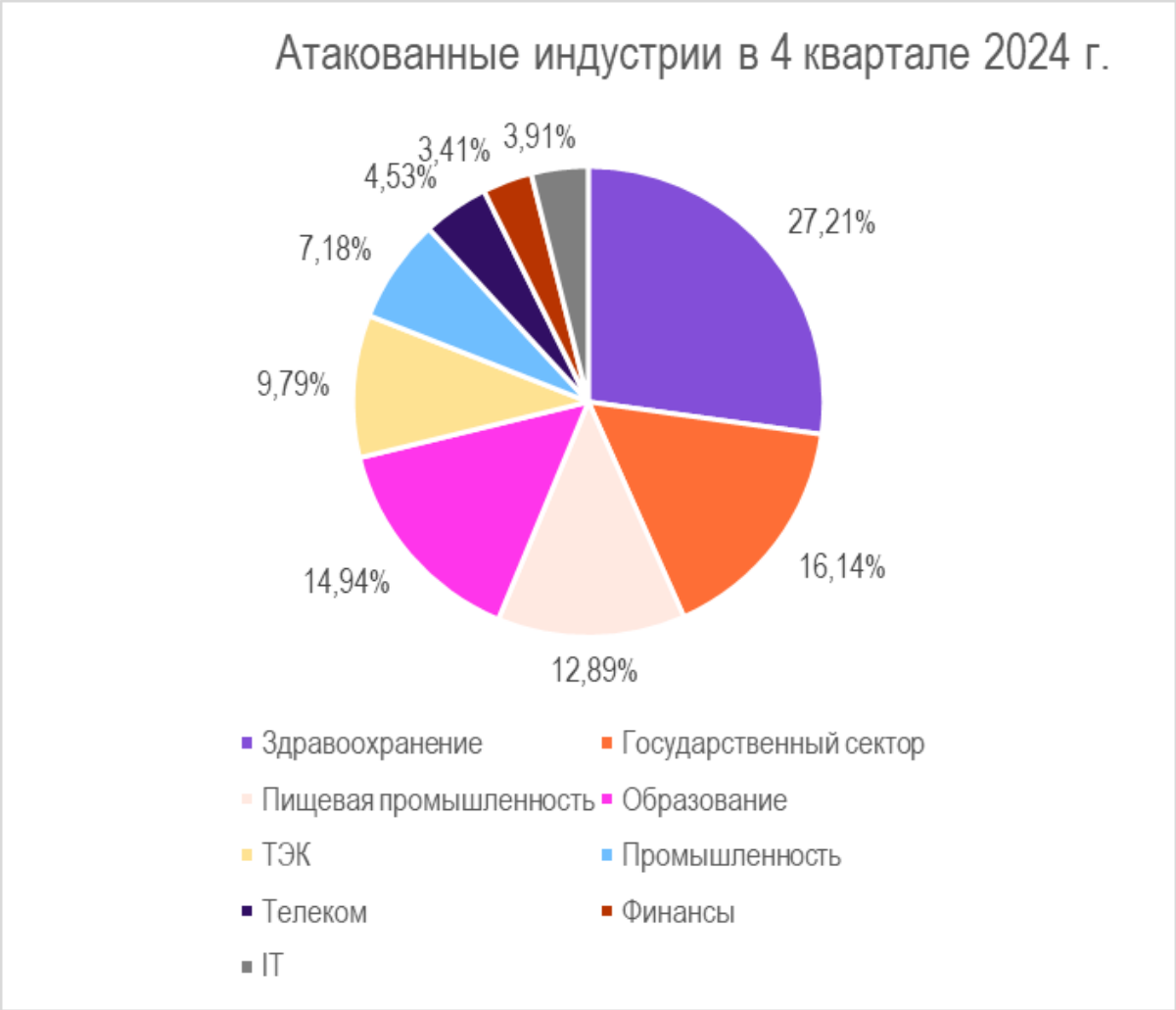
В абсолютном выражении количество срабатываний на все типы угроз за квартал снизилось.

Тип угрозы	3 квартал	4 квартал	Изменение
Средства удаленного доступа	429241	295443	- 45,29%
APT	335291	283265	- 18,37%
Ботнеты	314484	250114	- 25,74%
Стилеры	301992	249068	- 21,25%
Майнинг	140398	70090	- 100,31%
Загрузчики	57271	30749	- 86,25%
Фишинг	46965	24579	- 91,08%

Вымогатели	10565	6937	- 52,3%

Атакованные индустрии

Большинство вредоносных срабатываний в 3-м квартале фиксировалась в сетях организаций здравоохранения, государственного сектора, пищевой промышленности и образования. В 4-м квартале ситуация не изменилась, хотя доли здравоохранения, образования, а также ТЭК незначительно увеличились.



При этом число атакованных организаций менялось, и это позволяет понять частоту, с которой в среднем организации демонстрировали признаки заражения ВПО. Среднее количество срабатываний в пересчете на одну организацию в индустрии выглядит так.

Индустрия	Среднее за 3 квартал	Среднее за 4 квартал	Изменение
Здравоохранение	127,77	80,24	- 37,2%
Государственные органы	56,018	27,27	-51,32%
Пищевая промышленность	79,01	41,97	-46,88%
Образование	19,94	16,45	-17,5%

ТЭК	54,35	59,54	-9,55%
Промышленность	69,01	34,04	-50,67%
Телеком	72,76	81,32	+11,76%
Финансы	39,97	19,18	-52,01%
IT	79,68	42,91	-46,15%

В 3-м квартале чаще всего признаки заражения фиксировались в организациях здравоохранения, IT, телекоммуникаций, пищевой и прочей промышленности, а также ТЭК. В 4-м квартале “самыми атакуемыми” стали: телекоммуникации, здравоохранение, ТЭК, IT и пищевая промышленность.

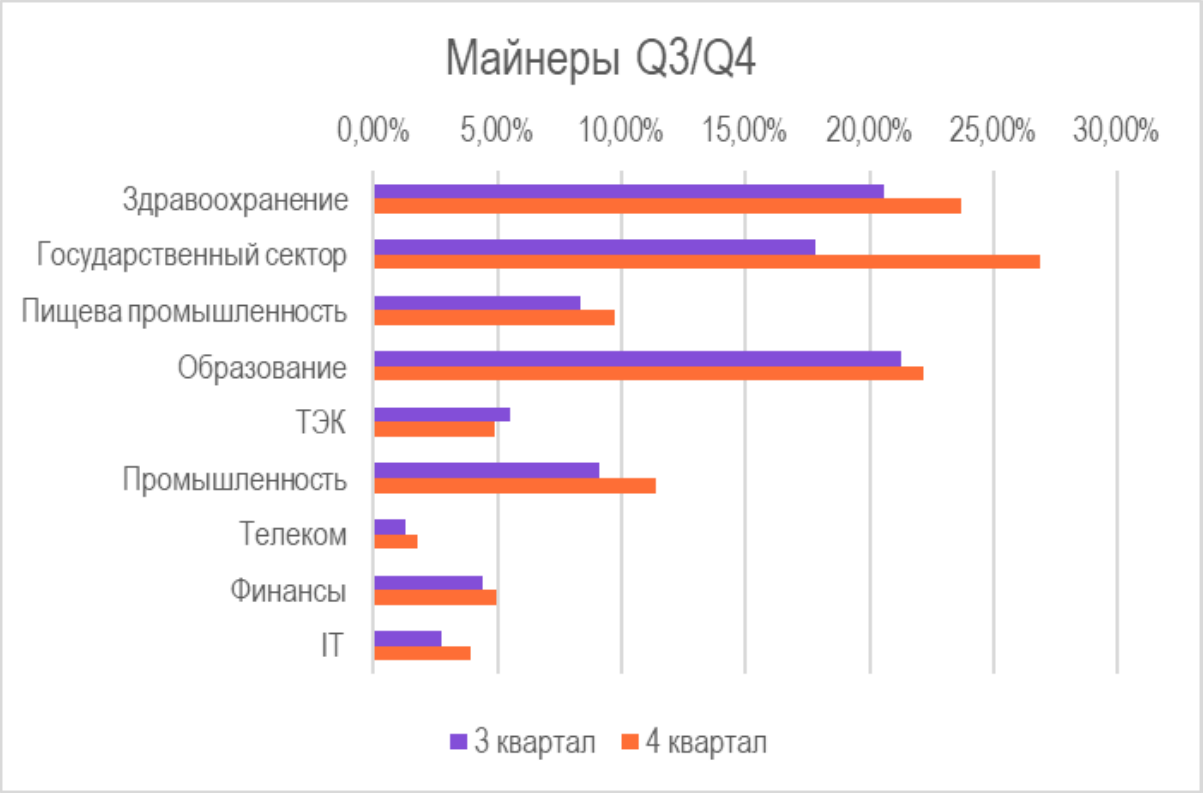
Типы угроз: детали

Далее рассмотрим в деталях, какие угрозы чаще встречаются в предприятиях из разных отраслей.

Майнеры


Майнеры в 3 квартале 2024 г.
20,54%
26,84%
8,34%
21,29%
5,50%
9,08%
1,30%
4,39%
2,72%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Майнеры в 4 квартале 2024 г.
4,94%
3,71%
1,78%
23,70%
11,38%
4,85%
17,80%
22,14%
9,70%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Майнеры Q3/Q4
0,00%
5,00%
10,00%
15,00%
20,00%
25,00%
30,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

Вымогатели


Вымогатели в 3 квартале 2024 г.
7,67%
9,62%
2,92%
4,58%
2,85%
3,89%
2,24%
1,53%
64,70%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Вымогатели в 4 квартале 2024 г.
13,74%
7,96%
11,98%
5,61%
10,09%
8,81%
2,21%
2,78%
36,83%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Вымогатели Q3/Q4
0,00% 10,00% 20,00% 30,00% 40,00% 50,00% 60,00% 70,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

Стилеры


Стилеры в 3 квартале 2024 г.
3,02%
3,99%
1,77%
7,03%
33,29%
8,40%
14,19%
8,36%
19,95%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT

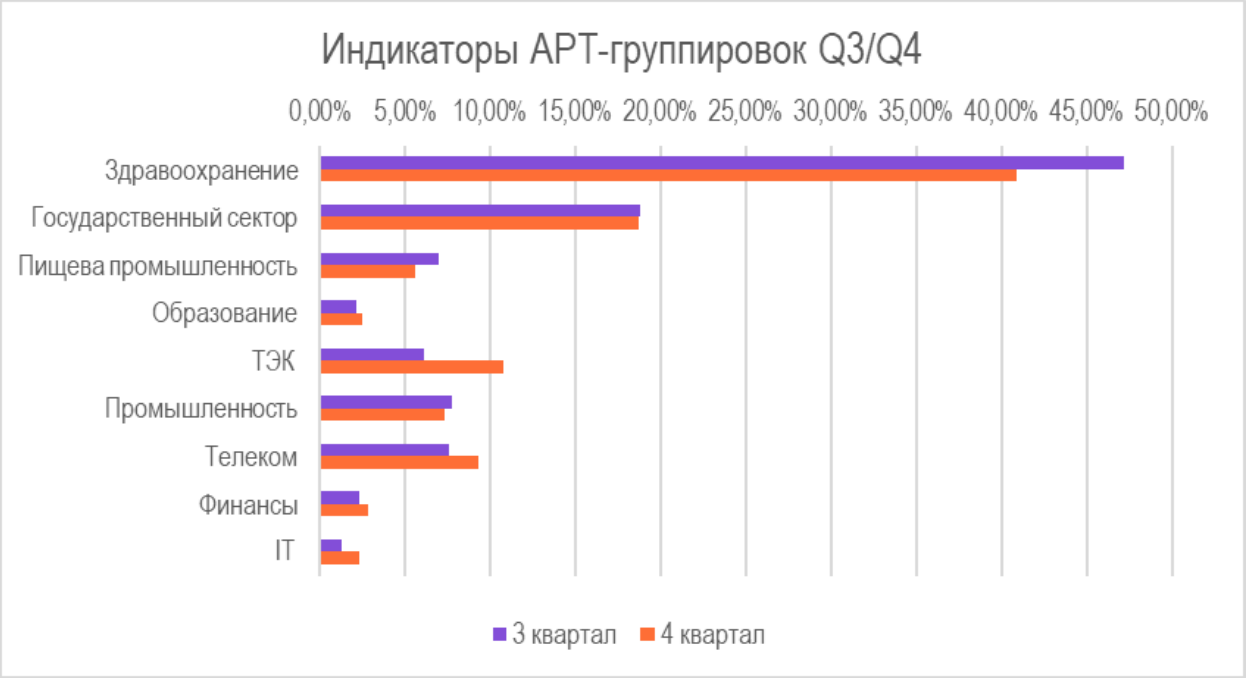

Стилеры в 4 квартале 2024 г.
3,63%
3,67%
2,50%
7,27%
33,67%
12,39%
14,75%
14,16%
7,94%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Стилеры Q3/Q4
0,00% 5,00% 10,00% 15,00% 20,00% 25,00% 30,00% 35,00% 40,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

APT


Индикаторы APT-группировок в 3 квартале 2024 г.
1,24%
2,33%
7,54%
7,71%
6,13%
2,14%
6,95%
47,20%
18,76%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Индикаторы APT-группировок в 4 квартале 2024 г.
2,25%
2,82%
9,31%
7,29%
40,84%
10,77%
2,49%
5,57%
18,65%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Индикаторы APT-группировок Q3/Q4
0,00% 5,00% 10,00% 15,00% 20,00% 25,00% 30,00% 35,00% 40,00% 45,00% 50,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

Загрузчики


Загрузчики в 3 квартале 2024 года
1,84%
3,19%
3,37%
17,20%
7,93%
17,91%
17,88%
12,09%
18,58%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT

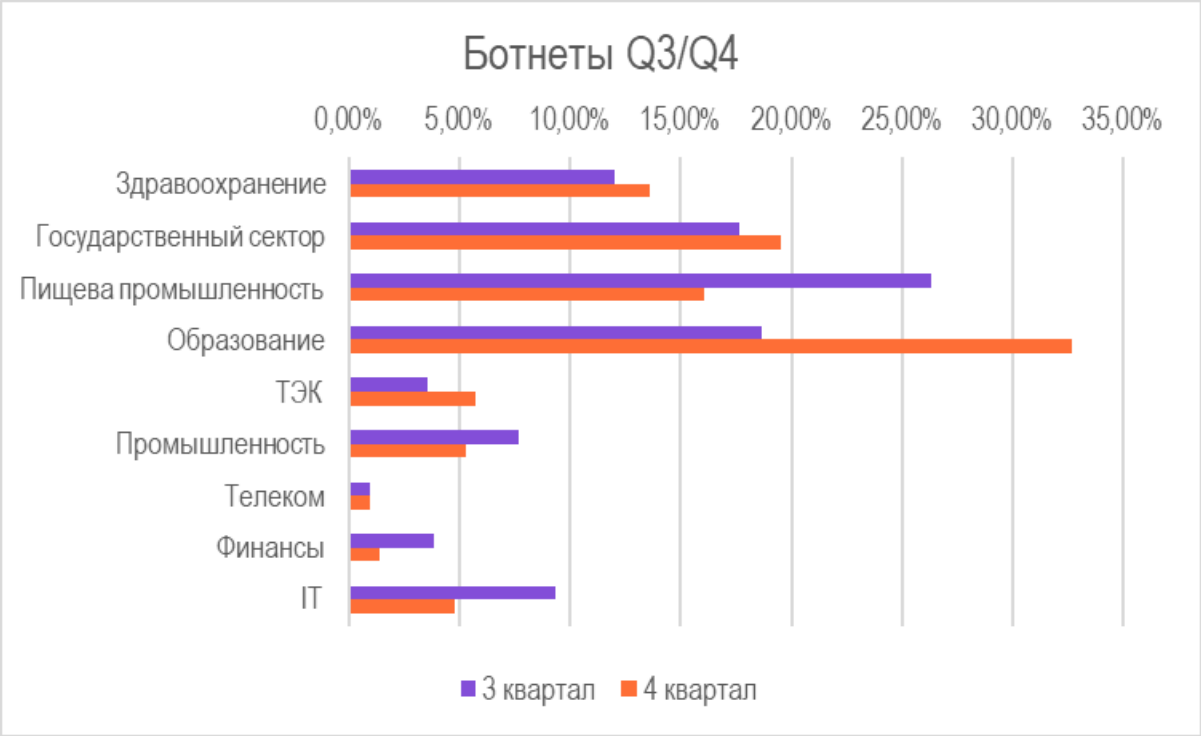

Загрузчики в 4 квартале 2024 г.
24,66%
16,51%
21,70%
15,81%
6,79%
6,30%
4,08%
2,21%
1,95%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Загрузчики Q3/Q4
0,00%
5,00%
10,00%
15,00%
20,00%
25,00%
30,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

Ботнеты


Ботнеты в 3 квартале 2024 г.
11,99%
17,64%
26,34%
18,67%
3,52%
7,68%
0,97%
3,83%
9,35%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT

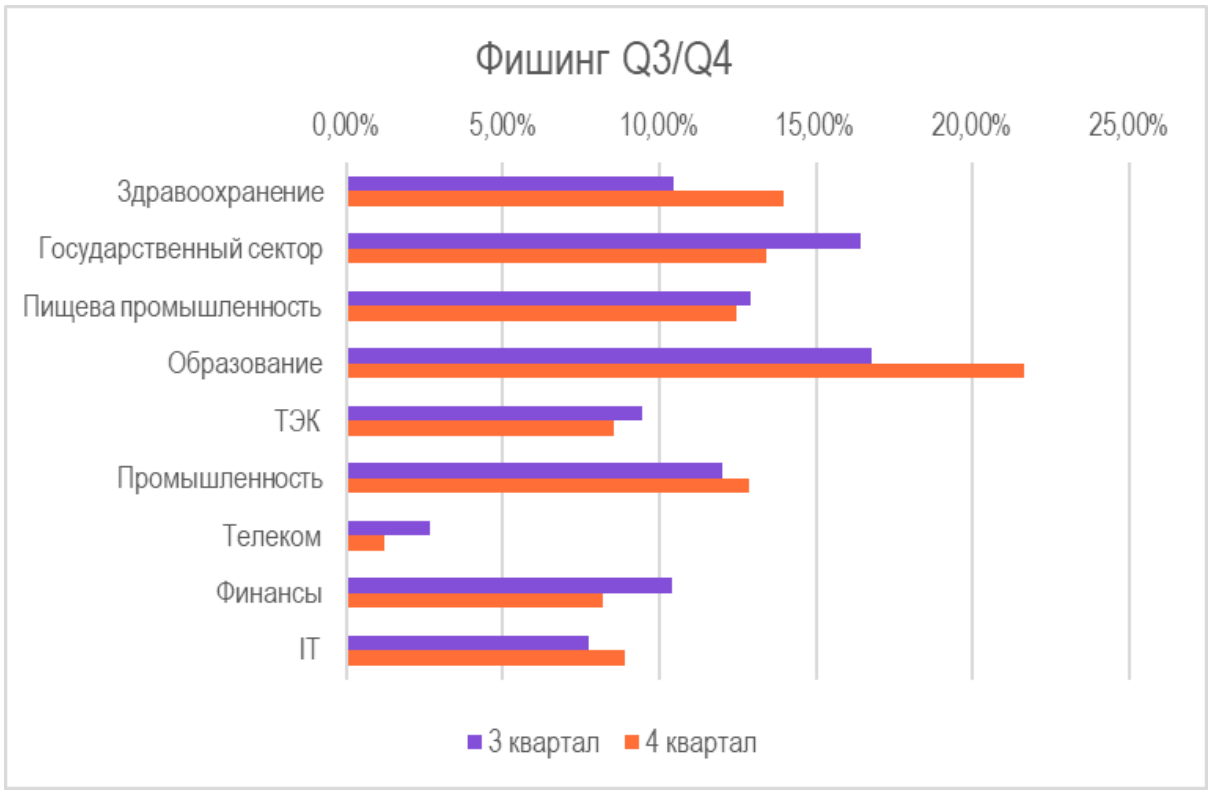

Ботнеты в 4 квартале 2024 г.
13,61%
19,53%
16,05%
32,63%
5,75%
5,32%
0,96%
1,36%
4,79%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Ботнеты Q3/Q4
0,00%
5,00%
10,00%
15,00%
20,00%
25,00%
30,00%
35,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

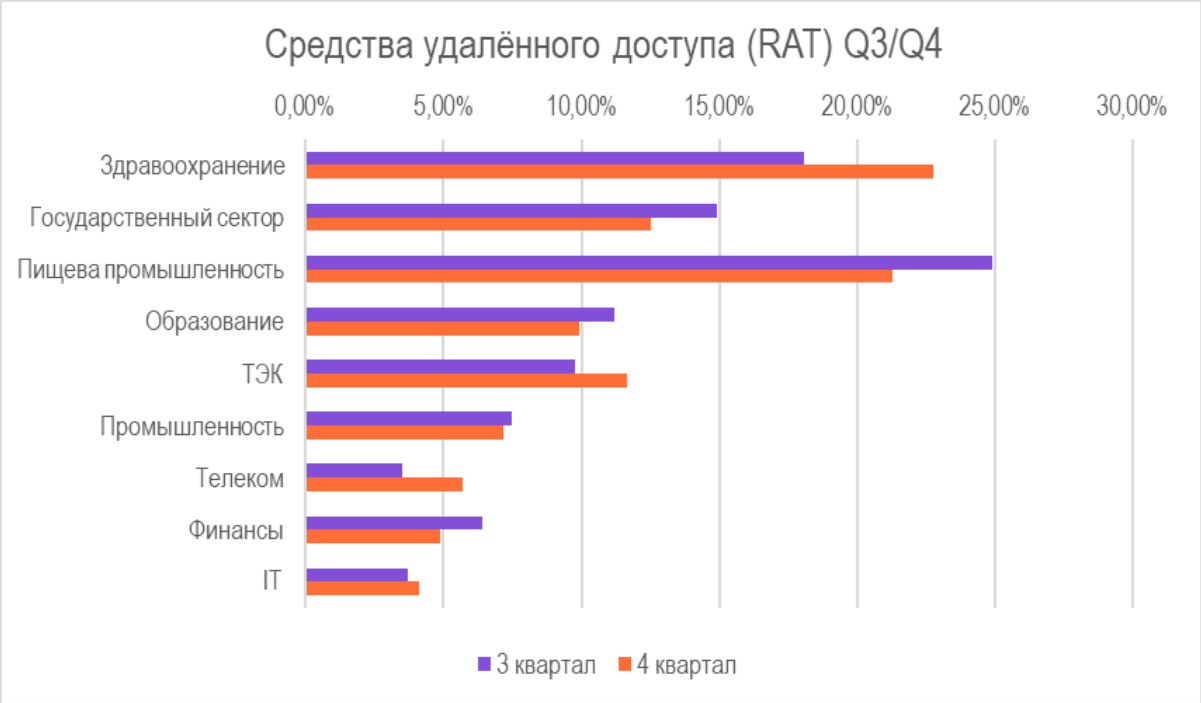
Фишинг


Фишинг в 3 квартале 2024 г.
8,92%
10,45%
10,38%
16,43%
2,69%
12,02%
12,89%
9,46%
16,76%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Фишинг в 4 квартале 2024 г
7,75%
13,96%
8,17%
1,20%
13,43%
12,87%
8,54%
12,44%
21,65%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT


Фишинг Q3/Q4
0,00%
5,00%
10,00%
15,00%
20,00%
25,00%
Здравоохранение
Государственный сектор
Пищева промышленность
Образование
ТЭК
Промышленность
Телеком
Финансы
IT
3 квартал
4 квартал

Средства удаленного доступа (RAT)



Регионы и индустрии

В этом разделе рассмотрим, как менялся средний показатель количества атак от индустрии к индустрии в разных регионах. Данные получены путём подсчета фактического количества срабатывания всех угроз на предприятиях в конкретной индустрии. Результаты нормализованы с учётом количества предприятий конкретной индустрии в рассматриваемом регионе.

Пищевая промышленность

Пищевая промышленность в 3 квартале 2024 г.	Среднее количество срабатываний	**Пищевая промышленность в 4 квартале 2024 г.**	Среднее количество срабатываний
Нижегородская область	253,87	Республика Марий Эл	151,22

Вологодская область	250,89	Вологодская область	145,85
Чувашская Республика	179,29	Нижегородская область	128,55
Республика Марий Эл	167,57	Город Санкт-Петербург	128,11
город Санкт-Петербург	135,8	Чувашская Республика	91,83
Тюменская область	113,2	Тюменская область	91,18
Кировская область	76,5	Удмуртская Республика	45,73
Удмуртская Республика	75,93	Ростовская область	40,9
Приморский край	64,74	Приморский край	37,75
Самарская область	64,68	Самарская область	32,75
Остальные	39,44	Остальные	25,06

IT

IT в 3 квартале 2024 г.	Среднее количество срабатываний	**IT в 4 квартале 2024 г.**	Среднее количество срабатываний
Самарская область	516,78	Пензенская область	375,38

Пензенская область	486,088	Самарская область	203,66
Саратовская область	252,8	Республика Татарстан	196,43
Омская область	168,95	Свердловская область	149,3
Калининградская область	164	Саратовская область	130,22
Вологодская область	163,53	Вологодская область	121,53
Кировская область	104,65	Республика Мордовия	95,9
Республика Мордовия	67,34	Калининградская область	90,52
Красноярский край	61,84	Тюменская область	46,03
Нижегородская область	27,9	Ульяновская область	19,51
Остальные	17,69	Остальные	8,17

Государственный сектор

Государственный сектор в 3 квартале 2024 г.	Среднее количество срабатываний	**Государственный сектор в 4 квартале 2024 г.**	Среднее количество срабатываний
Республика Саха (Якутия)	1531,1	Сахалинская область	205,14

Удмуртская Республика	332,8	Удмуртская Республика	167,53
Свердловская область	121,98	Кировская область	100,85
Архангельская область	109,84	Архангельская область	66,92
Ульяновская область	84,83	Республика Саха (Якутия)	58,47
Кировская область	65,65	Ульяновская область	54,54
Нижегородская область	59,44	Республика Мордовия	36,8
Самарская область	57,9	Новосибирская область	31,93
Красноярский край	53,6	Самарская область	30,47
Остальные	38,92	Ростовская область	27,83
Новосибирская область	33,05	Остальные	19,84

ТЭК

ТЭК в 3 квартале 2024 г.	Среднее количество срабатываний	**ТЭК в 4 квартале 2024 г.**	Среднее количество срабатываний
Карачаево-Черкесская Республика	1743,85	Карачаево-Черкесская Республика	4059,4

Мурманская область	805,63	Тамбовская область	2448,66
Республика Карелия	796,75	Ямало-Ненецкий автономный округ	346,34
Ханты-Мансийский автономный округ	336,6	Республика Карелия	323,18
Пензенская область	245,63	Удмуртская Республика	240,22
Краснодарский край	208,92	Пензенская область	157,35
Самарская область	168,63	Ханты-Мансийский автономный округ	70,48
Удмуртская Республика	140,62	Краснодарский край	54
Нижегородская область	111,52	Приморский край	49,22
Кемеровская область - Кузбасс	100,42	Самарская область	46,19
Остальные	49,88	Остальные	14,07

Образование

Образование в 3 квартале 2024 г.	Среднее количество срабатываний	**Образование в 4 квартале 2024 г.**	Среднее количество срабатываний
Республика Саха (Якутия)	2128,86	город Санкт-Петербург	101,74

Волгоградская область	450,75	Республика Саха (Якутия)	98,81
город Санкт-Петербург	296,73	Удмуртская Республика	35,98
Омская область	124,11	Республика Марий Эл	26,67
Ростовская область	117,2	Архангельская область	23,64
Удмуртская Республика	44,26	Чувашская Республика	23,15
Оренбургская область	34,53	Оренбургская область	23,02
Самарская область	29,94	Новосибирская область	14,71
Нижегородская область	25,99	Остальные	11,27
Краснодарский край	24,28	Ростовская область	11,22
Остальные	22,55	Нижегородская область	6,19

Промышленность

Промышленность в 3 квартале 2024 г.	Среднее количество срабатываний	**Промышленность в 4 квартале 2024 г.**	Среднее количество срабатываний
Ямало-Ненецкий автономный округ	2066,4	Кировская область	207,87

Кировская область	305,88	Свердловская область	196,06
Город Санкт-Петербург	257	город Санкт-Петербург	106,8
Чувашская Республика	217,81	Саратовская область	77,77
Саратовская область	174,61	Челябинская область	66,23
Челябинская область	144,69	Нижегородская область	58,3
Самарская область	108,18	Чувашская Республика	54,9
Нижегородская область	100,04	Самарская область	42,9
Ростовская область	88,33	Ростовская область	28,18
Удмуртская Республика	60,86	Удмуртская Республика	25,95
Остальные	53,46	Остальные	17,16

Здравоохранение

Здравоохранение в 3 квартале 2024 г.	Среднее количество срабатываний	**Здравоохранение в 4 квартале 2024 г.**	Среднее количество срабатываний
Республика Бурятия	20574	Удмуртская Республика	2822,4

Удмуртская Республика	4442,6	Республика Мордовия	346,42
Саратовская область	1797,59	Калининградская область	309,15
Республика Мордовия	308,02	Ульяновская область	66,27
Калининградская область	199,42	Республика Саха (Якутия)	59,21
Чувашская Республика	159	Нижегородская область	38,25
Омская область	68,47	Пензенская область	33,78
Нижегородская область	66,32	Краснодарский край	31,74
Краснодарский край	43,3	Чувашская Республика	31,61
Самарская область	38,63	Саратовская область	24,78
Остальные	29,49	Остальные	20,15

Финансы

Финансы в 3 квартале 2024 г.	Среднее количество срабатываний	**Финансы в 4 квартале 2024 г.**	Среднее количество срабатываний
Город Санкт-Петербург	766,94	Город Санкт-Петербург	200,26

Ульяновская область	366,079	Свердловская область	130,78
Челябинская область	356,11	Ульяновская область	89,93
Удмуртская Республика	340,02	Удмуртская Республика	72,58
Республика Мордовия	244,28	Камчатский край	45,68
Краснодарский край	78,69	Новосибирская область	40,6
Нижегородская область	71,3	Кировская область	33,17
Кемеровская область - Кузбасс	69,09	Нижегородская область	32,7
Оренбургская область	64,65	Приморский край	26
Кировская область	56,51	Оренбургская область	14,82
Остальные	30,73	Остальные	11,49

Телеком

Телеком в 3 квартале 2024 г.	Среднее количество срабатываний	**Телеком в 4 квартале 2024 г.**	Среднее количество срабатываний 2
Магаданская область	2823	Архангельская область	1487,39

Архангельская область	1695,77	Пензенская область	183,55
Красноярский край	238,81	Республика Мордовия	132,26
Пензенская область	147,57	Курганская область	72,16
Республика Мордовия	131,82	Омская область	68,94
Омская область	97,22	Республика Татарстан	62,6
Ульяновская область	55,3	Ульяновская область	27,76
Ханты-Мансийский автономный округ - Югра	47,06	Чувашская Республика	20,53
Приморский край	22,82	город Санкт-Петербург	19,09
Остальное	18,49	Оренбургская область	6,89
Амурская область	15,47	Остальные	4,21

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 количества атак типа Bruteforce может свидетельствовать о том, что злоумышленники активно работают над получением доступов во всевозможные инфраструктуры, а значит специалистам стоит уделять больше внимания подготовке своих сервисов к защите от атак грубой силы.

Среди попыток эксплуатации уязвимостей лидируют UPnP и Fortinet, что тоже указывает, на 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 PDNS также позволяет сделать несколько выводов. Средства удаленного доступа, APT-группировки, ботнеты и стилеры – остаются главной проблемой российских организаций.

Индустриям и регионам, в которых особенно высок показатель среднего количества срабатываний на организацию, стоит внимательнее относиться к обеспечению защиты своих инфраструктур. Высокий средний показатель указывает на признаки устойчивого заражения вредоносным ПО, а значит, и на необходимость оперативного принятия защитных мер.

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

- 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;