ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Отчёт Центра мониторинга
за II квартал 2017 года

Отчёт за III квартал 2016 года.

Отчёт за IV квартал 2016 года.

Отчёт за I квартал 2017 года.

Что и как мы считаем

В рамках данного отчёта:

- **Событие ИБ** — идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
- **Инцидент ИБ** — появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

Источниками событий выступают сетевые и хостовые IDS, сетевые устройства, сканеры защищённости, антивирусные решения и honeypot'ы.

В рамках внутренней обработки мы классифицируем инциденты в зависимости от затронутых ресурсов.

Высокая критичность	Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).
Средняя критичность	Инциденты, связанные с некритичными ресурсами серверного сегмента.
Низкая критичность	Инциденты, связанные с некритичными ресурсами пользовательского сегмента (рядовой пользователь).

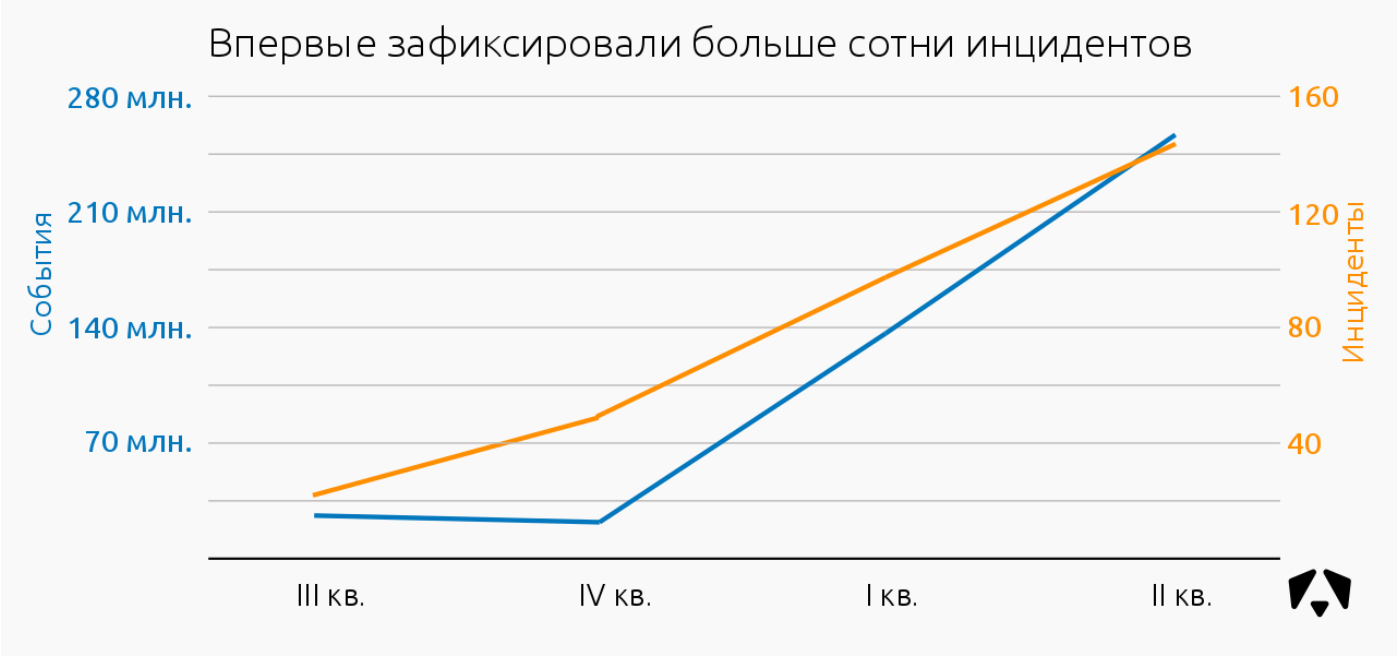
Аналитик Центра мониторинга произвольно определяет степень критичности, если считает, что инцидент может привести к серьёзным негативным последствиям.

Результаты мониторинга

В период с 1 апреля по 30 июня 2017 года сотрудники Центра мониторинга контролировали информационные системы нескольких организаций с общим числом подключённых узлов около 15 500 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.).

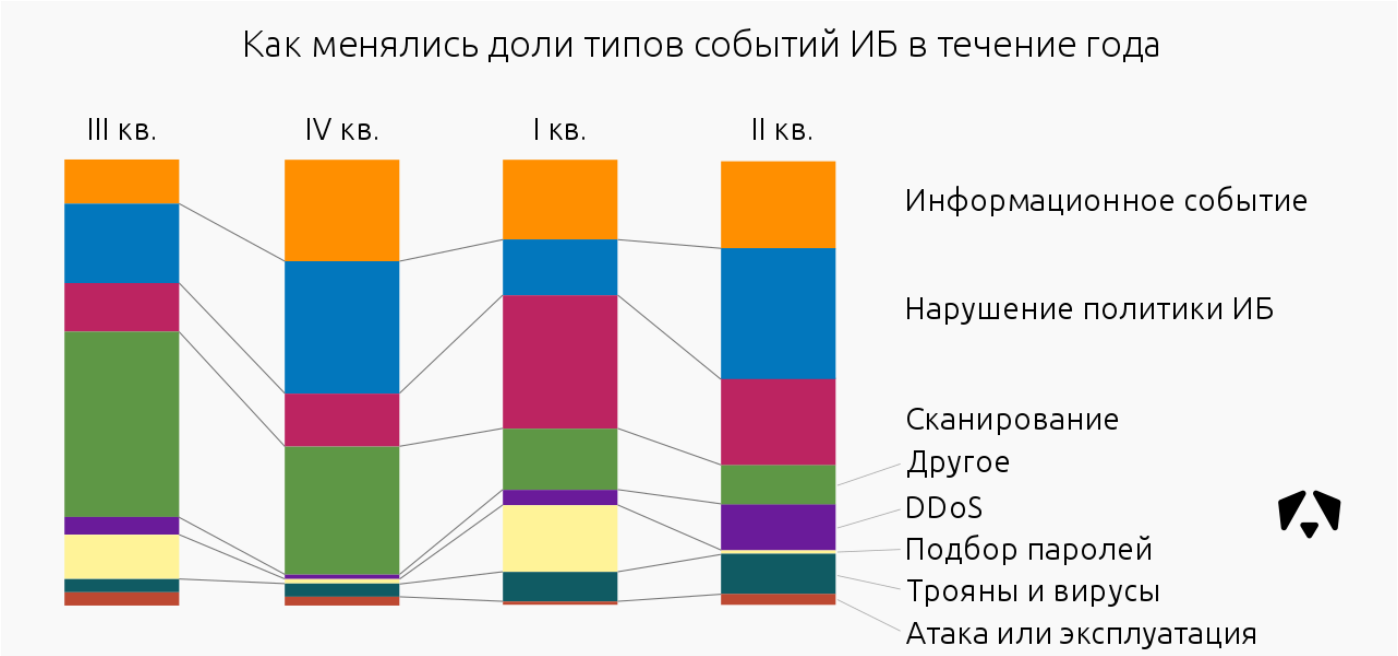
За три месяца сенсоры зафиксировали и проанализировали **254 453 172 события** информационной безопасности и выявили **144 инцидента**.

За предыдущий I квартал 2017 года Центр мониторинга зафиксировал **137 873 416 событий** ИБ и **98 инцидентов**.



Мы видим значительный рост количества зафиксированных событий (+85%) и инцидентов (+47%). При этом количество узлов на мониторинге росло медленнее, прирост за II кв. 2017 года составил около 30%.

Как будет видно на одном из графиков ниже, очень сильно увеличилось количество попыток эксплуатации уязвимостей (например EternalBlue, используемой при ransomware-атаках WannaCry и Petya).



«Информационное событие» — события, несущие информационную направленность, которые могут быть полезны при разборе инцидента.

«Нарушение политики ИБ» — события, свидетельствующие о действиях, предположительно нарушающих требования Политики ИБ контролируемой организации.

«Атака или эксплуатация» — события, свидетельствующие о попытках удалённого исполнения кода или эксплуатации уязвимостей на контролируемых ресурсах.

«Сканирование» — события, свидетельствующие об исследовании сети перед попыткой атаки.

«Подбор паролей» — события, свидетельствующие о попытках получения доступа к контролируемым ресурсам путём подбора аутентификационных данных.

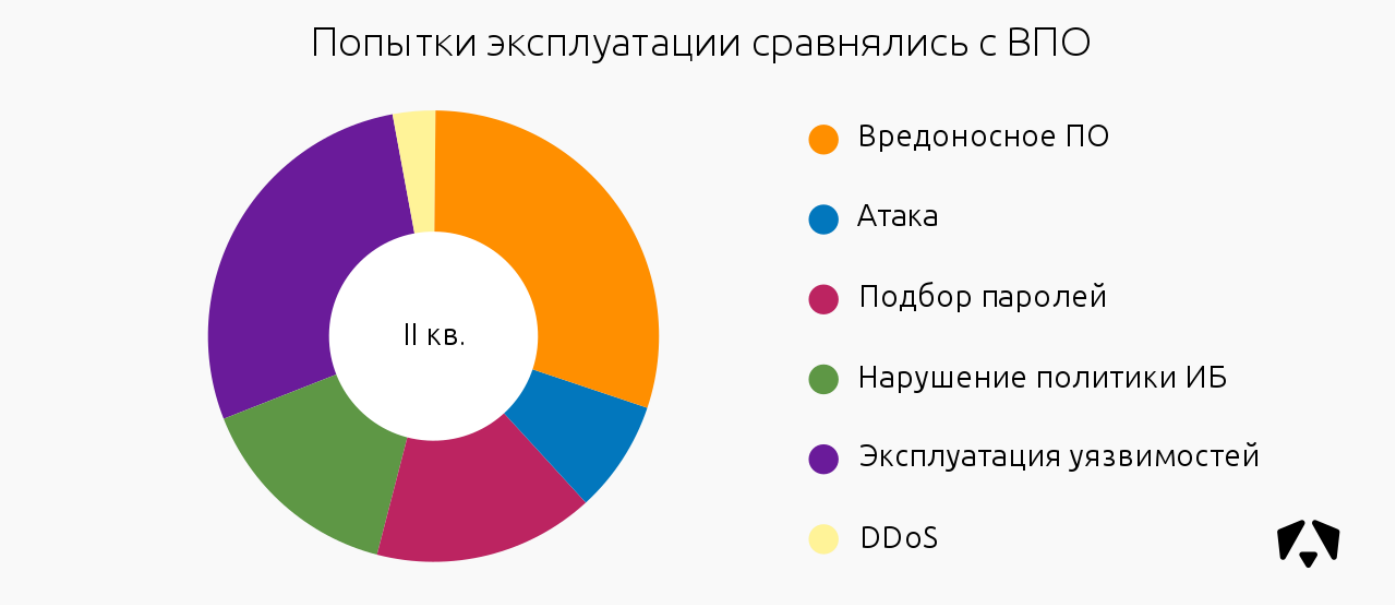
«Трояны и вирусы» — события, свидетельствующие о факте заражения контролируемых ресурсов вирусами или активности вредоносного ПО.

«DDoS» — события, свидетельствующие о попытках осуществления распределённых атак на отказ в обслуживании.

«Другое» — события которые по своей сути не могут быть отнесены к одному из вышеперечисленных классов.

Среди выявленных 144 инцидентов:

Класс инцидента	Высокая критичность	Средняя критичность	Низкая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО	8	21	14	43	30%
Атака	4	5	3	12	8%
Подбор паролей	11	8	4	23	16%
Нарушение политики ИБ	2	6	13	21	15%
Эксплуатация уязвимостей	12	21	7	40	28%
DDoS	3	2		5	3%
Всего:	40	63	41	144	100,0%



В I кв. 2017 года ситуация была немного другой:

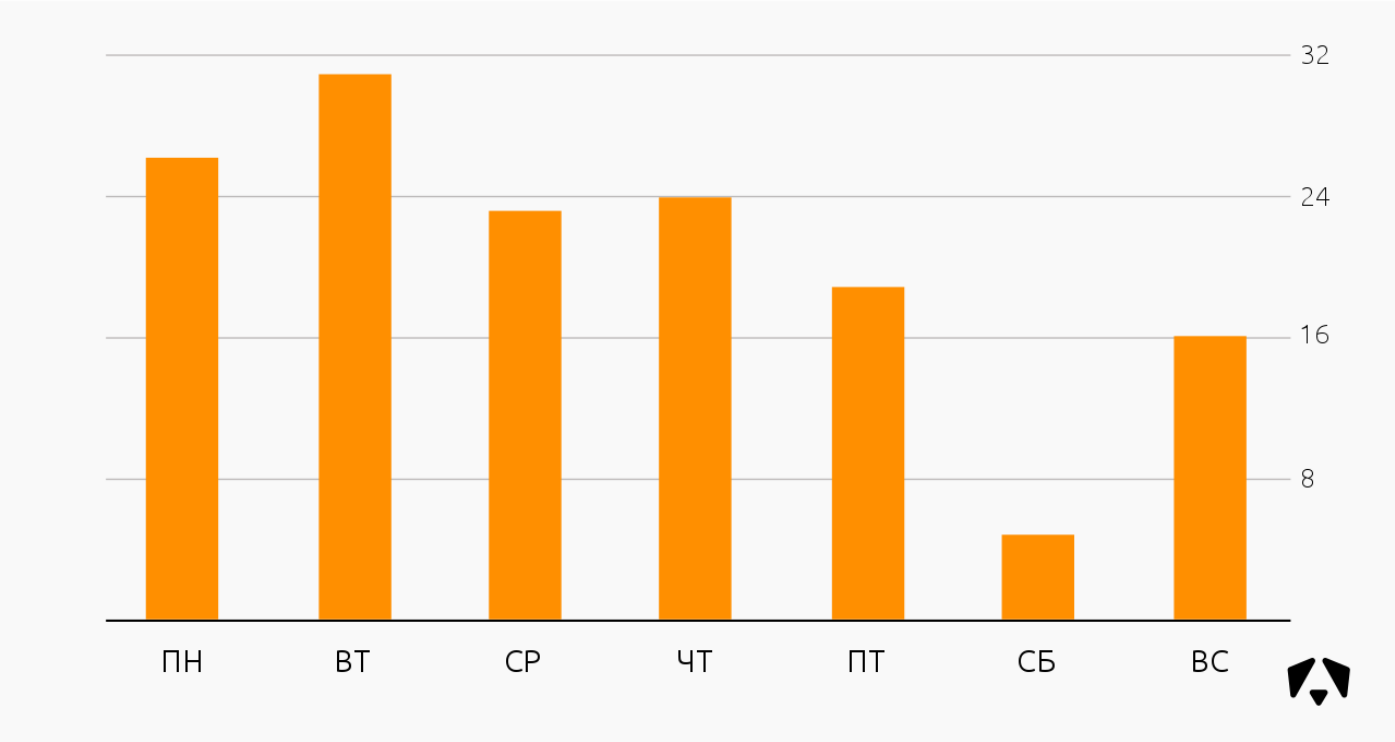
Соотношение типов зарегистрированных инцидентов ИБ в течение года менялось следующим образом:

	Доля инцидентов, %			
Класс инцидента	III кв. 2016	IV кв. 2016	I кв. 2017	II кв. 2017
Вредоносное ПО	42,8	51	52	30
DDoS	14,3	1,9	3	3
Нарушение политики ИБ	14,3	13,2	9	15
Подбор паролей	23,8	13,2	14	16
Атака		11,3	16	8
Эксплуатация уязвимостей	4,8	9,4	6	28

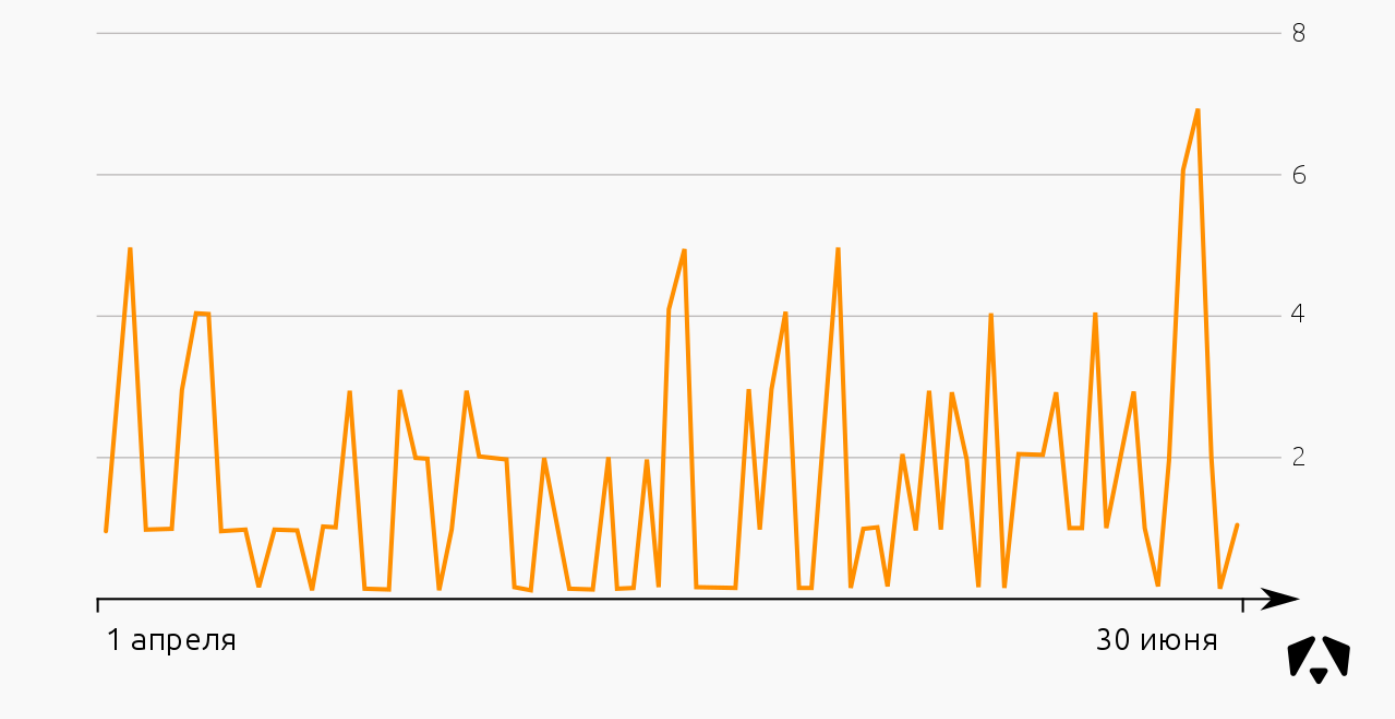
Недавняя публикация уязвимостей, обнаруженных зарубежными правительственными агентствами, и эксплойтов на них не прошла незамеченной в нашем Центре мониторинга. Мы увидели отчётливый рост количества попыток эксплуатации. К счастью, к моменту масштабных атак мы уже написали сигнатуры для сетевых средств защиты и «ловили» эти атаки на ранней стадии, поэтому удалось избежать большинства ОЧЕНЬ серьёзных последствий.

В I квартале 2017 года мы видели попытки некоторых сотрудников организаций, подключённых к Центру мониторинга, майнить криптовалюты на корпоративных ИТ-ресурсах. К сожалению, высокий курс bitcoin и ethereum провоцирует продолжать пробовать это делать. Такие инциденты попали в «Нарушение политики».

Распределение инцидентов ИБ относительно дней недели во II квартале 2017 года:



Распределение инцидентов ИБ за II квартал 2017 года:

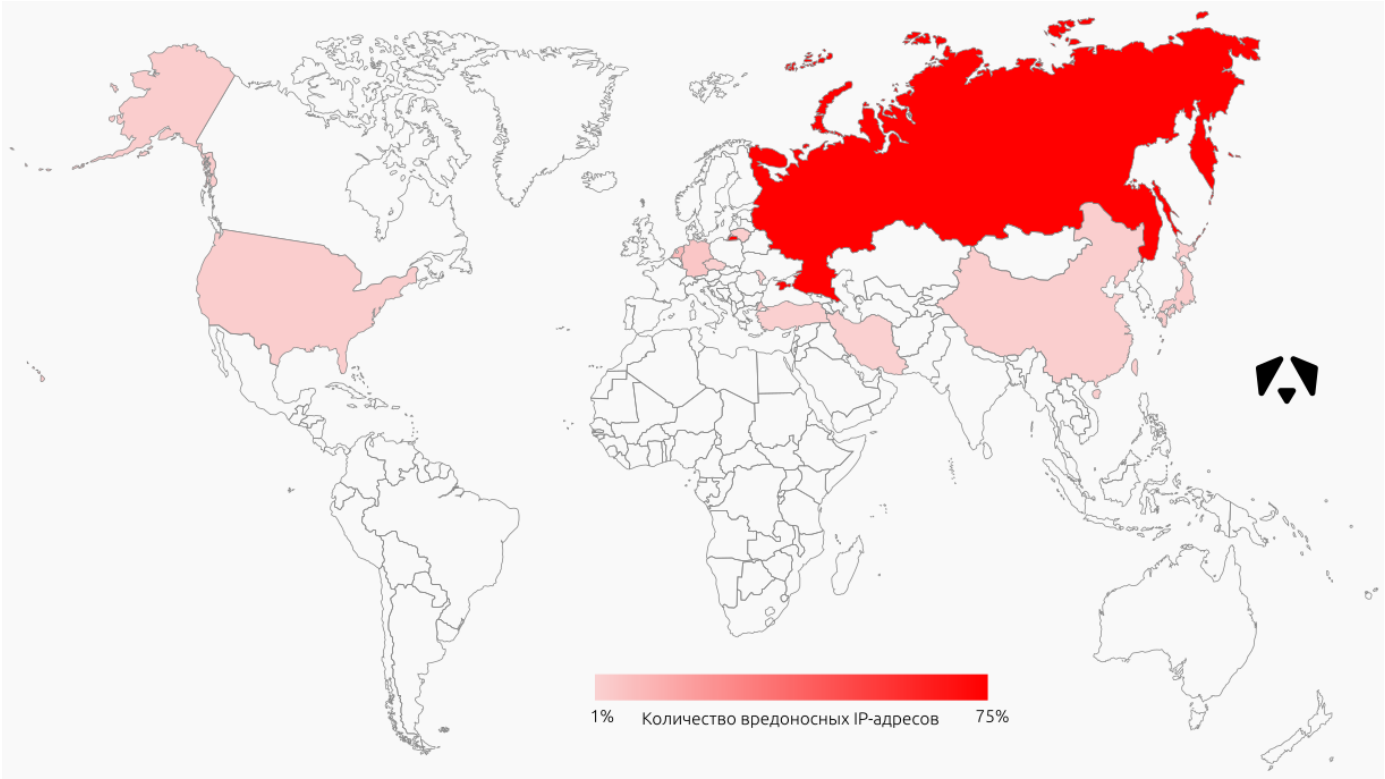


В этот раз наблюдаем достаточно ровную картину, без резких пиков.

ТОП источников

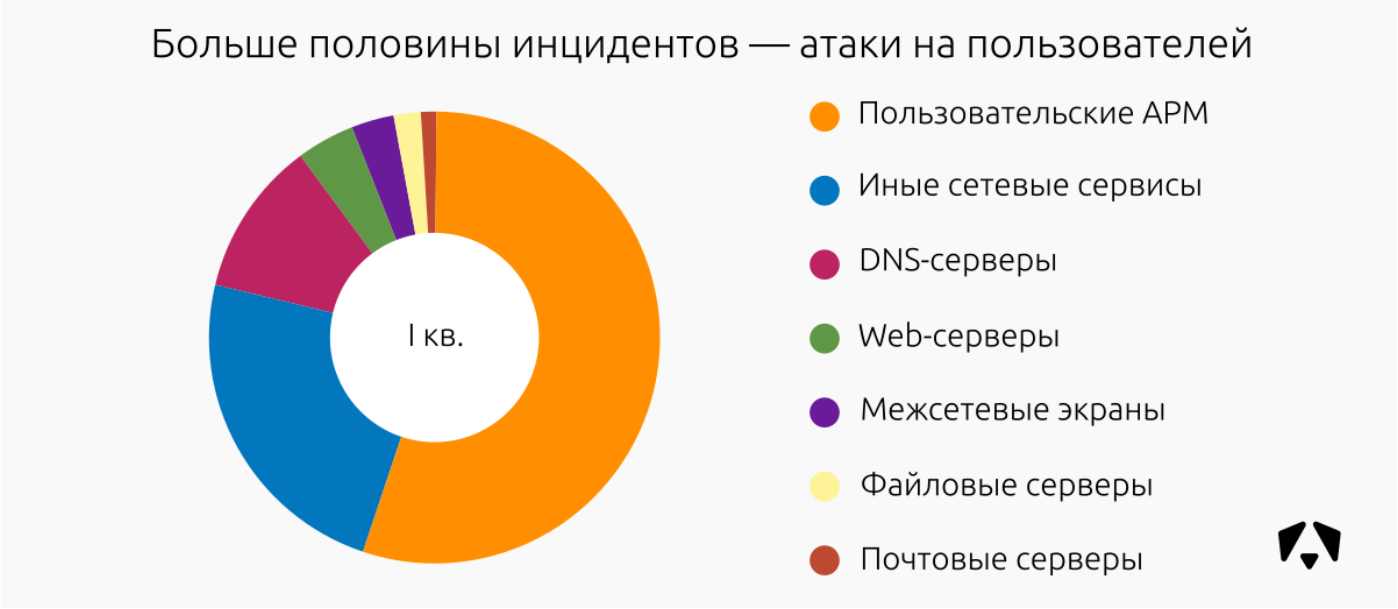
Под источниками атак в данном случае понимаются IP-адреса, которые были участниками сетевого взаимодействия с контролируемыми адресами.

На графике отражено расположение первой сотни IP-адресов по количеству зарегистрированных событий. Большинство таких адресов расположено в России, Нидерландах и Германии, хотя, конечно, нельзя утверждать, что атакующие были именно из этих стран.



ТОП подверженных инцидентам сегментов

Ситуация по целям атак немного изменилась по сравнению с предыдущим периодом. В I кв. 2017 года больше половины всех атак было направлено на пользовательские рабочие места.



В отчётном же периоде веб-сегменты так же часто подвергались атакам, как и пользовательские АРМ. Мы связываем это с составом подключённых на мониторинг узлов. Какой-то особой вредоносной активности не было.

Наиболее часто используемые техники воздействия на системы, повлёкшие инцидент ИБ

Угроза	Техника воздействия
Подбор паролей	Попытки подбора аутентификационной информации для доступа к сервисам и ресурсам контролируемых организаций — RDP, SSH, SMB, DB, Web.
Нарушение политик ИБ	Нарушение пользователями/администраторами контролируемых ресурсов требований политик ИБ в части использования устаревших версий или недоверенного ПО. Данное ПО может быть использовано злоумышленником для атаки путём эксплуатации уязвимости. Также использование ресурсов компании для получения собственной выгоды (майнинг bitcoin/ethereum). Использование торрент-трекеров.
Вредоносное ПО	Заражение конечной системы, распространение вируса по локальной сети, отключение/блокировка служб, препятствующих распространению вируса, попытки проведения иных атак внутри сети для получения критичной информации и передачи на командные серверы.
Попытки эксплуатации уязвимостей	Использование недостатков в системе для нарушения КЦД и воздействие на правильную работу системы. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ошибки конфигурации, отсутствия обновлений. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.