ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Отчёт Центра мониторинга
за IV квартал 2016 года

Что и как мы считали

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.

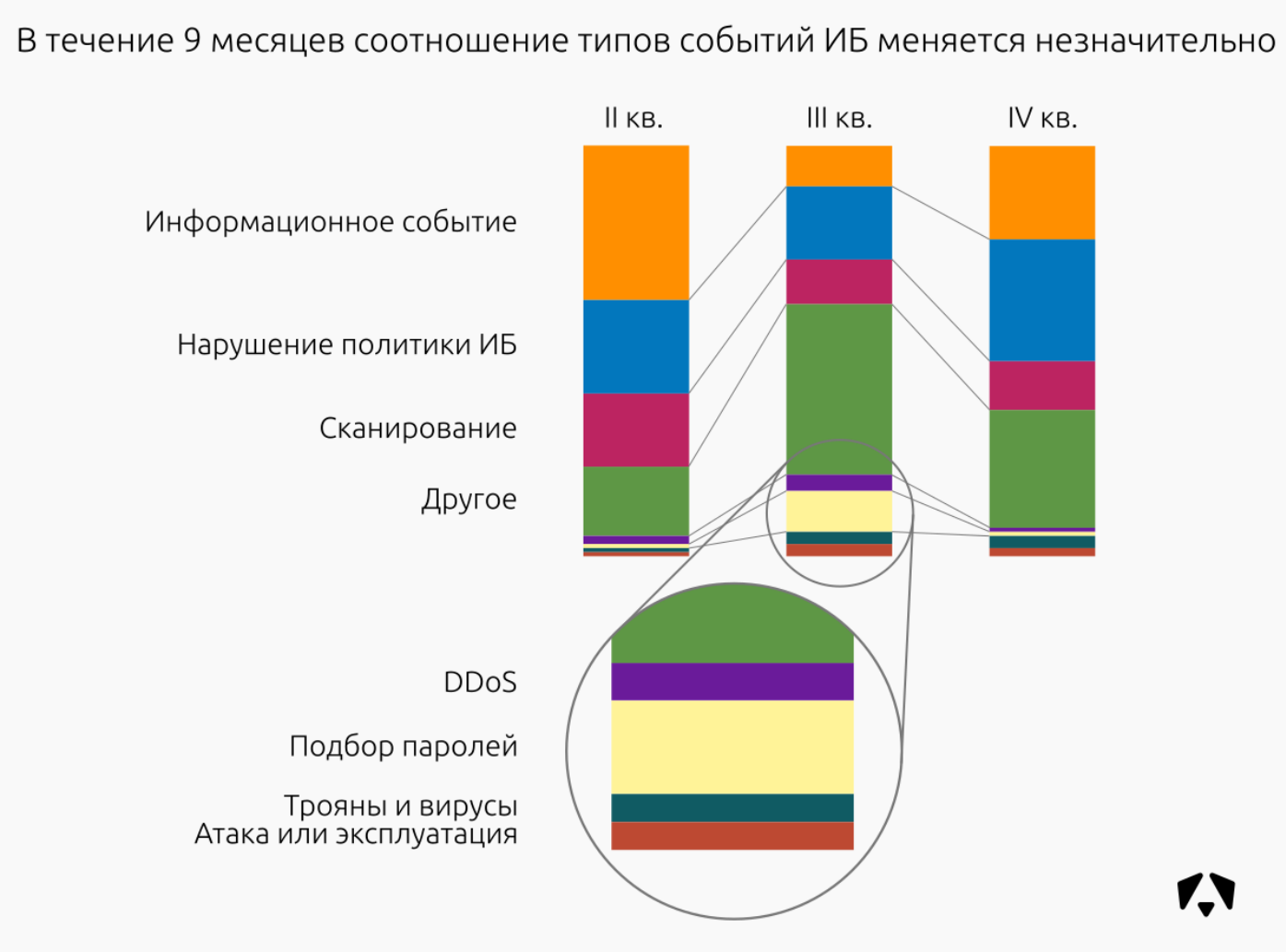
Высокая критичность	Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).
Средняя критичность	Инциденты, связанные с некритичными ресурсами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

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

Результаты мониторинга

В период с 1 октября по 31 декабря 2016 года сотрудники Центра мониторинга контролировали информационные системы нескольких организаций с общим числом подключённых узлов около 2 000 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.).

За три месяца сенсоры зафиксировали **21 788 201 событие** информационной безопасности и выявили **53 инцидента**.



«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.

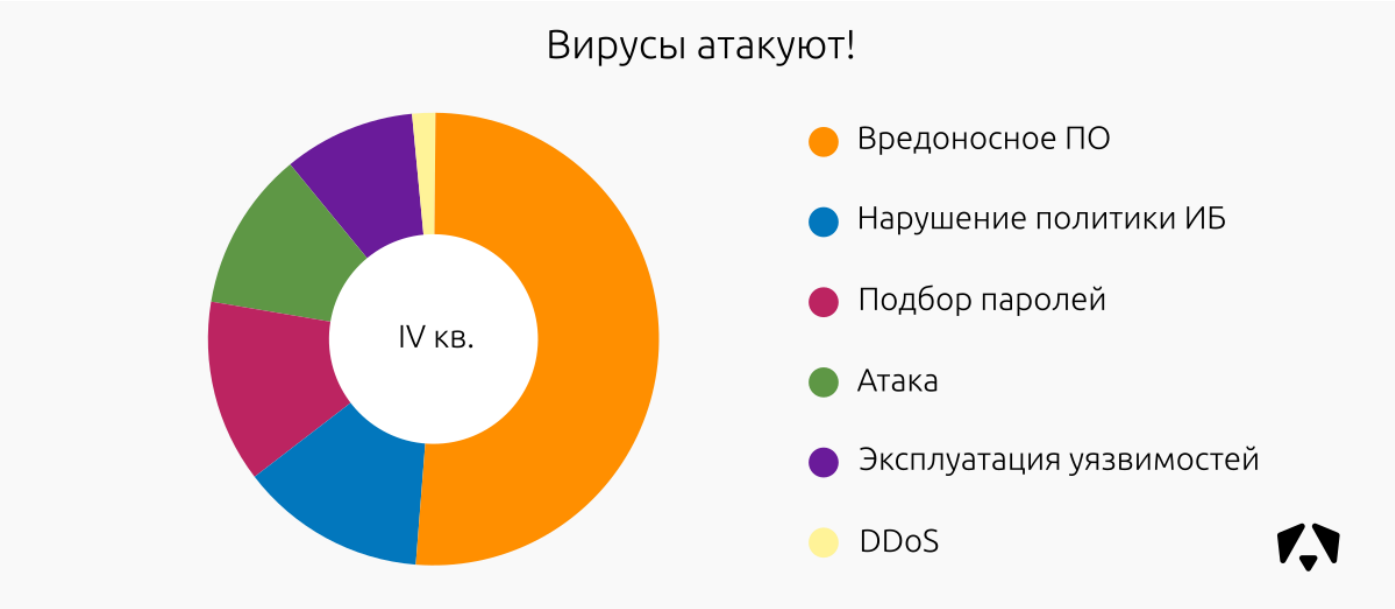
«Трояны и вирусы» — события, свидетельствующие о факте заражения контролируемых ресурсов вирусами или активности вредоносного ПО.

«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.

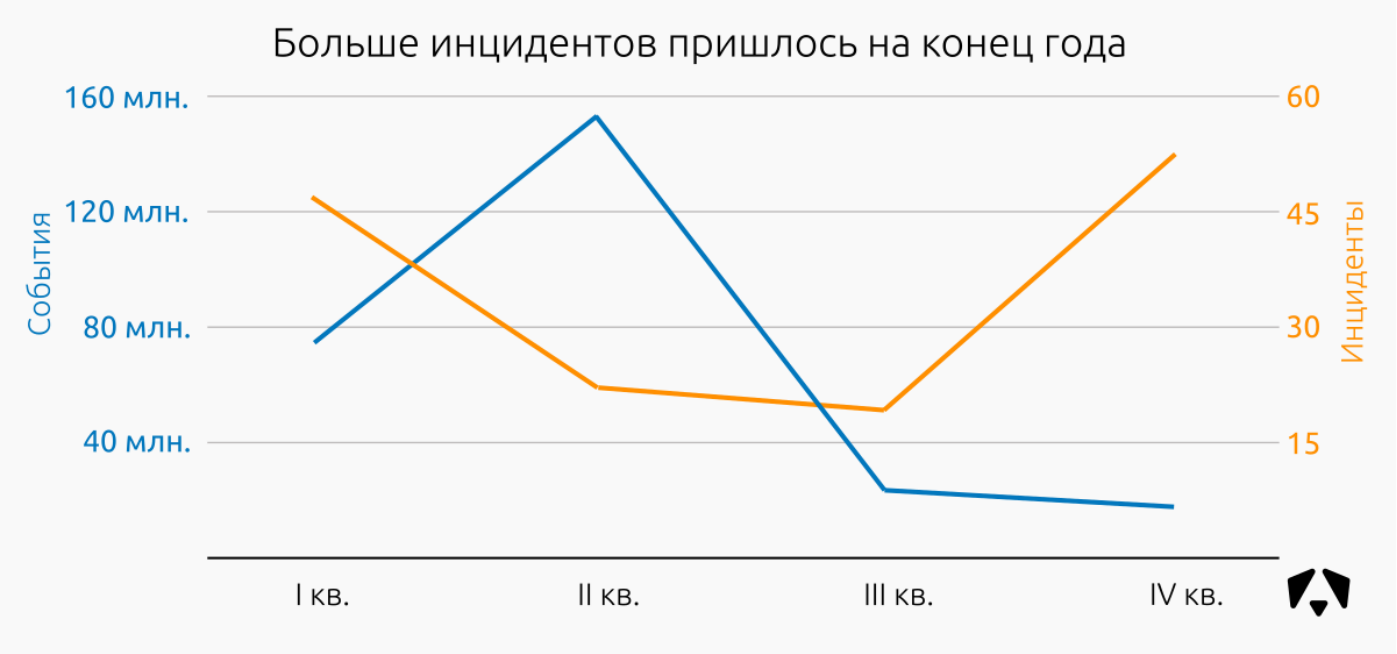
Среди выявленных 53 инцидентов:

Класс инцидента	Высокая критичность	Средняя критичность	Низкая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО	3	4	20	27	51%
Нарушение политики ИБ	3		4	7	13,20%
Подбор паролей	6	1		7	13,20%
Атака	6			6	11,30%
Эксплуатация уязвимостей	3	2		5	9,40%
DDoS	1			1	1,90%
Всего:				53	100,0%



Наиболее актуальными и критичными из выявленных являются атаки, связанные с попытками получения несанкционированного доступа к ресурсам организаций.

За предыдущий III квартал 2016 года Центр мониторинга зафиксировал **25 264 645 событий** ИБ и **21 инцидент**.

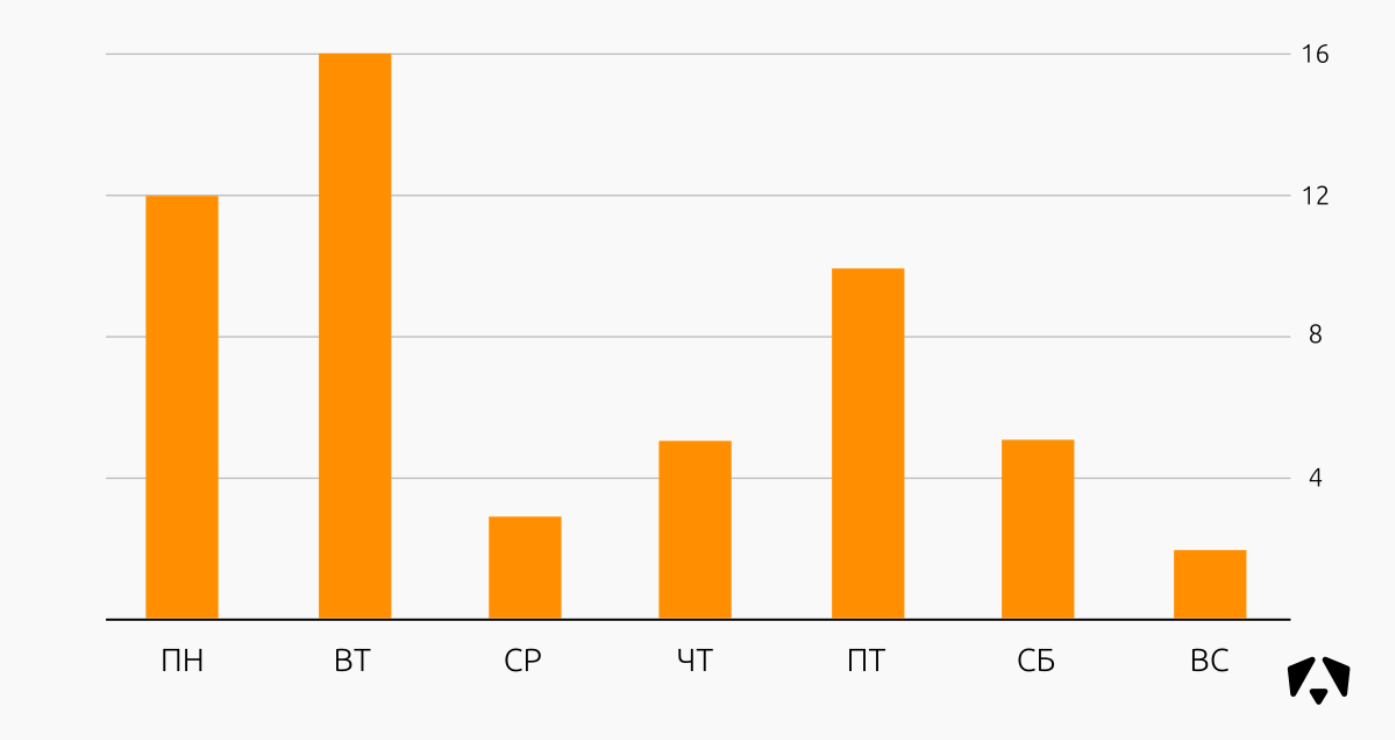


	Доля инцидентов, %			
Класс инцидента	I кв. 2016	II кв. 2016	III кв. 2016	IV кв. 2016
Вредоносное ПО	84,6	43,5	42,8	51
DDoS		8,7	14,3	1,9
Нарушение политики ИБ	2,6	30,4	14,3	13,2
Подбор паролей	5,1	17,4	23,8	13,2
Атака	7,7			11,3
Эксплуатация уязвимостей			4,8	9,4

Снижение количества зарегистрированных событий ИБ, с учётом увеличения количества контролируемых ресурсов, обусловлено тремя факторами:

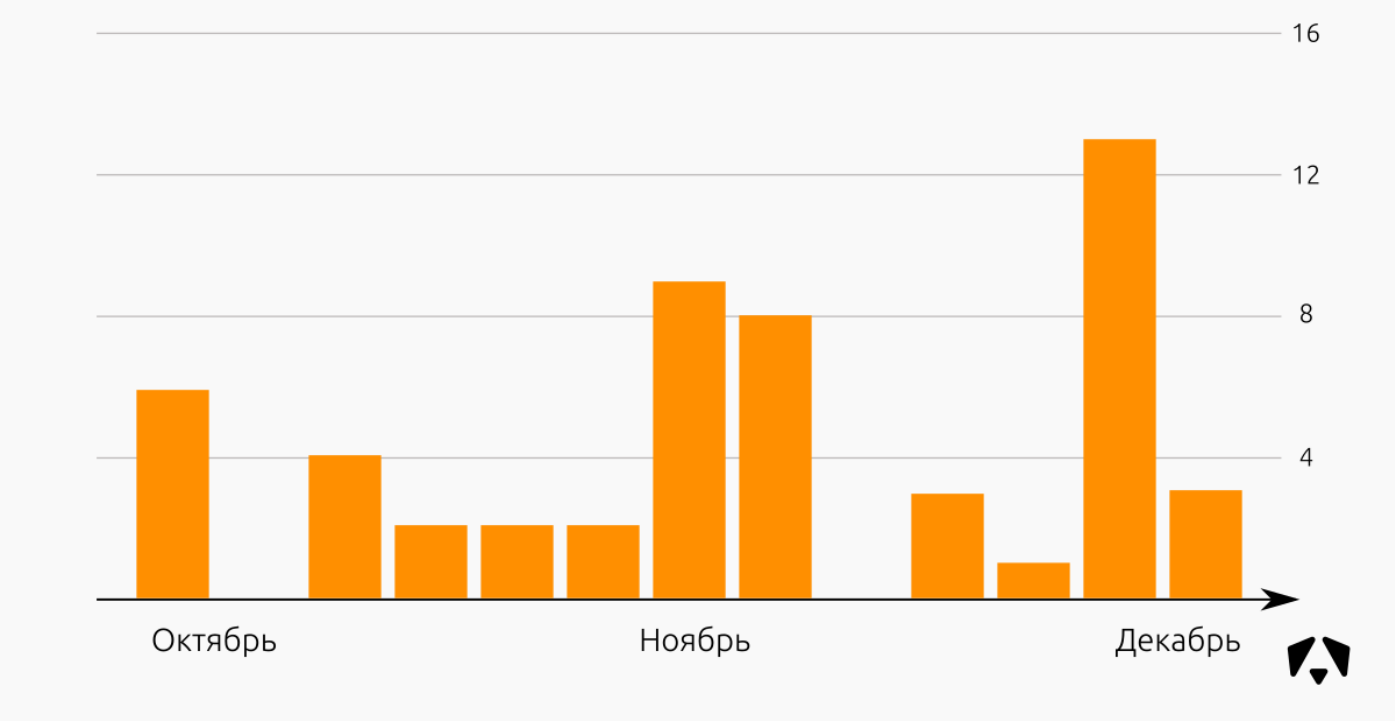
1. Сигнатурные аналитики доработали несколько десятков сигнатур, которые давали большое число false-positive срабатываний в конкретной контролируемой информационной системе.
2. Были оптимизированы некоторые правила базы AM Rules. Благодаря этому множество одинаковых событий теперь «склеиваются» в одно.
3. Благодаря первым двум пунктам Центр мониторинга быстрее реагирует на DDoS-атаки и другие инциденты ИБ, проявляющиеся в большом количестве срабатываний сигнатур, и помогает предотвращать их развитие на ранней стадии.

Распределение инцидентов ИБ относительно дней недели в IV квартале 2016 года:



В IV квартале 2016 года гипотеза о том, что большинство атак совершается вечером пятницы и в выходные дни не подтвердилась — инциденты распределяются по дням достаточно равномерно. Пики на графике в понедельник и вторник связаны с конкретными датами, когда произошло заражение нескольких рабочих станций.

Распределение инцидентов ИБ за IV квартал 2016 года:

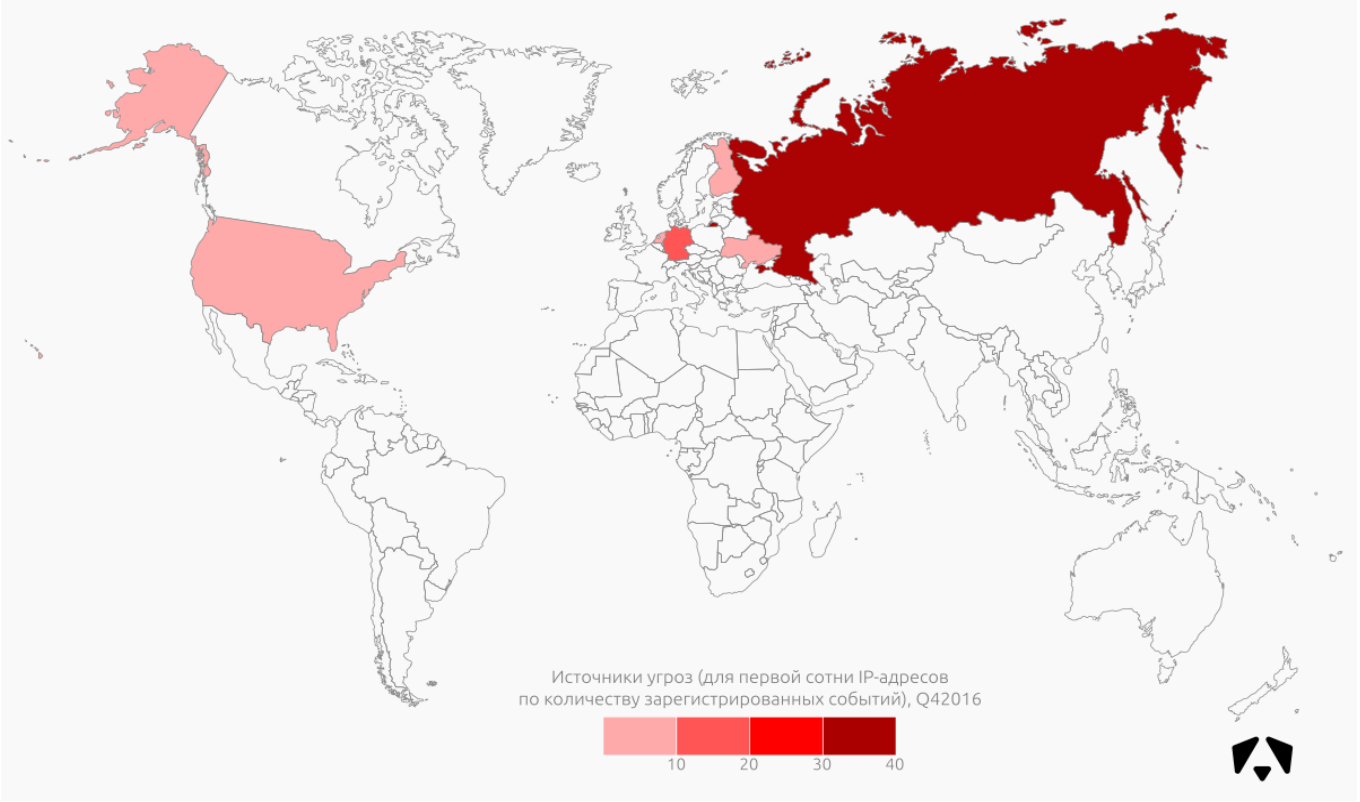


Также в отчётном квартале было зафиксировано несколько случаев e-mail фишинга, направленного против бухгалтеров и HR-специалистов. В темах писем содержались характерные слова: «сверка», «приостановка», «резюме». К письмам были прикреплены doc и docx файлы, анализ которых в Центре мониторинга подтвердил наличие в них вредоносного кода. Пока мы не фиксируем эти

случаи в публикуемой статистике, но, если они будут продолжаться, мы отразим это в следующем отчёте.

ТОП источников

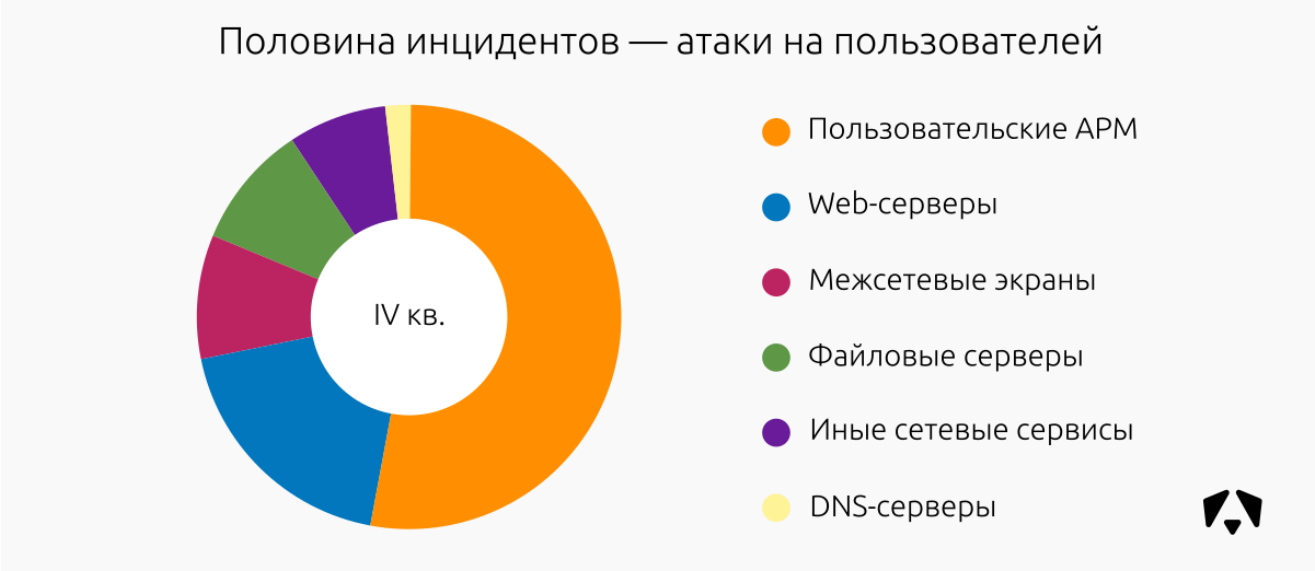
Под источниками атак в данном случае понимаются IP-адреса, с которых средства сетевой безопасности зафиксировали негативные действия. Большинство таких адресов расположено в России и Германии, хотя, конечно, нельзя утверждать, что атакующие были именно из этих стран.



Есть одна интересная особенность. Во II и III кварталах среди лидеров по количеству IP-адресов, с которых осуществлялись атаки, был Китай. В этом квартале мы не зафиксировали вредоносной активности оттуда. Предполагаем, что злоумышленники оттуда стали пользоваться российскими прокси.

ТОП подверженных инцидентам сегментов

Ситуация по целям атак изменилась непринципиально: наибольшую активность злоумышленники проявляли в отношении пользовательских рабочих мест и web-серверов, потому что это самые доступные для атак сегменты. На эти сегменты приходится три четверти всех инцидентов.



Наиболее часто используемые техники воздействия на системы, повлекшие инцидент ИБ

Угроза	Техника воздействия
Рекламное ПО	Заражение конечной системы, передача на командный сервер информации о пользователе, показ таргетированной рекламы.
Перебор 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 реализации атаки путём эксплуатации уязвимости.
Вирусное ПО (черви)	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.
DDoS с использованием ресурсов организации	DDoS Amplification — техника подмены своего адреса на адрес жертвы и генерации запросов небольшого размера к открытым сервисам. На запрос сервис возвращает ответ в несколько десятков раз большего объёма на адрес «отправителя». Используя большое количество ресурсов различных организаций, злоумышленник осуществляет DDoS-атаку на жертву.

Предыдущие отчёты

Отчёт за II квартал 2016 года.

Отчёт за III квартал 2016 года.