ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Отчёт Центра мониторинга
за второе полугодие 2017 года

С начала 2018 года мы переходим на полугодовой цикл публикации отчётов Центра мониторинга ПМ. Данный отчёт охватывает период с июля по декабрь 2017 года. Отчёты за предыдущие периоды доступны по ссылкам:

Отчёт за IV квартал 2016 года.

Отчёт за I квартал 2017 года.

Отчёт за II квартал 2017 года.

Что и как мы считаем

- **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.

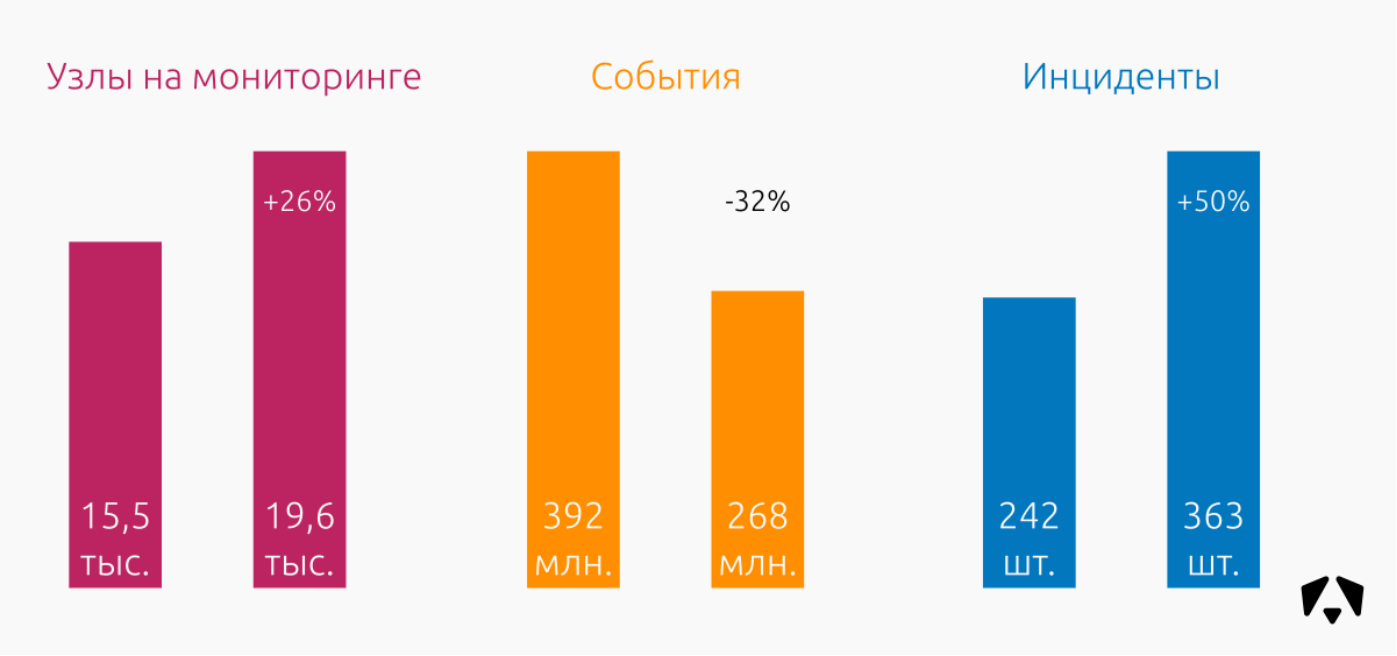
Источниками событий выступают сетевые и хостовые IDS, сетевые устройства, сканеры защищённости, антивирусные решения и honeypot'ы.

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 июля по 31 декабря 2017 года** сотрудники Центра мониторинга контролировали информационные системы организаций с общим числом подключённых узлов около **19 600** (рабочие места, веб, почта, файловые хранилища, VPN и т.д.). Благодаря растущему интересу к тематике создания и эксплуатации центров мониторинга информационной безопасности нам удалось во второй половине 2017 года привлечь новых постоянных клиентов и запустить несколько пилотных проектов.

За шесть месяцев сенсоры зафиксировали **268 млн. событий** информационной безопасности и выявили **363 инцидента**.

За первое полугодие 2017 года Центр мониторинга зафиксировал **392 млн. событий** ИБ и **242 инцидента**.

Падение числа зафиксированных событий связано с двумя причинами.

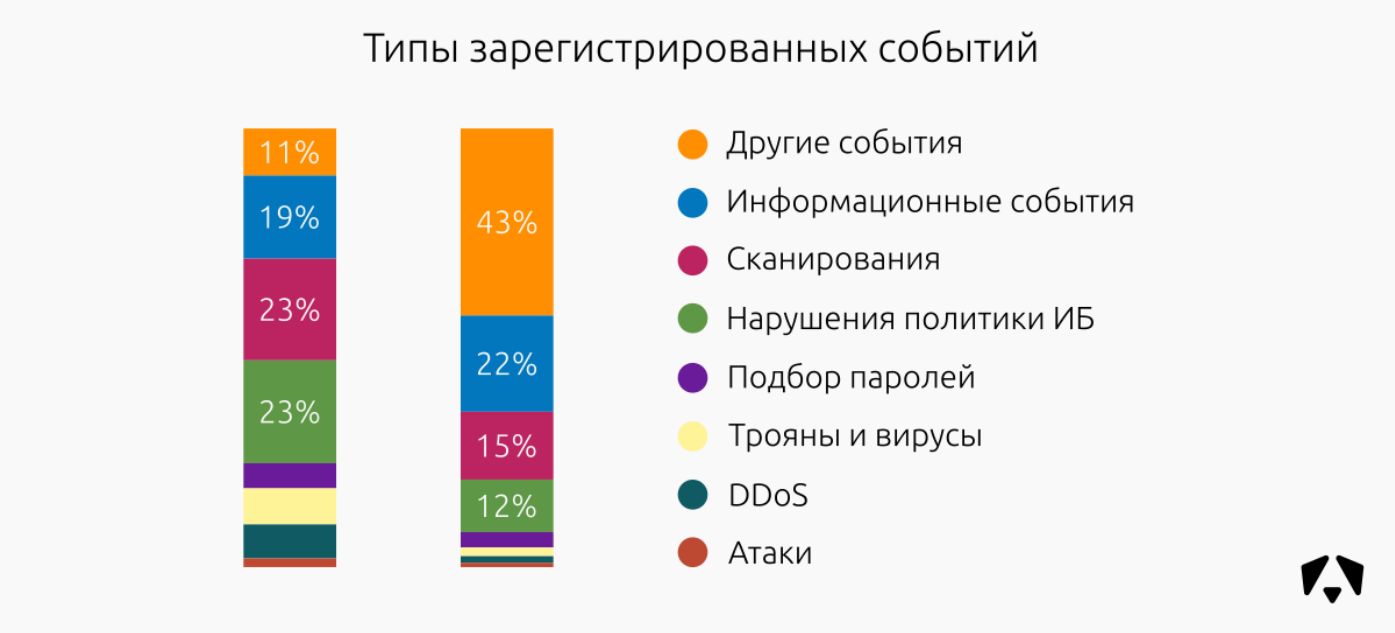
Первая причина — наши сенсоры стали работать лучше. На первый взгляд это несколько парадоксально, ведь очевидно, что чем больше узлов и заказчиков, тем больше трафик и, следовательно, должно быть больше событий. Поскольку мы сами разрабатываем правила обнаружения атак для сетевых сенсоров и сенсоров уровня хоста, у нас есть возможность их оперативно модернизировать.

> *Например, сотрудники дежурной смены центра мониторинга видят срабатывания определённого правила у заказчика. Если это явно ложное срабатывание средств защиты на легальную активность или правильное срабатывание, но средство защиты генерирует очень большое количество одинаковых сообщений, то дежурная смена создаёт заявку на доработку правил. Сигнатурные аналитики принимают эту заявку в работу, разбираются в ситуации и либо вносят правки в эти правила, либо делают так, чтобы эти многочисленные оповещения «склеивались» в одно. При следующем обновлении сенсора поток зафиксированных событий снизится.*

Вторая причина — более оперативное реагирование на инциденты ответственными сотрудниками заказчиков. Чем дольше мы взаимодействуем с администраторами ИТ и ИБ, тем более отработанными становятся их действия по реагированию, тем быстрее прекращается атака или

аномалия / осуществляется процесс сдерживания, тем меньшее в итоге количество событий мы получаем.

Пятидесятипроцентный рост количества инцидентов по сравнению с первым полугодием 2017 года вызван тем, что к Центру мониторинга активно подключались новые заказчики. А новая инфраструктура на мониторинге — это почти гарантированно всплеск количества выявленных инцидентов, которые владелец инфраструктуры ранее просто не мог заметить. Стоит разобраться с этим «новым пиком», и количество зафиксированных инцидентов резко снижается.



«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.

Распределение зафиксированных событий не сильно изменилось по сравнению с первой половиной 2017 года. Превалируют информационные события, попытки сканирования и нарушения политик информационной безопасности.

Самое заметное отличие — значительный рост т. н. «Других событий». Поскольку во втором полугодии они составили 43% от всех зафиксированных, мы сочли необходим подробно объяснить, почему так получилось.

По нашей текущей классификации «Другие события» — это большей частью события, сигнализирующие об аномалиях в сетевом трафике, которые связаны с:

- некорректной настройкой сетевой инфраструктуры («Работает и ладно!»);
- спецификой работы сетевого оборудования.

В качестве примера можно привести случай, с которым было связано много «других» событий. Один из сотрудников заказчика смотрел видео с камер наблюдения с сервера через терминал. Пока разбирались, что это за трафик, сенсоры нагенерировали огромное количество событий.

Ещё одна проблема, с которой обычно не сразу удаётся справится, — это активность самописного или редкого прикладного ПО во внутренней сети. Сетевые сенсоры просто не знают, что это за трафик, пока мы не доработаем набор правил.

Среди выявленных **363 инцидентов**:

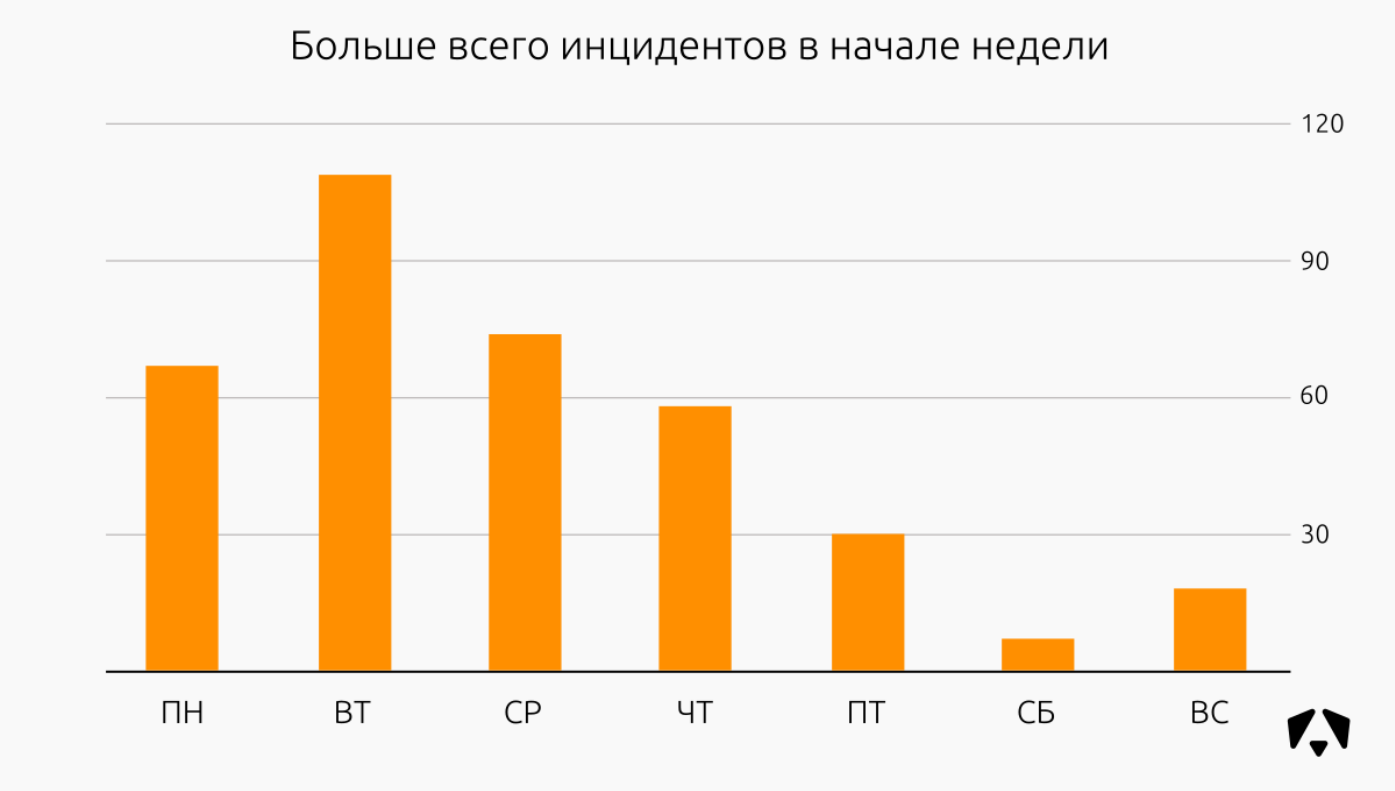
Класс инцидента	Высокая критичность	Средняя критичность	Низкая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО	59	29	66	154	42%
Эксплуатация уязвимостей	33	19	16	68	19%
Подбор паролей	26	23	10	59	16%
Атака	10	26	11	47	13%
Нарушение политики ИБ	11	9	8	28	8%
DDoS	4	3	0	7	2%
Всего:	143	109	111	363	100%

По вредоносному ПО мы наблюдали следующие тенденции:

1. Чем больше узлов на мониторинге — тем больше инцидентов с ВПО (очевидно).
2. Как и во втором квартале 2017 года продолжаются заражения семейством вредоносов WannaCry и Petya/notPetya.
3. Мы столкнулись с новым видом ВПО, в котором используются компоненты WannaCry. Оно не шифрует данные, а распространяется по сети, заражая подверженные уязвимости EternalBlue узлы. После этого «стучится» наружу. Если попытка заражения удалась, это значит, что машина подвержена RCE, что для нас крайне неприятно.
4. Всё чаще находим ВПО для майнинга криптовалют.

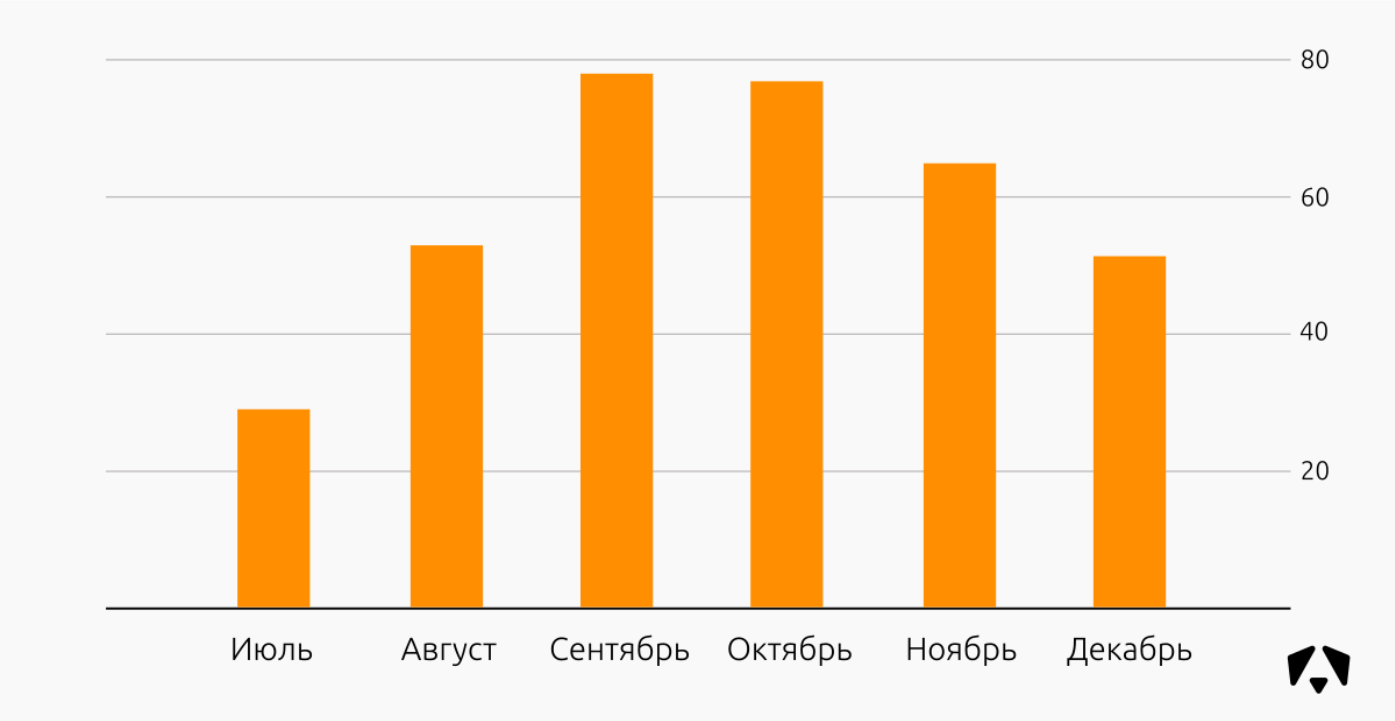
Что касается «Эксплуатации уязвимостей», то мы увидели рост попыток эксплуатации уязвимостей в Apache Struts, эксплойты на которые попали в набор Metasploit как раз в отчётный период.

Распределение инцидентов ИБ относительно дней недели во втором полугодии 2017 года:



Как правило, услуги мониторинга для новых заказчиков мы начинаем оказывать с начала недели, поэтому пики понятны и предсказуемы. В понедельник – вторник в Центр мониторинга начинают поступать события, мы фиксируем инциденты и помогаем с ними разобраться.

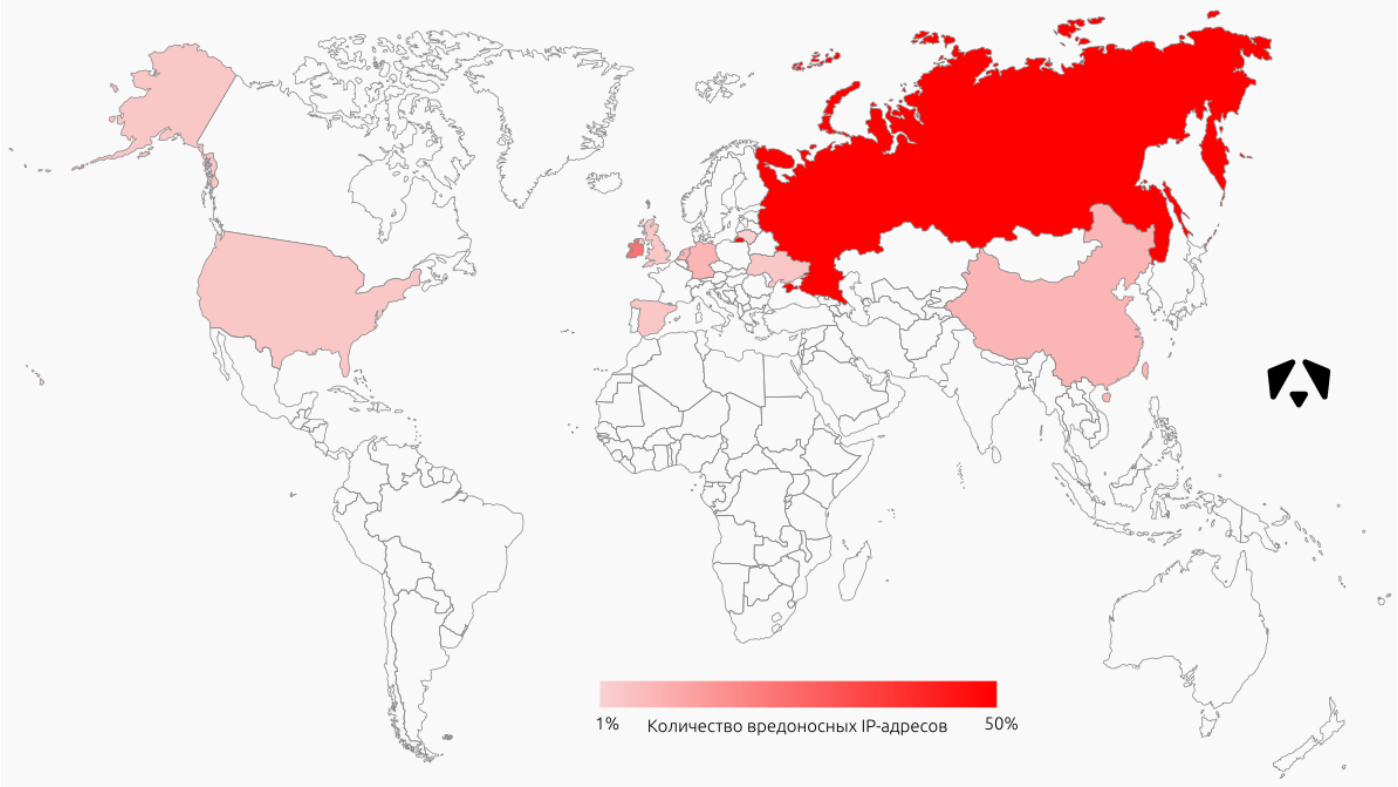
Распределение инцидентов ИБ за второе полугодие 2017 года:



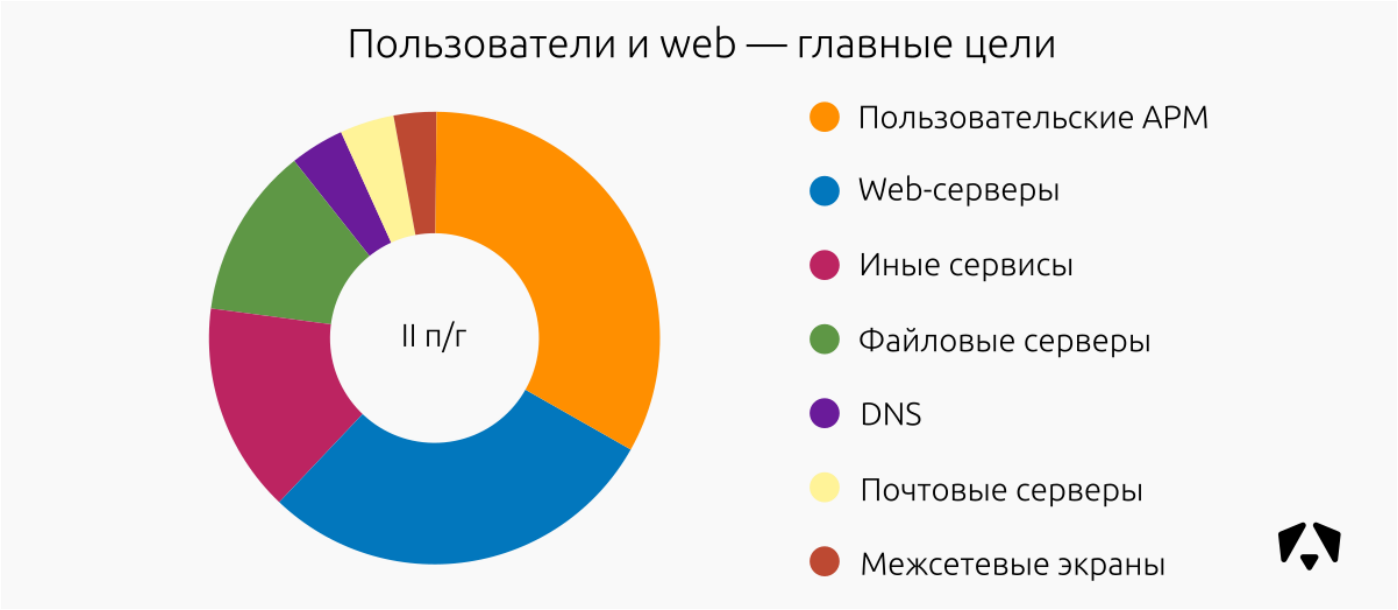
ТОП источников

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

На карте отражено расположение первой сотни IP-адресов по количеству зарегистрированных событий. Большинство таких адресов расположено в России, Ирландии (новичок наших отчётов, все адреса принадлежат Амазону), Германии и Нидерландах.



ТОП подверженных инцидентам сегментов



Во втором полугодии (как и во втором квартале) 2017 года веб-сегменты так же часто подвергались атакам, как и пользовательские АРМ. В сумме это две трети всех атак на контролируемые ресурсы. Это достаточно очевидные и вполне доступные из внешних сетей цели.

Основные типы атак на веб — брутфорс и попытки эксплуатации уязвимостей, в том числе и на веб-сервер Apache, о чём мы писали выше. На пользовательские АРМ — вредоносное ПО.

Центр мониторинга ЗАО «ПМ»

Отчёт подготовлен сотрудниками Центра мониторинга в феврале 2018 года.

Сообщить об инциденте информационной безопасности и получить помощь в реагировании можно по ссылке — https://amonitoring.ru/incident/ или по телефону +7 495 737-61-97.

Описание всех услуг компании «Перспективный мониторинг» — https://amonitoring.ru/service/