ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Отчёт Центра мониторинга
за I квартал 2017 года

Этим отчётом мы закрываем первый год регулярных публикаций о событиях и инцидентах информационной безопасности, обнаруженных Центром мониторинга.

За этот год поменялись правила выявления и учёта событий (некоторые события «склеиваются» в одно) и количество узлов на мониторинге, поэтому напрямую сравнивать количество событий и инцидентов сейчас и год назад будет не совсем правильно. Тем не менее, вся статистика за предыдущие периоды доступна на сайте компании.

Отчёт за II квартал 2016 года.

Отчёт за III квартал 2016 года.

Отчёт за IV квартал 2016 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.

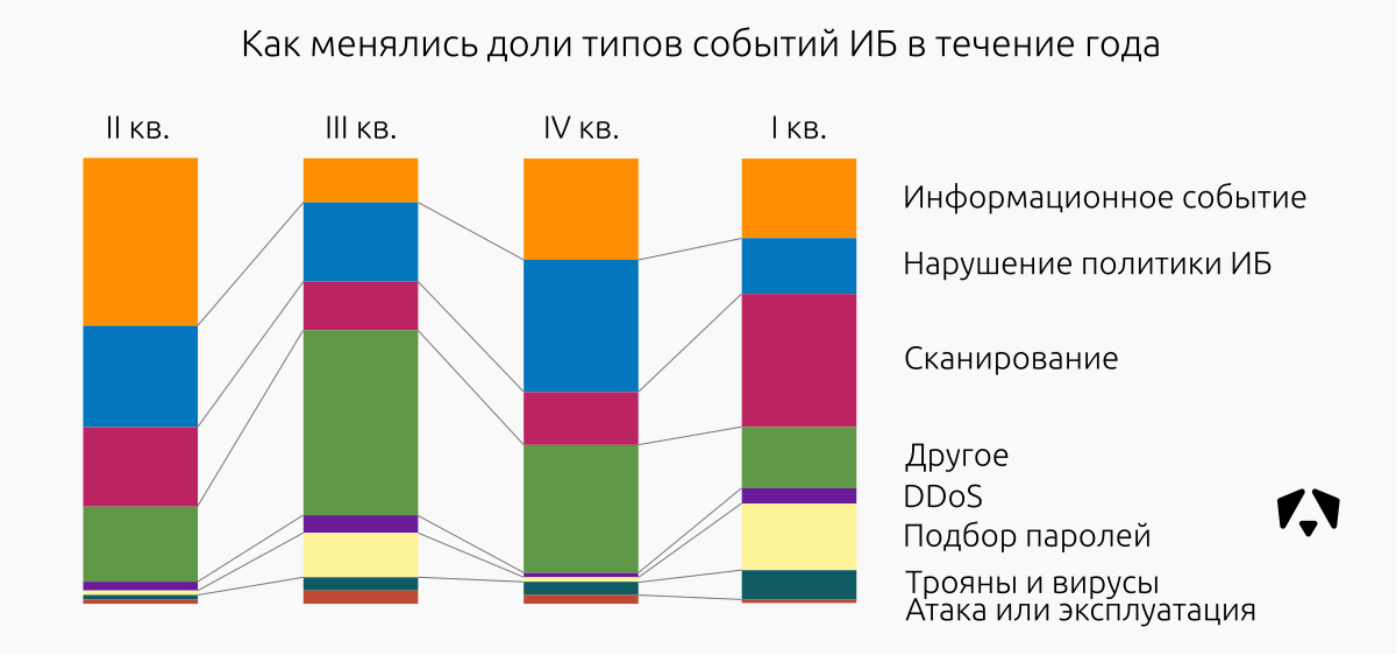
Высокая критичность	Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).
Средняя критичность	Инциденты, связанные с некритичными ресурсами 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 января по 31 марта 2017 года сотрудники Центра мониторинга контролировали информационные системы нескольких организаций с общим числом подключённых узлов около 12 000 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.).

За три месяца сенсоры зафиксировали и проанализировали **137 873 416 событий** информационной безопасности и выявили **98 инцидентов**.



Самое значимое изменение по сравнению с предыдущим периодом — рост доли событий, связанных со сканированием информационных ресурсов и попытками подбора паролей к различным информационным системам. Также немного увеличилась доля событий, связанных с активностью вредоносного ПО.

На рисунке выше показано, как изменялось соотношение типов событий ИБ. Чтобы оценить размер поступающих данных, стоит упомянуть, что «Сканирование» в I квартале 2017 года — это 30% и 41 646 524 зафиксированных события; а «Подбор паролей» — 15% и почти 21 млн. событий.

«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.

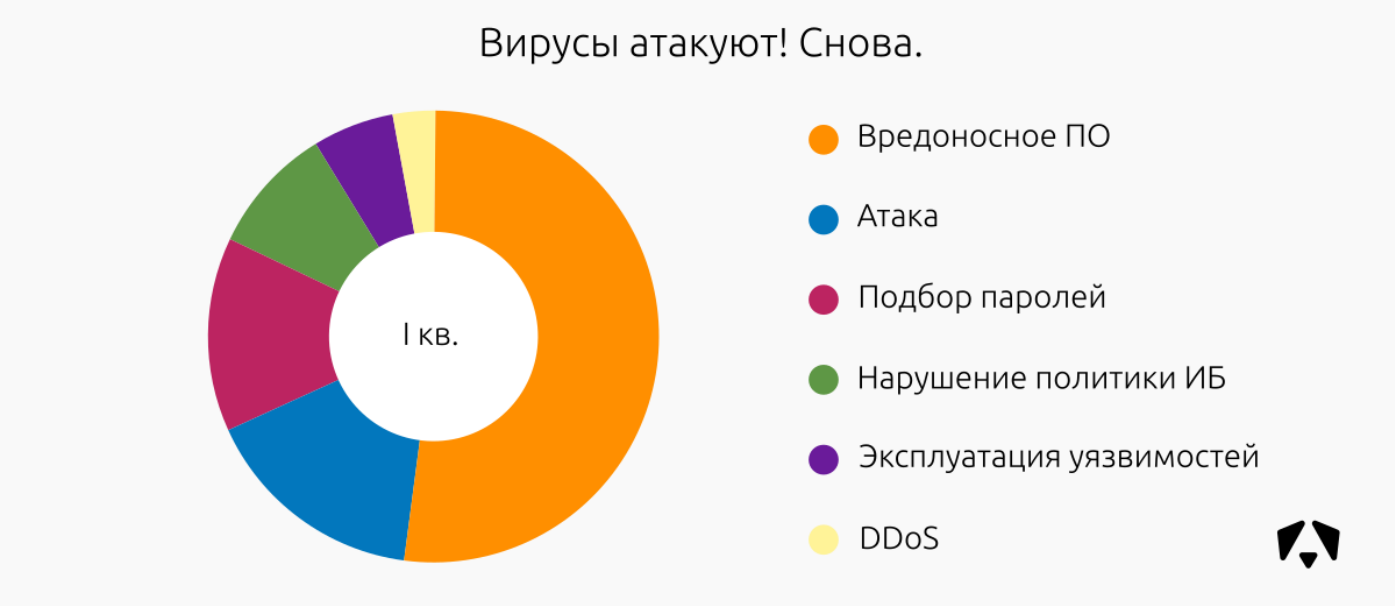
«Трояны и вирусы» — события, свидетельствующие о факте заражения контролируемых ресурсов вирусами или активности вредоносного ПО.

«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 98 инцидентов:

Класс инцидента	Высокая критичность	Средняя критичность	Низкая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО	16	20	15	51	52%
Атака	9	5	1	15	16%
Подбор паролей	11	3		14	14%
Нарушение политики ИБ	2	4	3	9	9%
Эксплуатация уязвимостей	3	3		6	6%
DDoS	3			3	3%
Всего:				98	100,0%



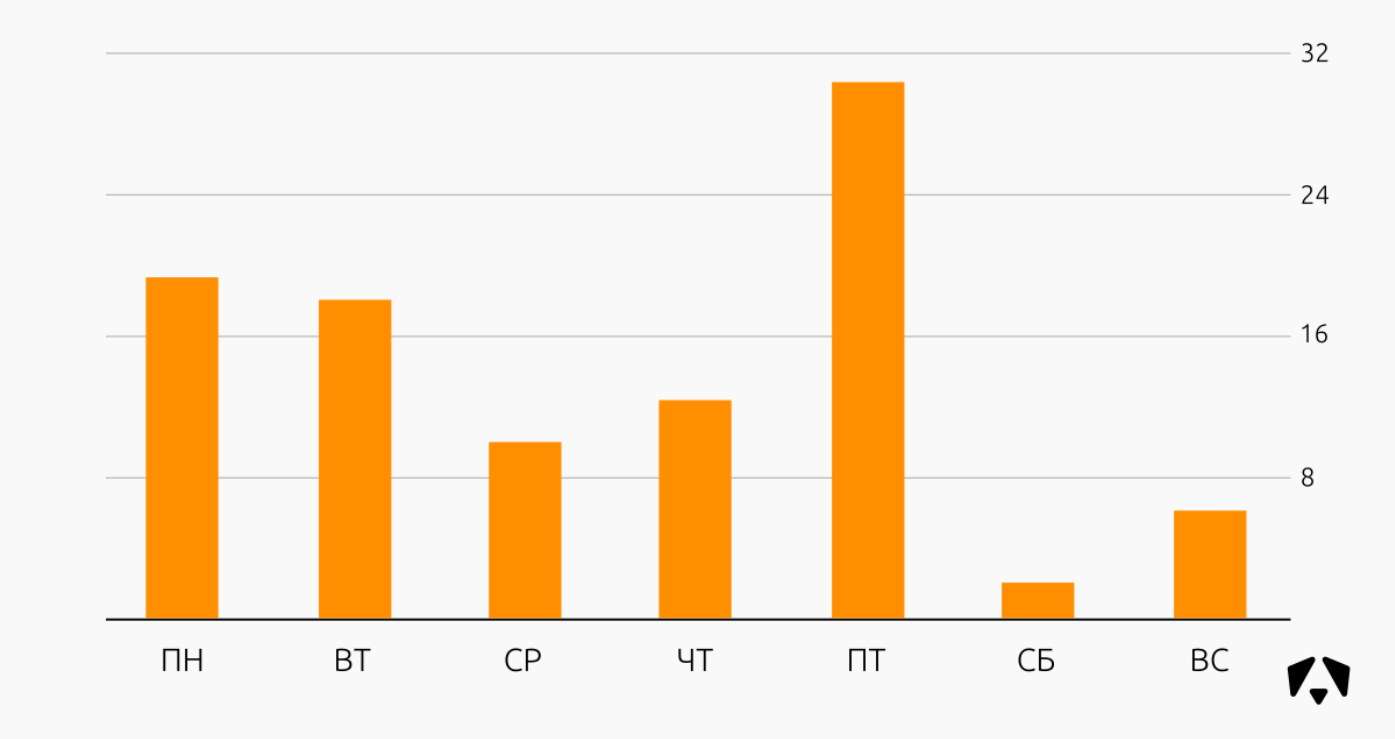
	Доля инцидентов, %			
Класс инцидента	II кв. 2016	III кв. 2016	IV кв. 2016	I кв. 2017
Вредоносное ПО	43,5	42,8	51	52
DDoS	8,7	14,3	1,9	3
Нарушение политики ИБ	30,4	14,3	13,2	9
Подбор паролей	17,4	23,8	13,2	14
Атака			11,3	16
Эксплуатация уязвимостей		4,8	9,4	6

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

Одно интересное наблюдение. Сотрудники часто используют корпоративные ресурсы в своих личных целях: от распечатки доклада ребёнку в школу до доступа в личный интернет-банк. Сейчас же мы столкнулись с тем, что сотрудники майнят bitcoin и ethereum на вычислительных ресурсах организации. Такие инциденты попали в «Нарушение политики».

За предыдущий IV квартал 2016 года Центр мониторинга зафиксировал **21 788 201 событие** ИБ и **53 инцидента**.

Распределение инцидентов ИБ относительно дней недели в I квартале 2017 года:



Распределение инцидентов ИБ за I квартал 2017 года:

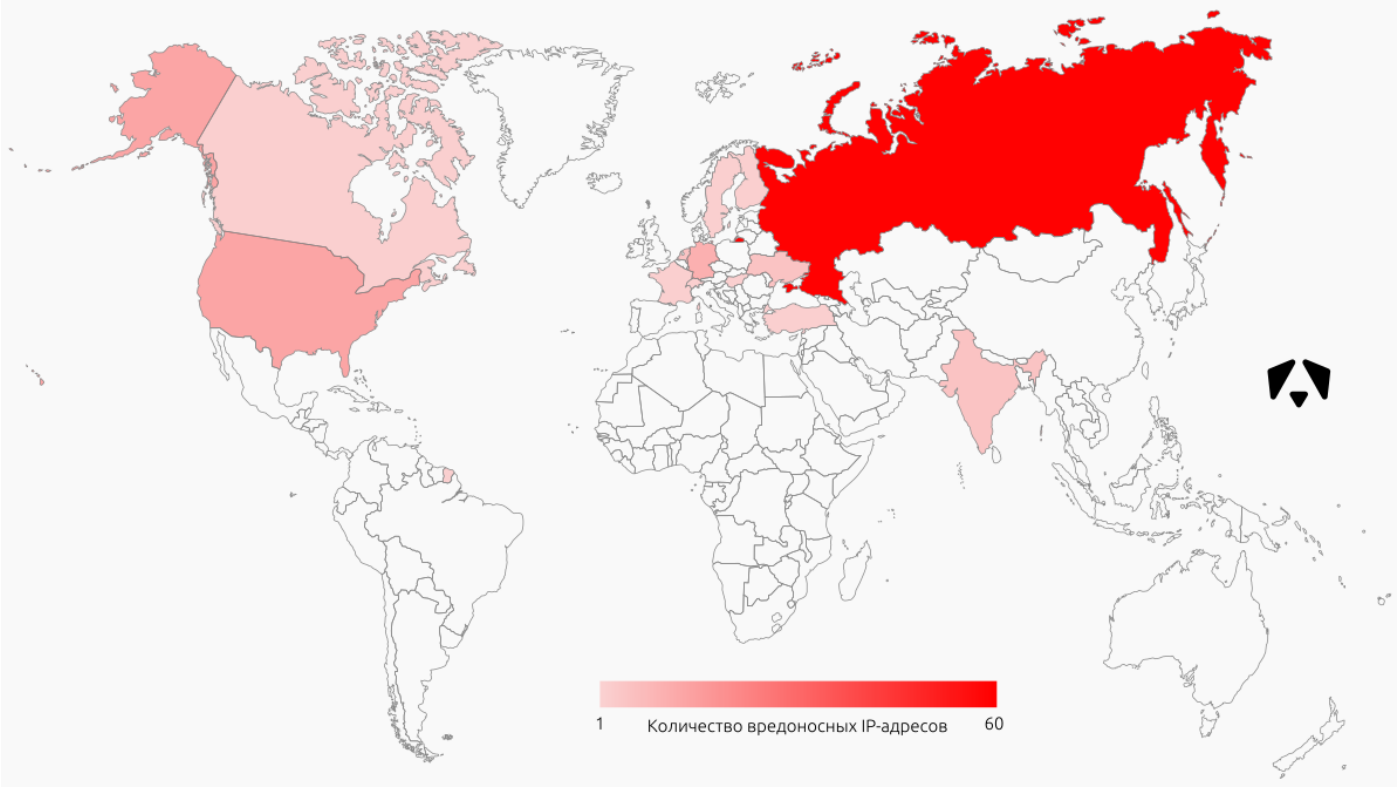
Если внимательно посмотреть на два графика выше, то видно, что «пятничный» пик инцидентов приходится на конкретный день — 17 февраля. В этот день в наш Центр мониторинга стали поступать и обрабатываться события от сети довольно крупной организации, соответственно сразу же стала видна и была зафиксирована в статистике вредоносная активность, уже присутствовавшая в этой сети. Постепенно по мере реагирования на эти инциденты количество новых зафиксированных инцидентов снижалось.

Если исключить этот конкретный день, то большая часть инцидентов приходится на начало недели. Связаны они, в первую очередь, с активностью вредоносного программного обеспечения на рабочих местах сотрудников. Серьёзных негативных последствий для контролируемых информационных систем такие инциденты не несут, но администраторы тратят время на антивирусные проверки, а пользователи в это время не могут полноценно работать.

ТОП источников

Под источниками атак в данном случае понимаются IP-адреса, с которых средства сетевой безопасности зафиксировали негативные действия.

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



Есть одна интересная особенность. Во II и III кварталах 2016 года среди лидеров по количеству IP-адресов, с которых осуществлялись атаки, был Китай. В IV квартале 2016 года и в I квартале 2017 года ситуация очень сильно изменилась — мы не зафиксировали вредоносной активности оттуда. Предполагаем, что злоумышленники перешли на российские прокси.

ТОП подверженных инцидентам сегментов

Ситуация по целям атак изменилась непринципиально: наибольшую активность злоумышленники проявляли в отношении пользовательских рабочих мест. На этот сегмент приходится больше половины всех инцидентов.

Наиболее часто используемые техники воздействия на системы, повлёкшие инцидент ИБ

Угроза	Техника воздействия
Рекламное ПО	Заражение конечной системы, передача на командный сервер информации о пользователе, показ таргетированной рекламы.
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.
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 объема на адрес «отправителя». Используя большое количество ресурсов различных организаций, злоумышленник осуществляет DDoS-атаку на жертву.
Попытки эксплуатации уязвимостей	Использование недостатков в системе для нарушения целостности и нарушения правильной работы системы. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадёжных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.

Deface WEB-ресурсов	Хакерская атака, при которой страницы и важная информация заменяются на другие, как правило вызывающего вида (реклама, предупреждение, угроза, пропаганда) Зачастую, доступ ко всему остальному сайту блокируется, или же прежнее содержимое удаляется.

Предыдущие отчёты

Отчёт за II квартал 2016 года.

Отчёт за III квартал 2016 года.

Отчёт за IV квартал 2016 года.