Отчёт Центра мониторинга ЗАО «ПМ» за второй квартал 2016 года

В данном отчёте мы обобщили информацию о зарегистрированных Центром мониторинга событиях и инцидентах информационной безопасности за второй квартал 2016 года.

Оглавление

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:

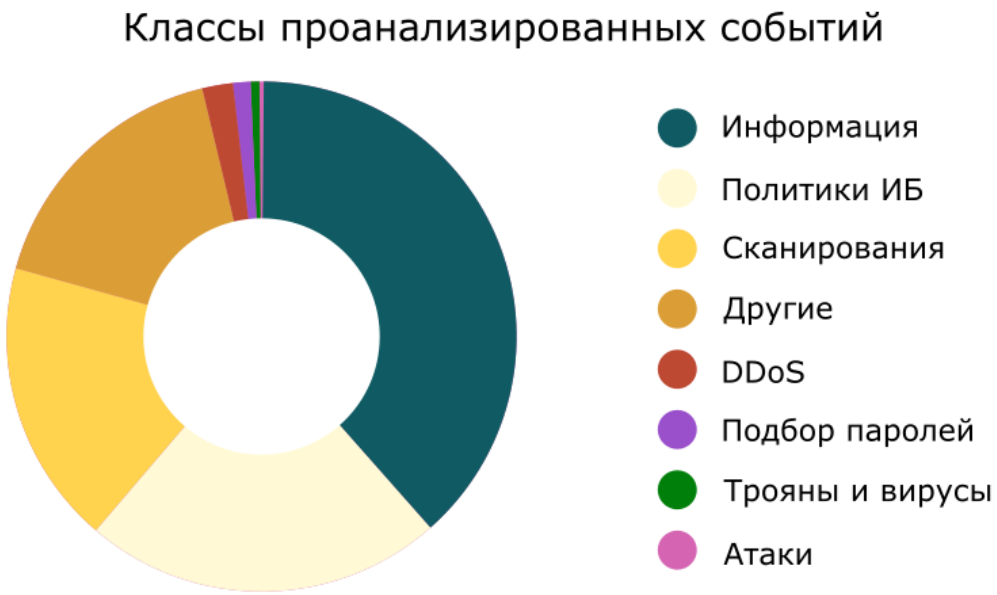
- **Инциденты высокой критичности**. Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).
- **Инциденты средней критичности**. Инциденты, связанные с некритичными ресурсами серверного сегмента.
- **Инциденты низкой критичности**. Инциденты, связанные с некритичными ресурсами пользовательского сегмента (рядовой пользователь).

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

Результаты мониторинга

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

За три месяца сенсоры зафиксировали и проанализировали **150 392 000 событий** информационной безопасности и выявили **23 инцидента**. Отметим, что распределённые атаки на отказ в обслуживании или атаки на перебор паролей вызывают большое количество срабатываний сенсора и генерацию большого количества событий. Например, в рамках одной DDoS-атаки генерируется несколько миллионов событий ИБ.



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

«Сканирования» — события, свидетельствующие о исследовании сети перед попыткой атаки.

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

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

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

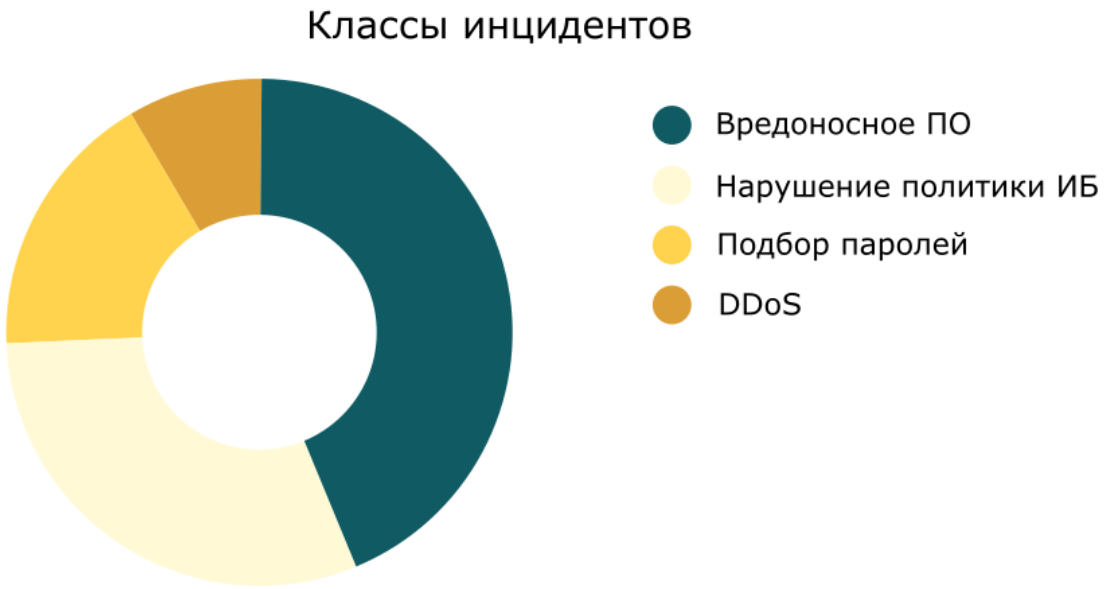
«DDoS» — события, свидетельствующие о попытках осуществления распределённых атак на отказ в обслуживании.

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

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

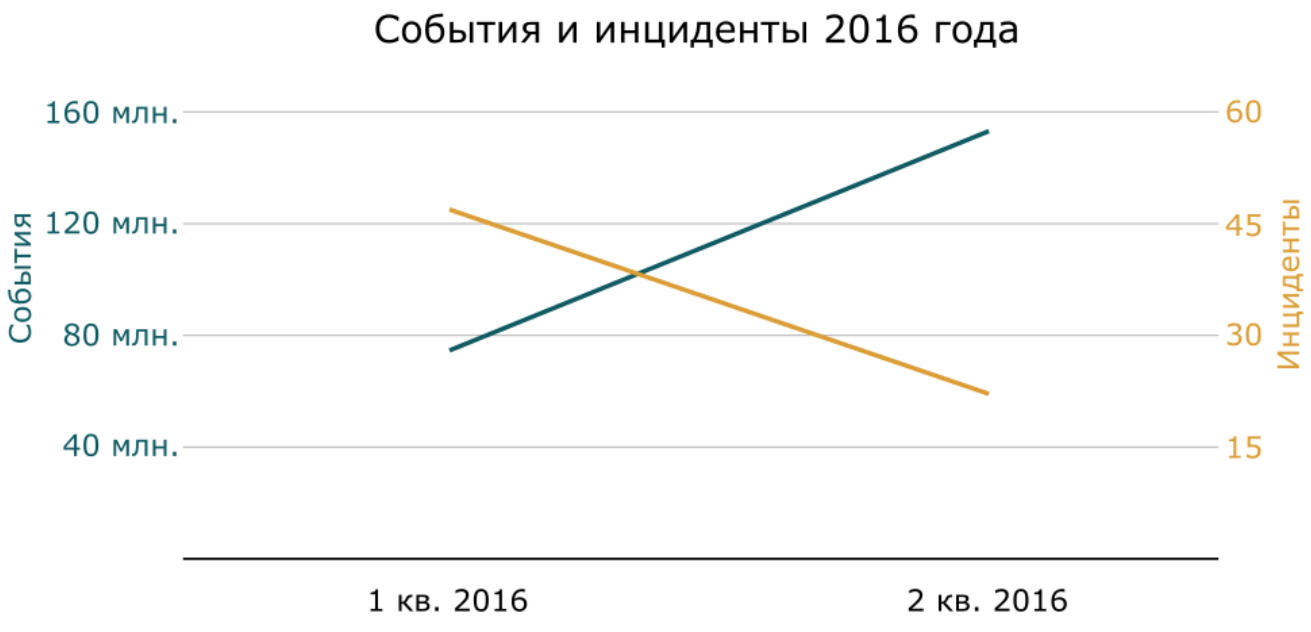
Среди выявленных 23 инцидентов:

Класс инцидента	Высокая критичность	Средняя критичность	Низкая критичность	Всего инцидентов	Доля инцидентов
Вредоносное ПО			10	10	43,5%
DDoS	1	1		2	8,7%
Нарушение политики ИБ			7	7	30,4%
Подбор паролей	2	1	1	4	17,4%
Атака					0,0%
Эксплуатация уязвимостей					0,0%
Всего инцидентов разной критичности:	3	2	18	23	100,0%



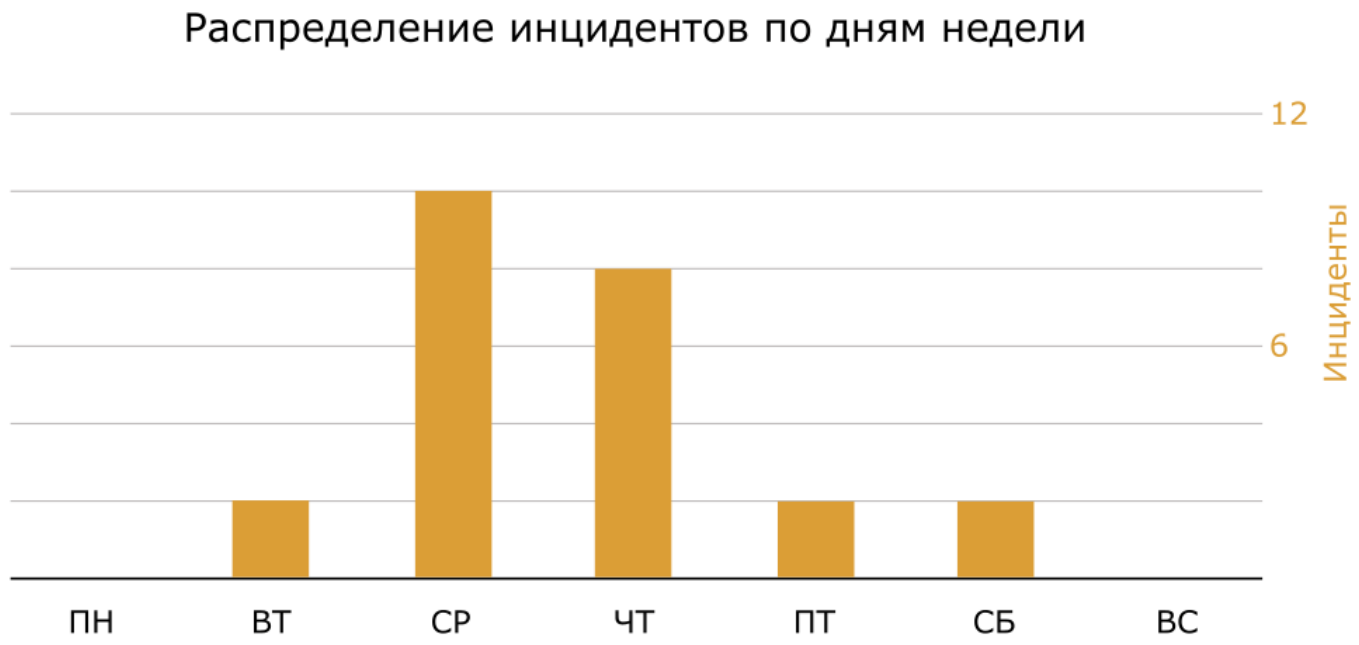
Наиболее актуальными и критичными из выявленных являются атаки, связанные с использованием ресурсов организаций для атак DDoS Amplification.

За предыдущий первый квартал 2016 года Центр мониторинга зафиксировал **75 163 000 событий** ИБ и **47 инцидентов**.



Класс инцидента	Доля инцидентов за 1 квартал 2016, %	Доля инцидентов за 2 квартал 2016, %
Вредоносное ПО	84,6	43,5
Распределённый отказ в обслуживании		8,7
Нарушение политики ИБ	2,6	30,4
Подбор паролей	5,1	17,4
Атака	7,7	
Эксплуатация		

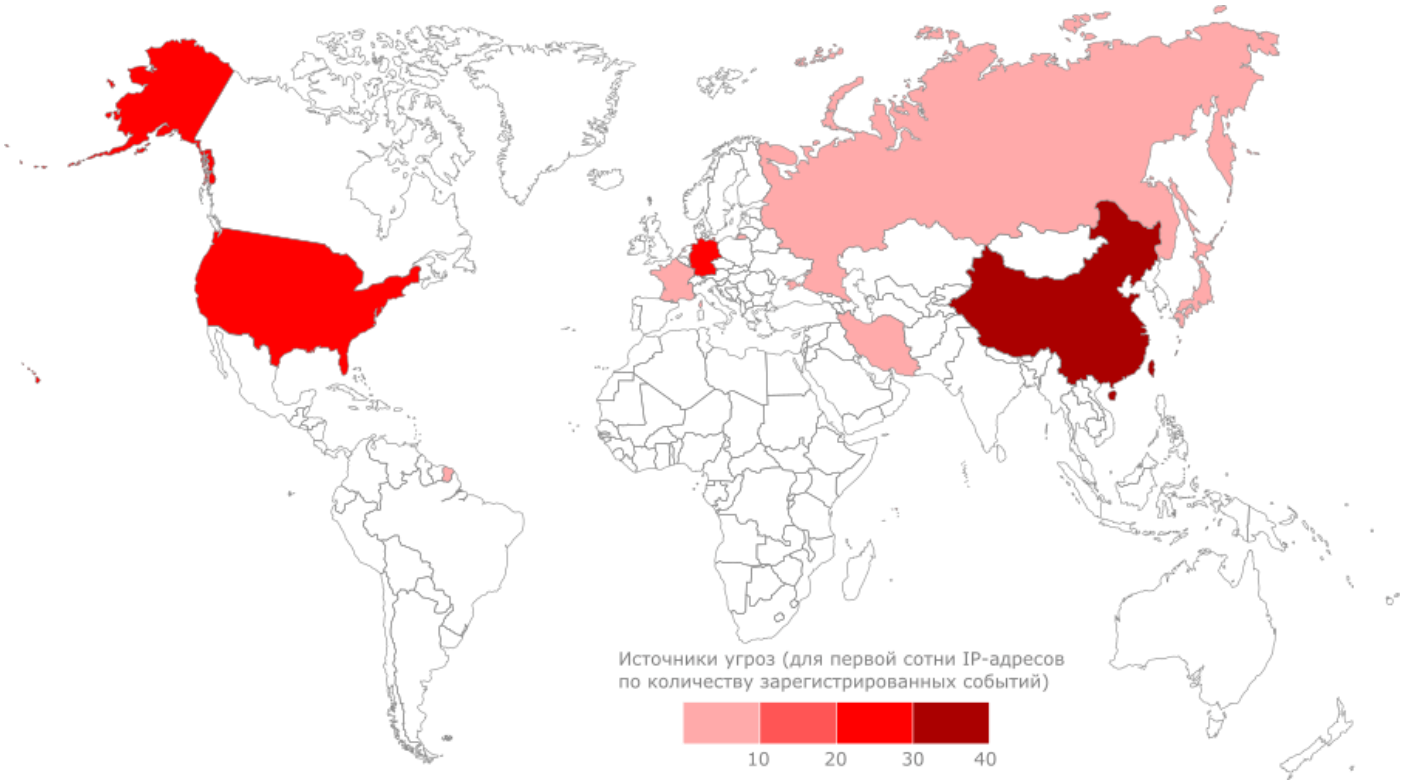
Распределение инцидентов ИБ относительно дней недели во втором квартале 2016 года:



Наибольшее количество инцидентов ИБ наблюдается в середине недели. Именно в среду и четверг сотрудники (пользовательские АРМ становились объектами атак в половине всех случаев) чаще всего посещают сомнительные с точки зрения безопасности развлекательные сайты и получают вредоносную «нагрузку».

Распределение инцидентов ИБ за второй квартал 2016 года:

ТОП источников



ТОП подверженных инцидентам сегментов

Наибольшую активность злоумышленники проявляли в отношении пользовательских рабочих мест и web-серверов. Это не удивительно, потому что именно эти сегменты проще всего атаковать.

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.
ПО для удалённого управления	Организация удалённого доступа к рабочему месту жертвы. Может использоваться в системе без ведома пользователя.
Перебор паролей	Попытки подбора аутентификационной информации для доступа к сервисам и ресурсам контролируемых организаций — RDP, SSH, SMB, DB, Web.
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 объема на адрес «отправителя». Используя большое количество ресурсов различных организаций, злоумышленник осуществляет DDoS-атаку на жертву.