Второй ежеквартальный отчет:

JSOC Security flash report 2014 Q4

Оглавление

Отчет JSOC Security flash report 2014 Q4 основан на данных, полученных в коммерческом центре мониторинга и реагирования на инциденты ИБ JSOC.

Это второй ежеквартальный отчет, подготовленный командой JSOC. В отчете приведены данные за четвертый квартал 2014 года в сравнении с двумя предыдущими кварталами.

Отчет предназначен для информирования служб ИТ и ИБ об основных трендах, касающихся угроз информационной безопасности.

Ключевые изменения в Q4:

01 В четвертом квартале зафиксирован существенный рост количества инцидентов, связанных с деятельностью внутренних пользователей. Основной рост наблюдается по инцидентам, связанным с утечками конфиденциальной информации.

02 В четвертом квартале значительно ускорилось погружение пользователей в «серую зону» интернета. Выросла популярность систем, маскирующих или скрывающих деятельность сотрудников.

03 По сравнению с предыдущим отчетным периодом наблюдается снижение доли ночных инцидентов в общей массе. Одной из основных причин этого является существенный прирост доли внутренних инцидентов.

04 Продолжается устойчивый рост процент атак, направленных на онлайн веб-сервисы, как на уровне веб-уязвимостей и управляющих служб, так и DoS-атак.

E-mail: is@jet.su
Тел.:+7 (495) 411-7601

Методология

Общие положения

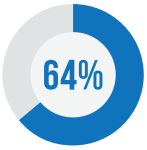
JSOC Security flash report является сводным материалом по анализу инцидентов, выявленных командой JSOC как при оказании регулярных услуг по мониторингу и реагированию на инциденты, так и в ходе консультативно-аналитической поддержки компаний российского рынка в рамках разовых обращений.

Деление инцидентов по категориям и типам угроз основано на внутренней классификации и методологии самого JSOC. Отчет является только информативным материалом и не претендует на то, что приведенные данные полностью отражают все угрозы российского рынка. Команда JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации.

Сводная статистика по JSOC

83 554

Всего за 2014 год в JSOC было зафиксировано 83 554 события с подозрением на инцидент, из них 29 278 событий – в Q4.



64% исследуемых событий зафиксировано при помощи основных сервисов инфраструктуры и базовой безопасности: межсетевых экранов и сетевого оборудования, VPN, AD, почтовых серверов, базовых средств защиты (антивирусы, прокси-серверы, IPS).

Оставшиеся инциденты, выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации и имеют высокую степень критичности для информационной и экономической безопасности клиента. Мониторинг JSOC позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные таргетированные инциденты.

Классификация инцидентов по критичности

Основным критерием при классификации инцидентов по критичности является воздействие инцидента на ключевые бизнес-процессы и данные заказчика. Инцидент считается критичным, если в его результате возможны и высоковероятны следующие события:

- длительное прерывание (более получаса) или остановка функционирования систем и сервисов клиента, относящихся к категориям Business и Mission Critical;
- повреждение, потеря или компрометация критичных сегментов данных и учетных записей, включая относящиеся к коммерческой и банковской тайне;
- прямые финансовые потери более 1 млн рублей в результате действий внутренних сотрудников или киберпреступников.

Коротко о JSOC

JSOC – первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ и управления информационной безопасностью. JSOC предоставляет сервисы:

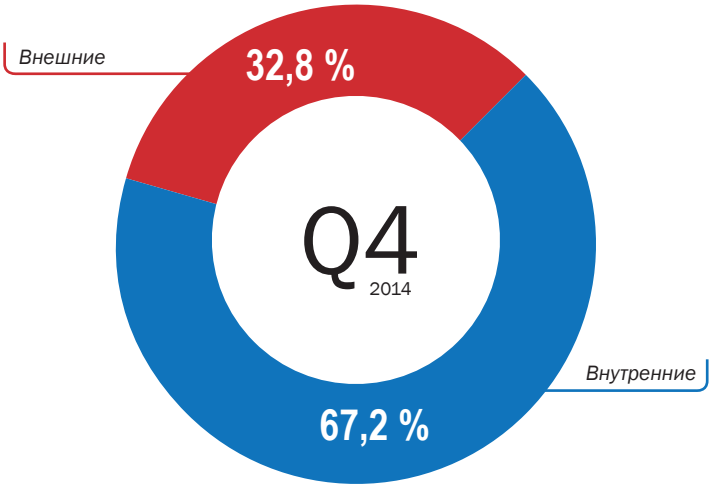
- *мониторинг, реагирование и противодействие инцидентам информационной безопасности;*
- *контроль защищенности ключевых информационных систем компании;*
- *защита компании от DDoS-атак;*
- *управление ключевыми ИБ-системами компании.*

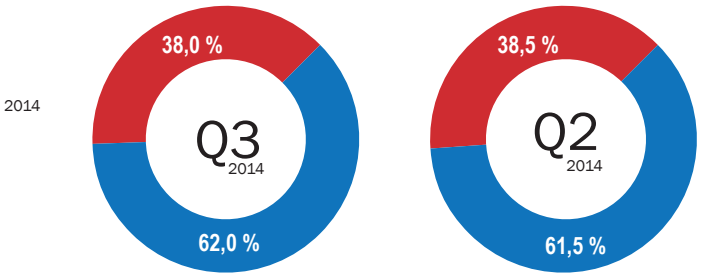
*В состав JSOC входят исследовательская лаборатория по анализу и прогнозированию инцидентов ИБ и несколько дежурных смен, которые работают 24*7: часть смен занимается мониторингом и разбором инцидентов, остальные – администрированием систем. Все сервисы JSOC предоставляются с гарантированным уровнем SLA, соответствующим лучшим международным практикам.*

На данный момент JSOC в круглосуточном режиме контролирует порядка 300 стандартных и более 170 собственных и постоянно пополняемых сценариев обнаружения атак, разработанных для компаний различных отраслей российского рынка.

Общие показатели по инцидентам

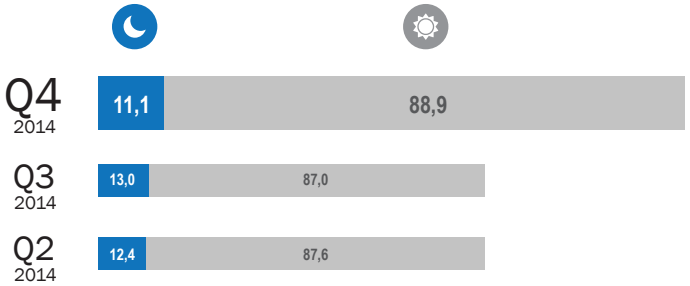
Распределение инцидентов по внешним и внутренним [1]



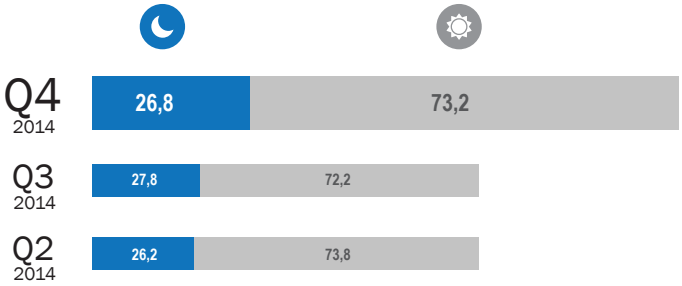


Распределение инцидентов по времени суток

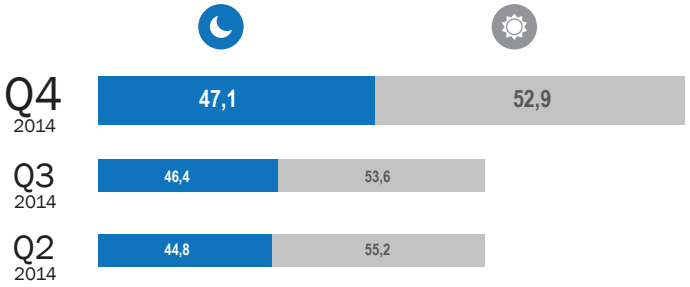
Общее распределение по времени суток (в %):



Распределение по критичным инцидентам (в %):



Распределение по критичным внешним инцидентам (в %):



Ночь
С 21:00 до 08:00 по времени расположения офиса заказчика

День
С 08:00 до 21:00 по времени расположения офиса заказчика

Итоговая картина демонстрирует:

по сравнению с предыдущим отчетным периодом наблюдается снижение доли ночных инцидентов в общей массе. Одной из основных причин этого является существенный прирост доли внутренних инцидентов: злонамеренные активности, инициируемые или являющиеся результатом деятельности пользователей, чаще всего происходят в дневное время. При этом по сегменту внешних атак продолжается устойчивый рост процента ночных инцидентов.

[1] К внутренним пользователям-инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты.

Внешние инциденты

В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся внутренними пользователями клиента JSOC. Из отчета исключены действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не приводящие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей.

Направления атак в %-ном соотношении от общего числа:

Особенности внутренних инцидентов в четвертом квартале

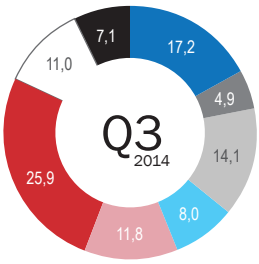
- 27% веб-инцидентов в четвертом квартале связаны с эксплуатацией уязвимости Shellshock;
- более 40% зафиксированных DDoS-атак были направлены сразу на несколько организаций.

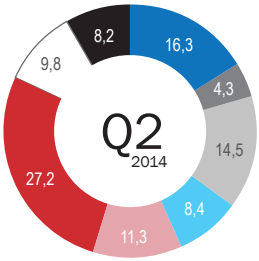
Статистика четвертого квартала подтверждает устойчивый рост процента атак, направленных на онлайн веб-сервисы. Злоумышленники используют уязвимости на уровне веб-приложений и управляющих служб, а также DoS-атаки.

Внутренние инциденты

В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников клиентов JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, компрометация или передача учетных данных сотрудников, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование систем клиента.

Направления атак в %-ном соотношении от общего числа:



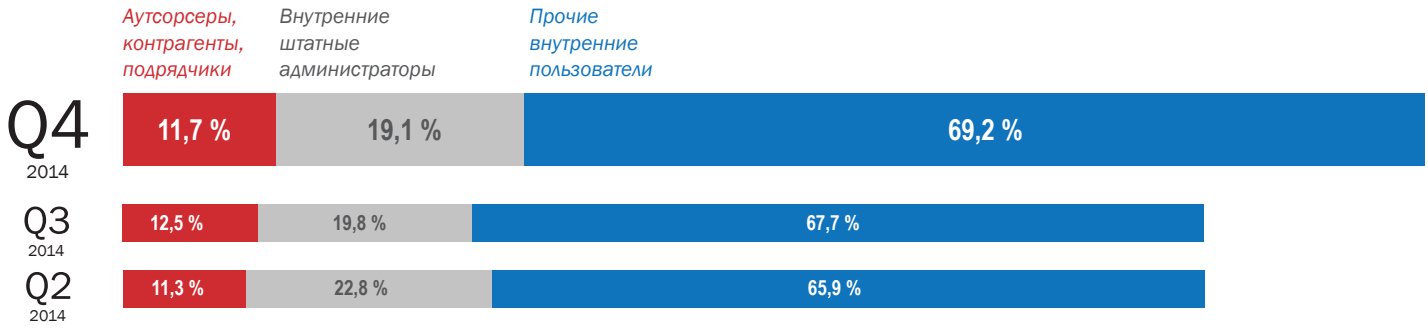


Особенности внутренних инцидентов:

• около 8% сотрудников ИТ-департамента используют утилиты удаленного администрирования как альтернативное средство доступа в сеть компании;
• более 45% случаев утечки конфиденциальных данных в четвертом квартале произошли в декабре.

Стоит отметить существенный рост инцидентов, связанных с утечками конфиденциальной информации. В рамках картины, наблюдаемой в начале 2015 года, можно прогнозировать последующее увеличение данного типа инцидентов.

Инициаторы внутренних инцидентов



E-mail: is@jet.su
Тел.:+7 (495) 411-7601