JSOC Security flash report
2014 Q3

Оглавление

Отчет JSOC Security flash report 2014 Q3 основан на данных, полученных в коммерческом центре мониторинга и реагирования на инциденты ИБ JSOC. Это первый отчет, подготовленный командой JSOC: в нем приведены данные за третий квартал 2014 года в сравнении с двумя предыдущими кварталами. В дальнейшем планируется выпуск данного отчета на ежеквартальной основе.

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

Ключевые выводы и тенденции:

01

За первые три квартала 2014 года наблюдается устойчивая тенденция по увеличению доли критичных для компании инцидентов в ночное время.

По нашим оценкам, уже к середине 2015 года именно на ночное время будет приходиться более половины критичных инцидентов.

02

Существенно растет использование систем, маскирующих или скрывающих деятельность в интернете, в том числе TOR, как внутренними сотрудниками, так и внешними злоумышленниками.

03

Статистика JSOC подтверждает отмечаемую многими исследователями тенденцию по постепенному смещению внешних атак на прикладной уровень.

04

Выявлен существенный прирост внешних и внутренних целенаправленных атак на бизнес-системы компаний, целью которых является получение прямой финансовой выгоды.

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

54 276

Всего за первые три квартала 2014 года в JSOC было зафиксировано 54 276 событий с подозрением на инцидент, из них 18 858 событий – в Q3;

56% исследуемых событий зафиксировано при помощи основных сервисов инфраструктуры и базовой безопасности: межсетевые экраны и сетевое оборудование, VPN, AD, почтовые серверы, базовые средства 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, что 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 результате него 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 суммой более 1 млн рублей в результате действий внутренних сотрудников или киберпреступников.

Коротко о JSOC

Jet Security Operations Center (JSOC) – первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ и управления информационной безопасностью.

Центром JSOC предоставляются сервисы:

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

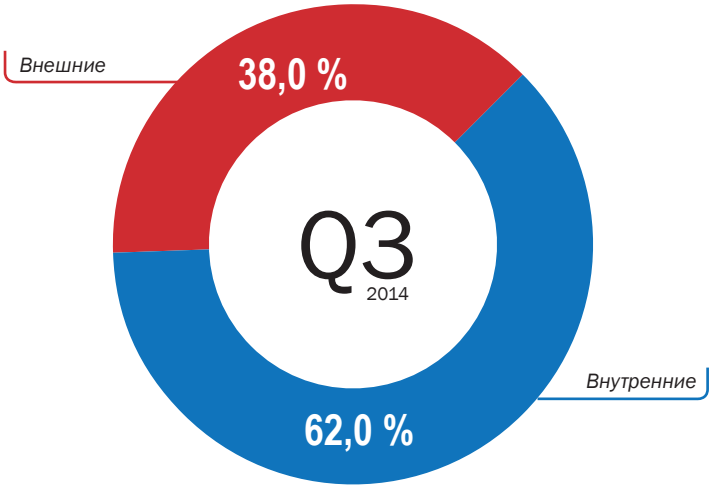
*В состав JSOC входят несколько дежурных смен, которые работают 24*7: часть смен занимается мониторингом и разбором инцидентов, остальные – администрированием систем. Все сервисы JSOC предоставляются с гарантированным уровнем SLA, соответствующим лучшим международным практикам.*

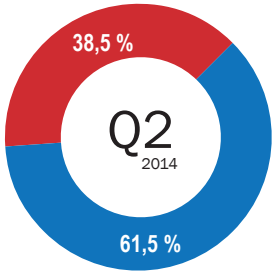
На данный момент JSOC в круглосуточном режиме контролирует более 170 различных сценариев выявления инцидентов.

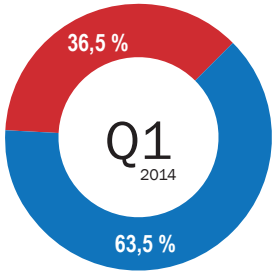
E-mail: is@jet.su
Тел.:+7 (495) 411-7601

Общие показатели по инцидентам

Распределение инцидентов по внешним и внутренним [1]

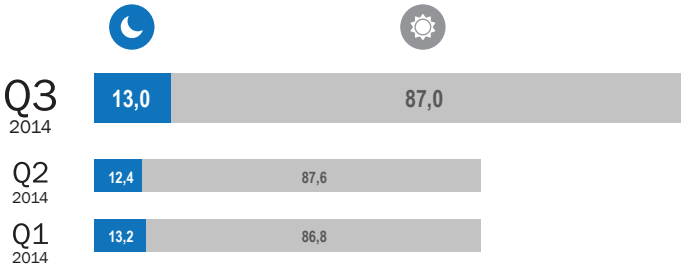




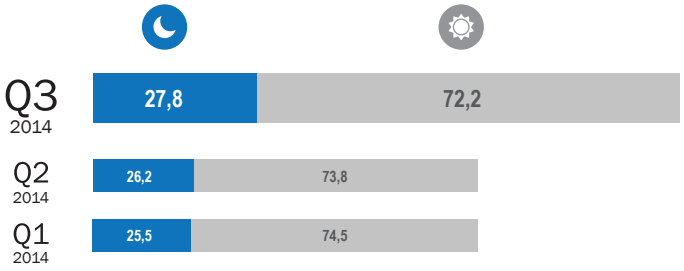


Распределение инцидентов по времени суток

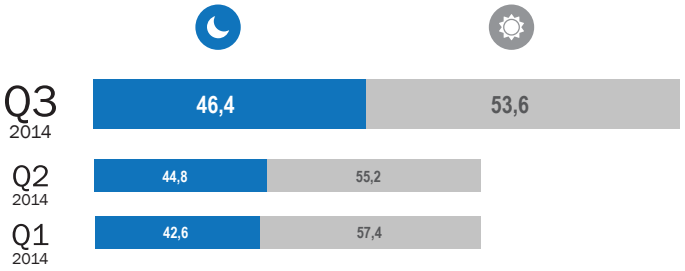
Общее распределение по времени суток (в %):



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:

несмотря на то, что максимальный объем событий, требующих внимания офицера ИБ, происходит в дневное время и может быть успешно разобран в достаточно короткие сроки, акцент по наиболее болезненным для компании инцидентам смещается на ночное время и те часы, когда сотрудники, ответственные за информационную безопасность, не могут реагировать с должной скоростью. Особенно ярко эта тенденция видна на внешних атаках, относящихся к действиям злоумышленников и киберпреступников.

[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 третьем квартале

- 7 из 8 успешных эксплуатаций уязвимостей своей целью ставят подсадку управляющего бота;
- 11 из 15 DDoS-атак направлены на приложение, а не на интернет-канал;
- 15 из 19 атак направлены с TOR-адресов.

Статистика показывает постепенное смещение внешних атак на прикладной уровень. Одной из причин этого является существенное увеличение количества внешних ресурсов и веб-сервисов в компаниях практически всех отраслевых сегментов. При этом уровень собственной защищенности приложений, к сожалению, существенно уступает возможностям злоумышленников.

Вывод и прогнозы

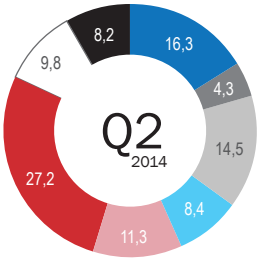
- Внешние атаки становятся все более изощренными и все чаще носят таргетированный характер.
- Основной целью атак является не снижение доступности или нарушение целостности систем, а получение прямой финансовой выгоды (хищение денежных сумм из бизнес-систем клиентов).

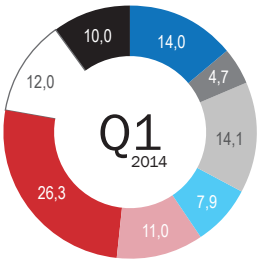
E-mail: is@jet.su
Тел.:+7 (495) 411-7601

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:



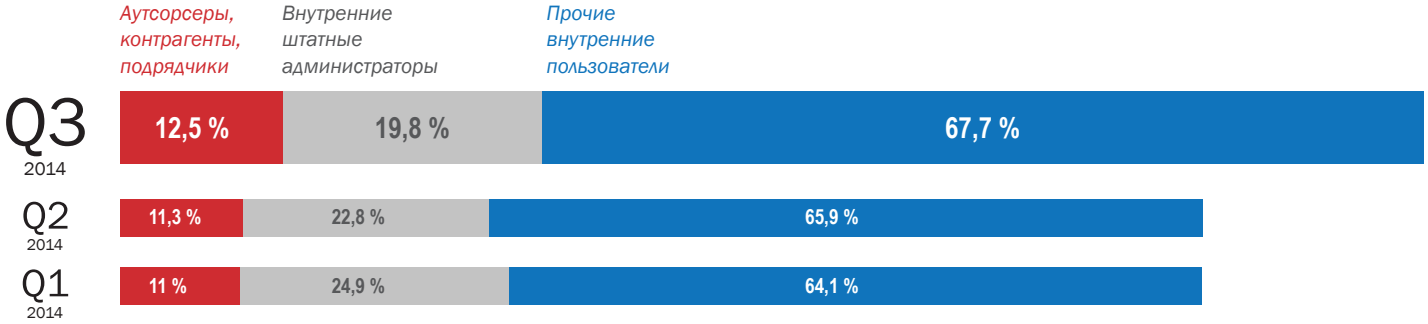


Особенности внутренних инцидентов в третьем квартале

- 22% инцидентов с доступом в интернет связано с использованием TOR-сетей;
- В компаниях с внедренной парольной политикой инцидентов с учетными записями на 76% меньше;
- Около 4% сотрудников ИТ-департамента средней компании являются регулярными посетителями хакерских форумов.

Существенных изменений в распределении внутренних инцидентов за время сбора информации по отчетам JSOC не установлено. Текущая динамика позволяет прогнозировать несущественное колебание показателей в течение следующих двух варталов.

Инициаторы внутренних инцидентов



Вывод и прогнозы

- Существенно растет процент внутренних инцидентов, связанных не с халатностью сотрудников, а с прямым злым умыслом и финансовой мотивацией.
- Идет рост погружения пользователей клиентов JSOC в «серую зону» интернета и растет популярность систем, максирующих или скрывающих деятельность пользователей.

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