JSOC Security flash report Q4 2015

Отчет **JSOC Security flash report Q4 2015** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC[1] за четвертый квартал 2015 года. В документе отражена сводная информация о выявленных инцидентах по различным категориям, отвечающая на вопрос о том, кто, как, в какое время и с использованием каких векторов и каналов утечки реализовывал угрозы ИБ.

Отчет предназначен для информирования служб ИТ и информационной безопасности о текущем ландшафте угроз и основных трендах.

Оглавление

Ключевые выводы

1. По характеру внешних инцидентов отмечается рост числа кибергруппировок, работающих по уже известным схемам мошенничества.
2. Доля критичных ночных инцидентов росла на протяжении всего 2015 года. С 26,8% в Q4 2014 года до 31,4% в Q4 2015 года. Это подтверждает необходимость мониторинга.
3. Возрастает процент инцидентов по утечкам конфиденциальных данных, связанных с умышленными нарушениями политики ИБ пользователями.
4. В течение всего 2015 года наблюдается уверенный рост числа DDoS атак. Связано это с ростом конкуренции и бизнес-активности, нарастающих к концу года.

[1]ссылка - http://solarsecurity.ru/products/jsoc

info@solarsecurity.ru
+7 (499) 755-0770

Общие положения

«Статистика угроз» является сводным материалом и результатом анализа инцидентов, выявленных командой Solar JSOC как в рамках оказания своих регулярных услуг мониторинга и реагирования на инциденты, так и консультативно-аналитической поддержки компаний российского рынка. Деление инцидентов по категориям и типам угроз основано на внутренней классификации и методологии самого Solar JSOC. Отчет является только информативным материалом и не претендует на то, что приведенные данные полностью отражают все угрозы российского рынка. Команда Solar JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации.

Сводная статистика за отчетный период

- Всего за четвертый квартал 2015 года в Solar JSOC было зафиксировано **51 412 событий** с подозрением на инцидент, в то время как в прошлом аналогичном периоде Q4 2014 года их количество составляло только **29 278**. Прирост за год составил **76%**, что обусловлено подключением новых клиентов к сервисам Solar JSOC в 2015 году.
- В четвертом квартале 2015 года доля критичных инцидентов составила **12,4%**, что существенно выше аналогичного показателя в Q3 2015 года, равного **8,2%**.
- Среднее время принятия инцидента в работу специалистом JSOC с момента выявления составило **20,2 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций Заказчику по критичным инцидентам составило **24,1 минуты** и **93,6 минут** по всем остальным с момента возникновения инцидента.
- Соблюдение клиентских SLA за четвертый квартал 2015 года составило **99,1%**. Данная метрика постоянно поддерживается на высоком уровне, и не опускалась ниже 98,3% за весь 2015 год.
- **61,2%** исследуемых событий зафиксировано при помощи основных сервисов инфраструктуры и базовой безопасности: межсетевые экраны и сетевое оборудования, VPN, AD, почтовые серверы, базовые средства защиты (антивирусы, прокси-серверы, IPS).
- При этом стоит отметить, что оставшиеся инциденты **(38,8%)**, выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации и критичность для информационной и экономической безопасности клиента, что позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные, третированные инциденты.

Классификация инцидентов по критичности

Основным критерием при классификации инцидентов по критичности является воздействие инцидента на ключевые бизнес-процессы и данные компании-клиента.

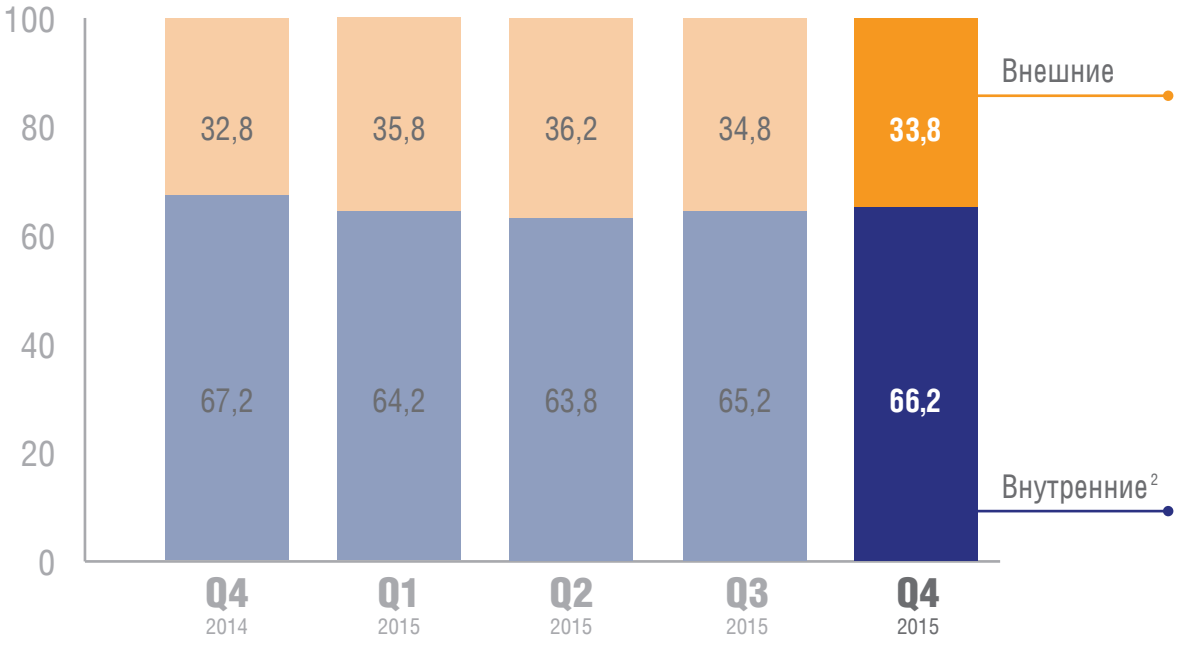
Инцидент считается критичным, если в результате него возможны и высоковероятны следующие события:

- Длительное прерывание (более получаса) или остановка функционирования систем и сервисов клиента, относящихся к категориям Business и Mission Critical.
- Повреждение, потеря или компрометация критичной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам.
- Прямые финансовые потери в результатах действия внутренних сотрудников или киберпреступников суммой более 1 млн рублей.

Общие показатели по инцидентам

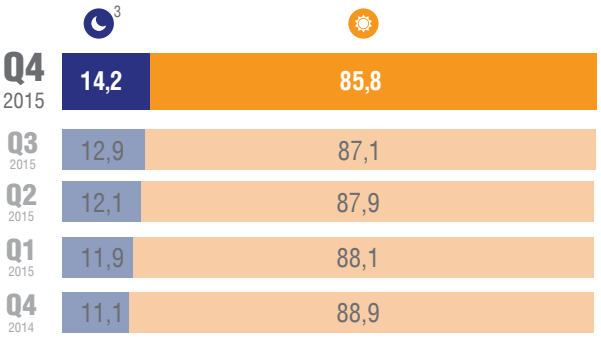
Q4 2015

Распределение инцидентов по внешним и внутренним

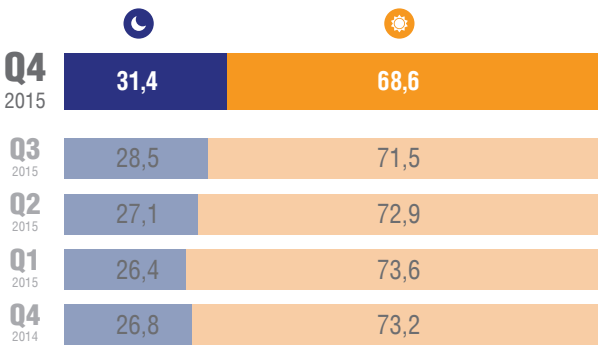


Распределение количества инцидентов по времени суток

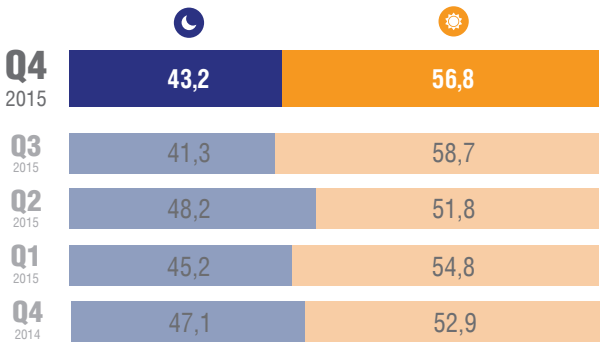
Время суток:



Распределение по критичным инцидентам:



Распределение по критичным внешним инцидентам:



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

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

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

[3] С 21:00 до 08:00 утра по времени расположения офиса и присутствия специалистов информационной безопасности Заказчика.

Общие показатели по инцидентам

За прошедший 2015 год существенно выросло количество инцидентов, регистрируемых 1-ой линией дежурной смены Solar JSOC в ночное время. Если в четвертом квартале 2014 года их было только 11,1% от общего числа, а именно 3 250 инцидентов, то в аналогичном периоде 2015 года их доля выросла до 14,2% или 7300 соответственно. Увеличение потока ночных инцидентов в 2,24 раза потребовало численного и методологического усиления дежурных линий и аналитического отдела департамента Solar JSOC для сохранения высокого уровня соблюдения клиентских SLA.

Если рассматривать только критичные ночные инциденты, то их доля на протяжении всего 2015 года росла. Так, в Q4 2014 года их было 26,8% от общего числа критичных инцидентов, а в Q4 2015 года уже 31,4%, что в абсолютных числах составляет 2001 инцидент. Как и отмечалось в предыдущем отчете за Q3 2015, такой тренд является сезонным и связан с повышением к концу года активности внешних легитимных категорий пользователей, таких как подрядчики, разработчики, службы эксплуатации и аутсорсеры. По мнению аналитиков Solar JSOC, ожидается незначительное снижение доли ночных критичных инцидентов в Q1 2016 года.

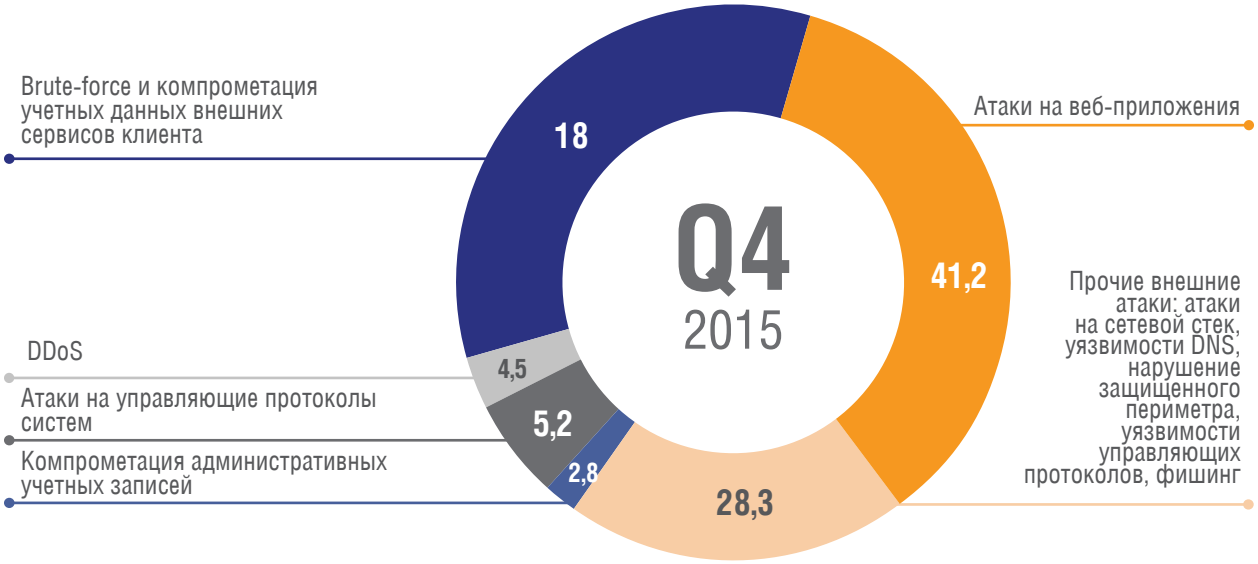
Внешние инциденты

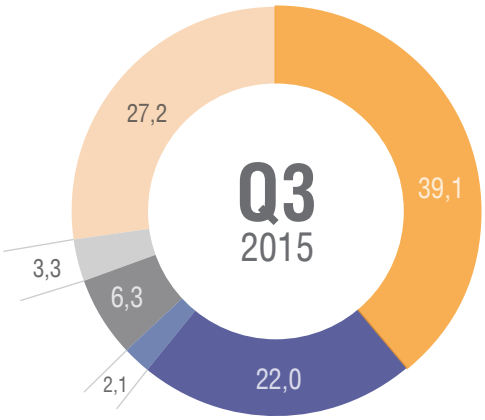
Q4 2015

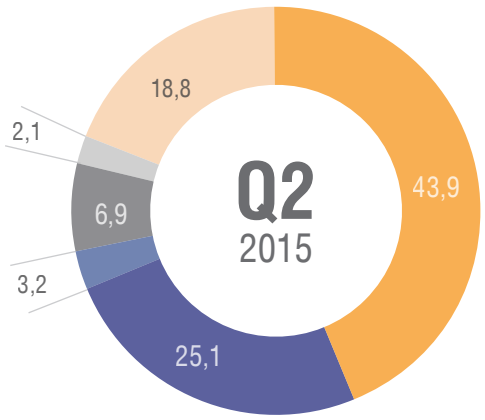
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся внутренними пользователями клиента.

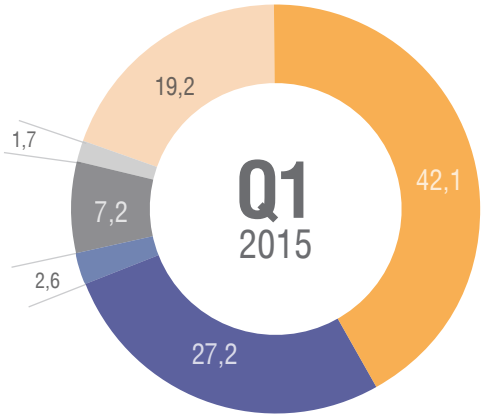
«Простые атаки», а именно действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не влекущие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей - из отчета исключены.

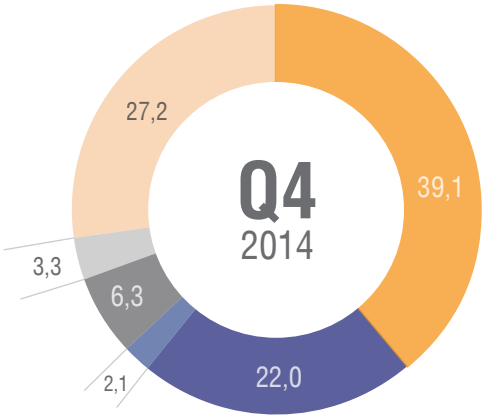
Направления атак в %-ном сообношении от общего числа











Особенности внешних инцидентов в четвертом квартале 2015г.:

- Вектор основных внешних атак на инфраструктуры компаний-клиентов Solar JSOC по-прежнему направлен на использование уязвимостей web-приложений и подбор паролей к внешним сервисам. Их совокупная доля значительно увеличилась с 61,1% до 69,5% по сравнению с аналогичным периодом в 2014 году.

- В течение всего 2015 года наблюдается уверенный рост числа DDoS атак. По мнению аналитиков Solar JSOC, связано это с ростом влияния конкуренции и бизнес-активности, обычно нарастающих к концу календарного года.

- Почти на 10% снизилась доля прочих внешних атак, требующих хорошей технической подготовки и творческого подхода к реализации угрозы.

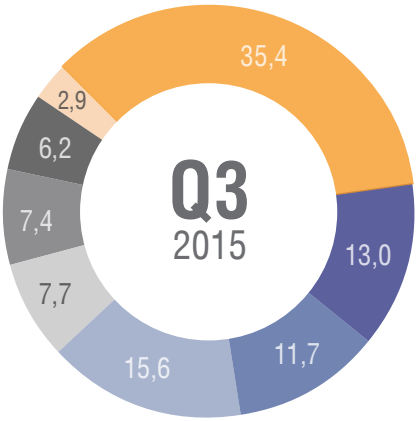
Увеличение числа атак на web-приложения и внешние сервисы при снижении количества прочих внешних атак, таких как атаки на управляющие протоколы, фишинг, использование уязвимостей сетевого стека протоколов и т.п., может говорить с одной стороны о росте числа преступных группировок, а с другой – об их относительно слабой технической подготовке по состоянию на Q4 2015. На протяжении 2016 года аналитиками Solar JSOC ожидается сохранение тренда по атакам на web-приложения и повышение сложности внешних атак со стороны новых хакерских групп.

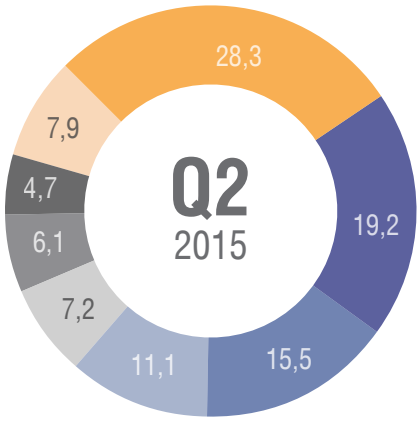
Внутренние инциденты

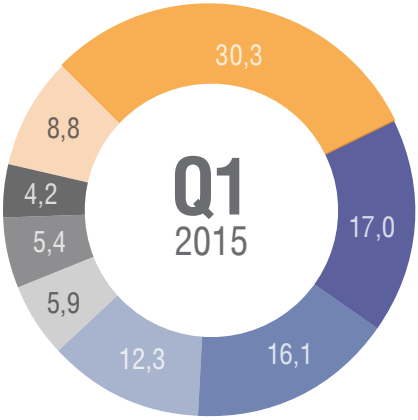
Q4 2015

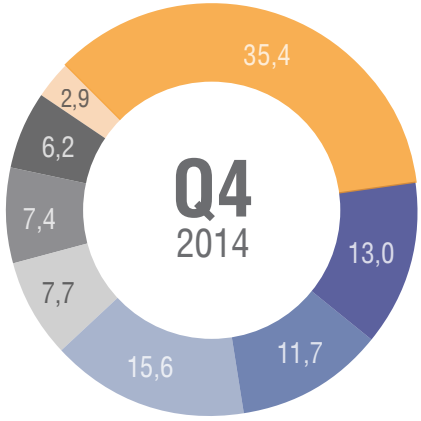
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников клиентов Solar JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных данных сотрудников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

Направления атак в %-ном сообношении от общего числа





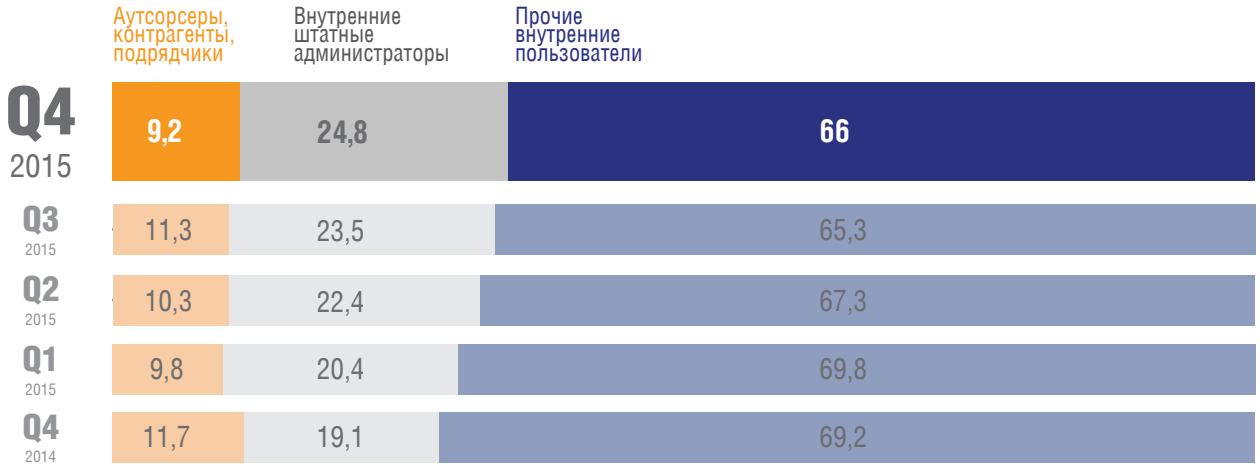




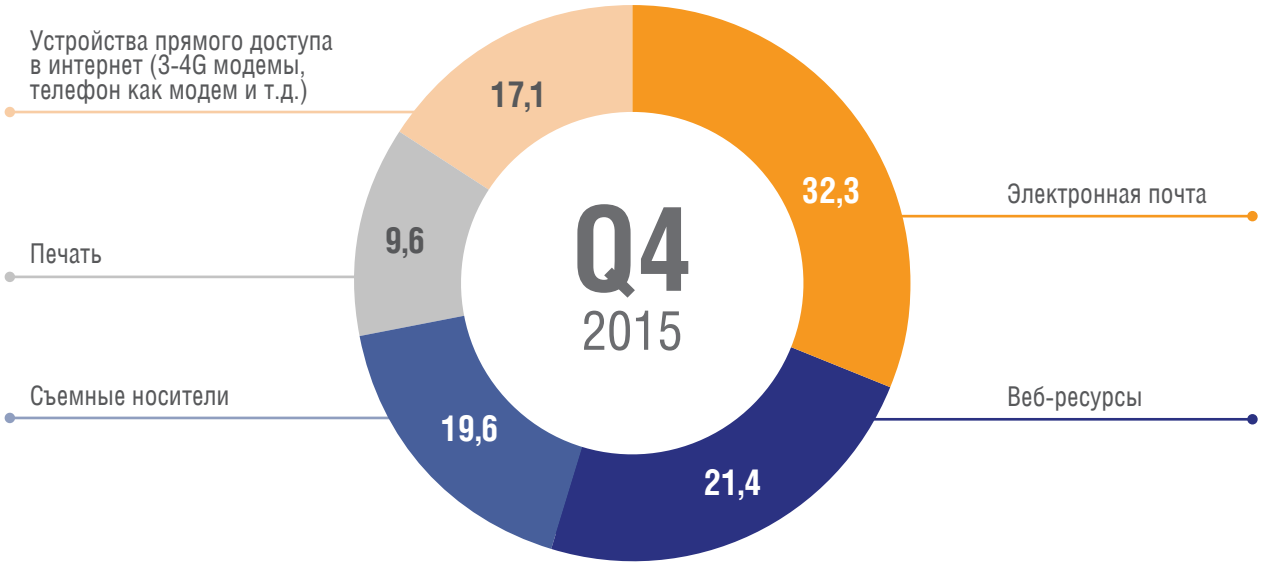
Особенности внутренних инцидентов в четвертом квартале 2015г.:

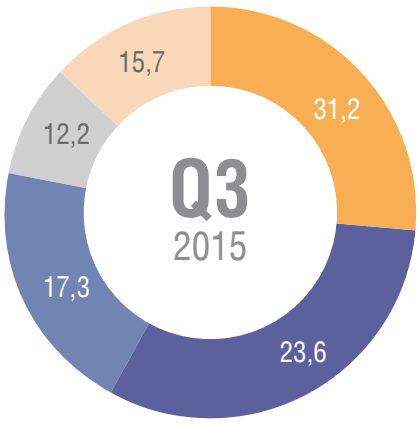
- На протяжении всего 2015 года уверенно растет доля инцидентов, связанных с утечками конфиденциальных данных. Число их выросло как по сравнению с прошлым аналогичным периодом в 2014 году, так и по сравнению с предыдущими кварталами 2015 года. В представленной категории инцидентов утечки являются ключевой проблемой ИБ, требующей организационных и технических способов решения. Стоит отметить, что возрастает процент инцидентов, связанных с умышленными действиями при отправке конфиденциальных данных с нарушением политики ИБ.
- Уровень количества инцидентов, связанных с вирусными заражениями, ransomware, а также с компрометацией учетных записей пользователей остается на относительно низком уровне. Как отмечалось в отчете за прошлый квартал, аналитики Solar JSOC связывают эту тенденцию с повышением осведомленности внутренних сотрудников.

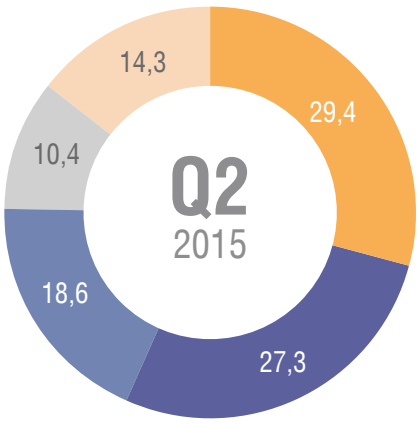
Инициаторы внутренних инцидентов

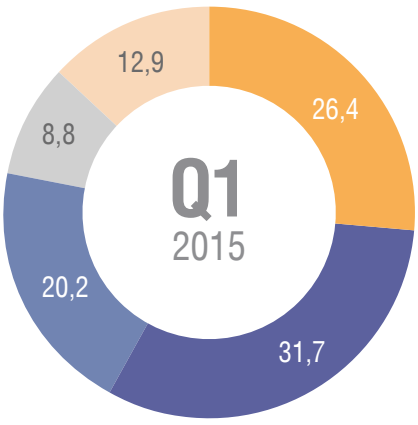


Распределение инцидентов по каналам утечек









Особенности, отмеченные в четвертом квартале 2015 года:

- В течение 2015 года наблюдалась постепенная смена «лидера» среди каналов утечки. Акцент с веб-ресурсов сместился в сторону передачи конфиденциальных данных по электронной почте.
- Использование устройств прямого доступа в интернет (3-4G модемы, телефон как модем и т.д.) для организации канала утечек по количеству инцидентов стало сопоставимо с подключением съемных носителей. Заметно повышение уровня технической подкованности пользователей, готовых организовывать дополнительные способы утечек информации, если традиционные каналы оказались закрытыми.

JSOC

Solar JSOC – первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ, являющийся провайдером сервисов безопасности (MSSP).

На всех этапах мониторинга и реагирования на инциденты ИБ Solar JSOC обеспечивает защиту клиентских данных. Обеспечение безопасности реализовано как на физическом, так и на информационном уровне с помощью средств разграничения доступа, аудита работы специалистов Solar JSOC, контроля целостности и защиты данных при передаче. Solar JSOC сертифицирован по требованиям PCI DSS, что подтверждает зрелость процессов обеспечения безопасности.

Уже более десятка клиентов получают аутсорсинговые услуги Solar JSOC. Сервис по мониторингу инцидентов был запущен в 2013 году, став первым подобным коммерческим центром в России. Сейчас в штате Solar JSOC более 30 специалистов дежурной смены, аналитиков и экспертов, которые обрабатывают более 100 000 событий с подозрением на инциденты в год.

Сервисы Solar JSOC

- Мониторинг инцидентов
- Контроль защищенности
- Противодействие кибепреступности
- Эксплуатация систем ИБ
- Анализ кода приложений
- Анти-DDoS
- Защита web-приложений

О компании Solar Security

Solar Security – это команда, создающая продукты и сервисы, позволяющие выстроить вертикаль управления и мониторинга ИБ, начиная с низкоуровневых инцидентов и заканчивая системами стратегической аналитики и ситуационными центрами по информационной безопасности.

Solar Security – это команда с двадцатилетним опытом разработки продуктов и собственная исследовательская лаборатория по анализу и прогнозированию инцидентов информационной безопасности. Наши знания позволяют гарантировать нашим клиентам уверенность в контроле над ситуацией в постоянно меняющемся мире внутренних и внешних киберугроз.

Solar Security – это продукты и сервисы, удобные в использовании и простые в восприятии. Они упрощают работу сотрудников ИБ, повышая их эффективность. Мы делаем технологии доступными руководителям и сотрудникам подразделений информационной безопасности, позволяя им выбрать удобный канал доставки в виде сервиса, приложения и комплексной системы.