JSOC Security flash report Q2 2015

SOLAR SECURITY
software&services

Отчет **JSOC Security flash report Q2 2015** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за второй 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 утечек реализовывал угрозы ИБ.

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

Оглавление

Ключевые выводы

01 Безопасность веб-приложений по-прежнему находится в зоне риска. 43,9% внешних атак приходятся на слабозащищенные, уязвимые веб-сервера, через которые злоумышленники не только получают доступ к информации самого веб-приложения, но и ко всей инфраструктуре.

02 Сохраняется тенденция роста числа инцидентов, инициаторами которых являются внутренние штатные администраторы. Количество их нарушений более чем в два раза превышает зафиксированные инциденты со стороны подрядчиков, аутсорсеров или контрагентов.

03 Снижение числа нарушений сотрудниками политик доступа в интернет говорит об усилении технического и организационного контроля внутри компаний и об использовании мобильных точек доступа личных смартфонов.

04 За второй квартал не произошло резких колебаний в сводной статистике по инцидентам ИБ, зафиксированным специалистами Solar JSOC. Это, в том числе, может быть связано с минимальным влиянием на ИБ экономических и политических событий.

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

Методология

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 второй квартал 2015 года в Solar JSOC было зафиксировано **47 876** событий с подозрением на инцидент, что на **37 %** выше, чем аналогичный показатель в Q1 2015.
- Доля критичных инцидентов составила **7,9 %** от общего числа.
- Среднее время принятия инцидента в работу специалистом Solar JSOC с момента выявления составило **24,5 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций клиенту Solar JSOC по критичным инцидентам составило **28,5 минуты** и **90,5 минут** по всем остальным.
- Соблюдение клиентских SLA за второй квартал составило **98,9 %**.
- **58,6 %** 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).
- При этом стоит отметить, что оставшиеся инциденты (**41,4 %**), 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. Информация по данным инцидентам 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 компании-клиента.

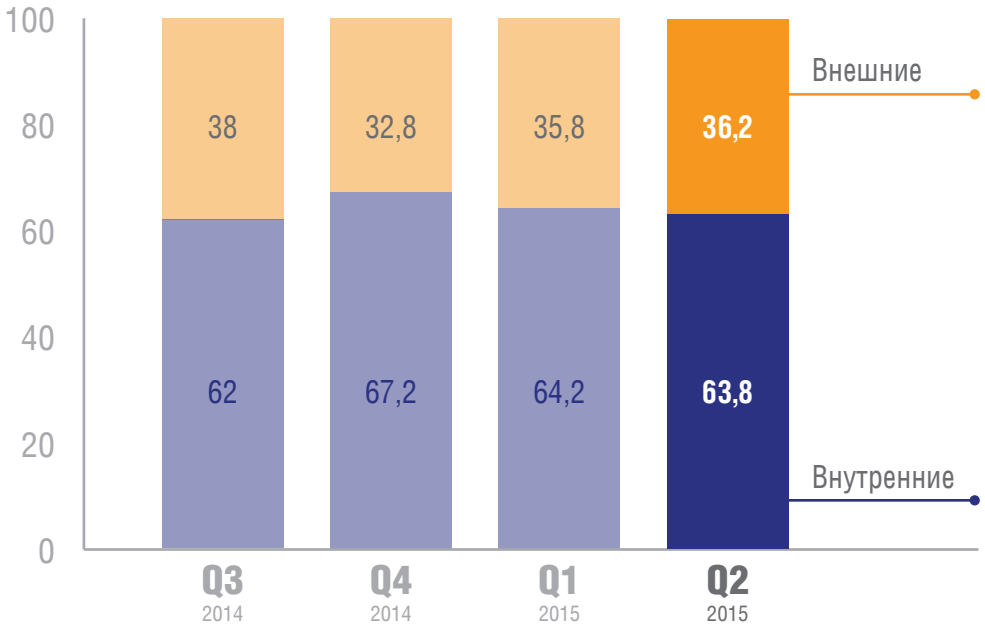
Инцидент считается критичным, если в его результате возможны и высоковероятны следующие события:

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

Общие показатели по инцидентам

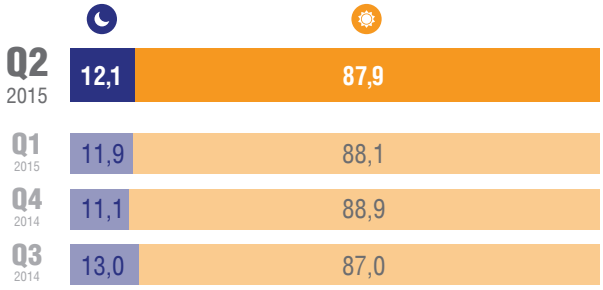
Распределение инцидентов по внешним и внутренним[1]

в %-ном соотношении от общего числа:

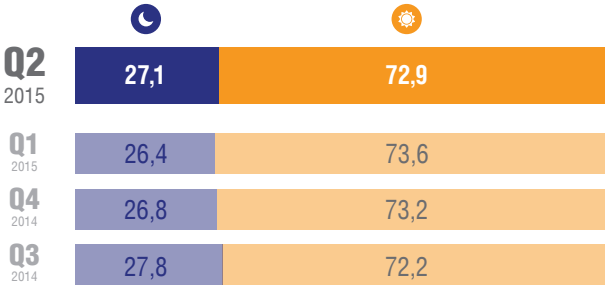


Распределение количества инцидентов по времени суток

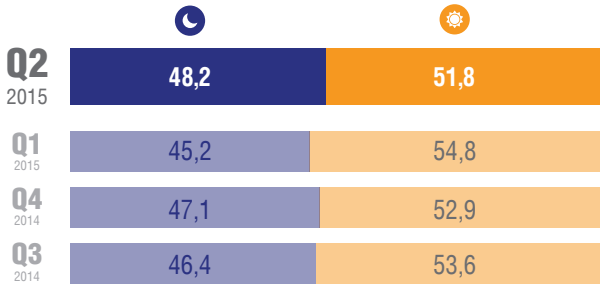
Общее распределение по времени суток (в %):



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

Во втором квартале 2015 года ситуация по распределению инцидентов по времени суток не претерпела существенных изменений. Однако, стоит отметить трехпроцентный рост критичных внешних инцидентов в ночной период: в абсолютных значениях это число выросло на 113 инцидентов по сравнению с предыдущим периодом.

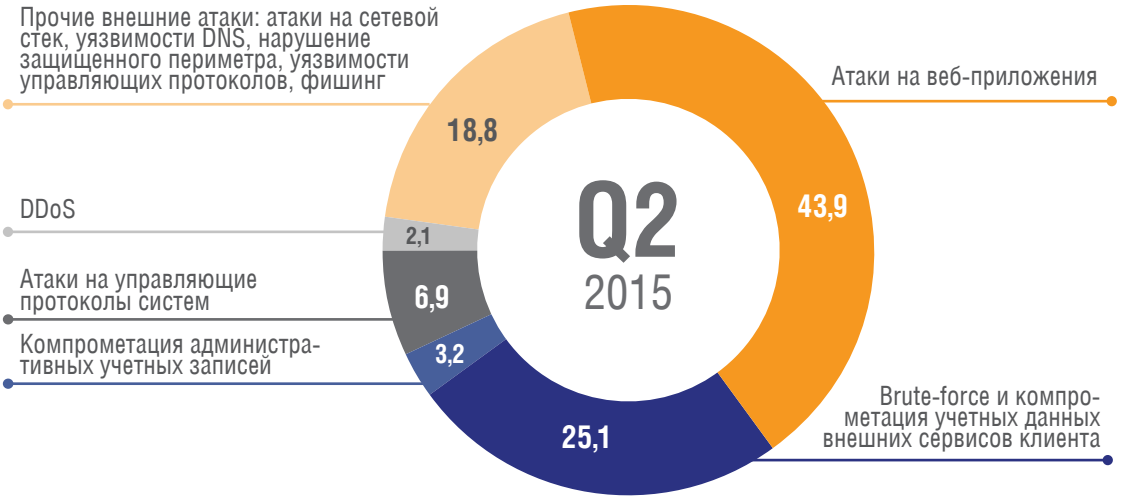
[1] К внутренним пользователям-инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты

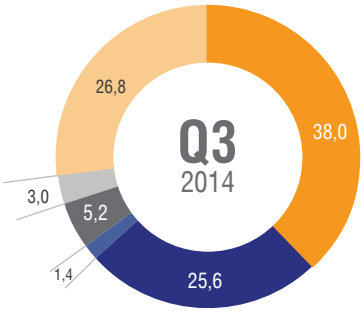
Внешние инциденты

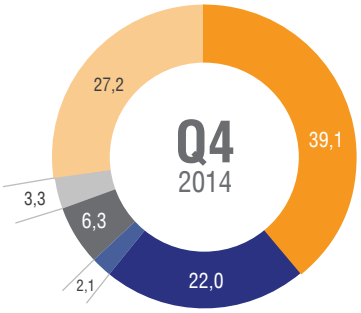
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся внутренними пользователями клиента.

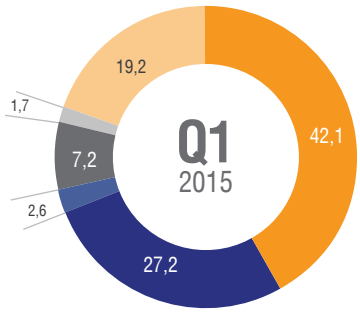
«Простые атаки», а именно действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не приводящие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей – из отчета исключены.

Направления атак в %-ном соотношении от общего числа:









Особенности внешних инцидентов во втором квартале 2015 г.

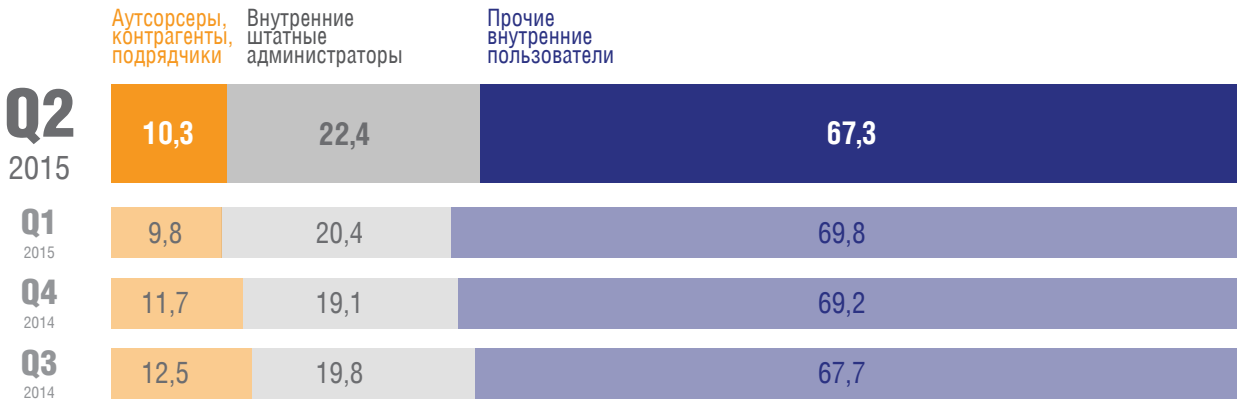
- Тенденция роста атак на веб-приложения сохраняется, до сих пор актуальна эксплуатация многих уязвимостей, известных с 2014 г. и ранее, например, в OpenSSH, OpenSSL, Apache HTTP Server и др. Технологии взлома веб-приложений становятся все более доступными и понятными широкому кругу злоумышленников.
- Продолжается рост числа инцидентов, связанных с компрометацией административных учетных записей. Это связано с повышенным интересом злоумышленников к получению привилегированного доступа и, как ни странно, слабой или отсутствующей парольной политикой служебных учетных записей на серверах ОС, СУБД, сетевом оборудовании.
- Сохраняется снижение доли «прочих внешних атак», что может быть связано как с постепенным усилением базовой защищенности клиентов Solar JSOC, так и с относительно долгим и, в свою очередь, неинтересным для злоумышленника путем реализации угроз ИБ.

Внутренние инциденты

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 соотношении от общего числа:

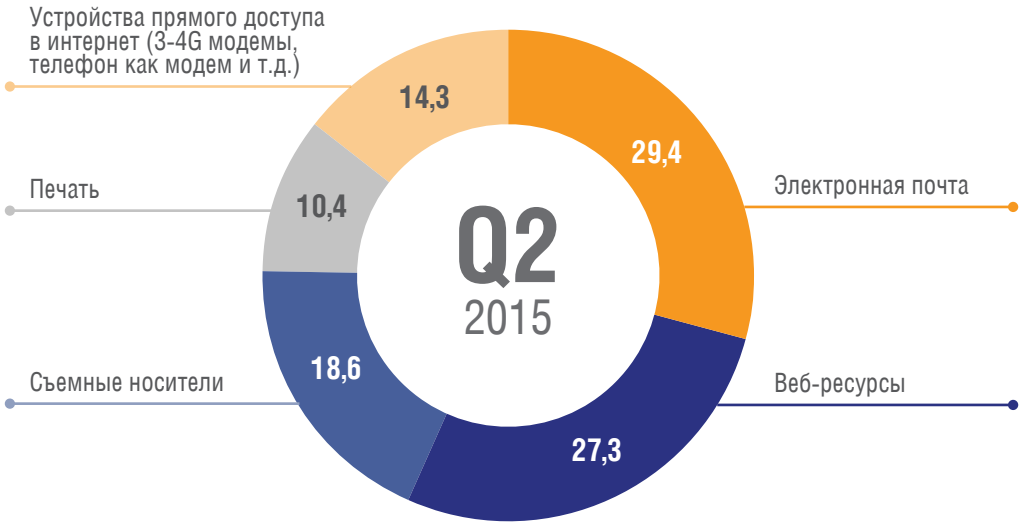
Инициаторы внутренних инцидентов в %-ном соотношении от общего числа:

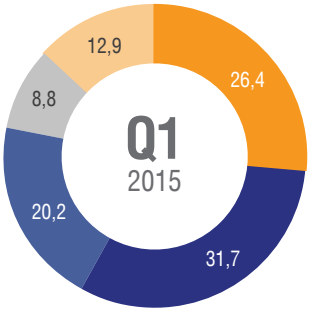


Внутренние инциденты

Распределение инцидентов по каналам утечек

в %-ном соотношении от общего числа:





Данные за периоды Q3 2014 и Q4 2014 отсутствуют (ранее не публиковались)

Особенности внутренних инцидентов во втором квартале 2015 г.

- Из квартала в квартал заметен значительный рост числа инцидентов, связанных с вирусными заражениями – как с массовыми, так и таргетированными. Это является показателем увеличения теневого рынка предложений вредоносного ПО, повышения конкуренции на этом рынке и, соответственно, снижения цен на профессиональные программные инструменты злоумышленников.
- Продолжает снижаться доля нарушений политик доступа в интернет. Как было упомянуто в отчете прошлого периода, это связанно с тем, что в компаниях стали осознавать этот риск и закрывать его техническими и организационными мерами. С другой стороны, есть экспертное мнение, что внутренние нарушители никуда не делись, а стали использовать иные каналы доступа в интернет, например, мобильные точки доступа собственных смартфонов.
- Доля инцидентов, связанных с деятельностью подрядчиков и аутсорсеров, вернулась на уровень прошлого года, так что статистика по первому кварталу 2015 г. говорит скорее о снижении активности подрядчиков в период с января по март.

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.