JSOC Security flash report Q2 2016

Отчет **Solar JSOC Security flash report** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за второй квартал 2016 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 реализовывал угрозы ИБ.

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

Оглавление

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

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

Ключевые выводы

I

В Q2 2016 г. зарегистрирован всплеск инцидентов, связанных с подключением устройств прямого доступа в сеть Интернет (3G-4G модемы, телефон как модем и т.д.).

II

Более 70% утечек реализуются посредством электронной почты, выгрузки на веб-ресурсы и копированием данных на съемные носители.

III

Информационные бюллетени FinCERT позволили выявить 10 подтвержденных инцидентов, из которых в 2 случаях совместное реагирование со службой клиента позволило целиком предотвратить ущерб от атаки.

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 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 2016 года в Solar JSOC было зафиксировано **68 823 событий** с подозрением на инцидент, в то время как в прошлом аналогичном периоде Q2 2015 года их количество составляло только **47 876**, а в **Q1 2016 – 54 726**.
- Во втором квартале 2016 года доля критичных инцидентов составила **11,2%**, что выше аналогичного показателя в Q1 2016 года, равного **10,6%**. Это связано с постепенным ростом бизнес-активности компаний, подключенных к середине года.
- Среднее время принятия инцидента в работу специалистом JSOC с момента выявления составило **19,3 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций по критичным инцидентам составило **28,7 минуты** и **80,5 минут** по всем остальным с момента возникновения инцидента.
- Соблюдение клиентских SLA за второй квартал 2016 года составило **97,2%**.
- **68,4%** исследованных событий зафиксировано при помощи основных сервисов ИТ-инфраструктуры и средств обеспечения базовой безопасности: межсетевые экраны и сетевое оборудование, VPN-шлюзы, контроллеры доменов, почтовые серверы, базовые средства защиты (антивирусы, прокси-серверы, системы обнаружения вторжений).
- При этом стоит отметить, что оставшиеся инциденты (**31,6%**), выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации и критичность для информационной и экономической безопасности компании-клиента, что позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные таргетированные атаки.

Классификация инцидентов по критичности

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

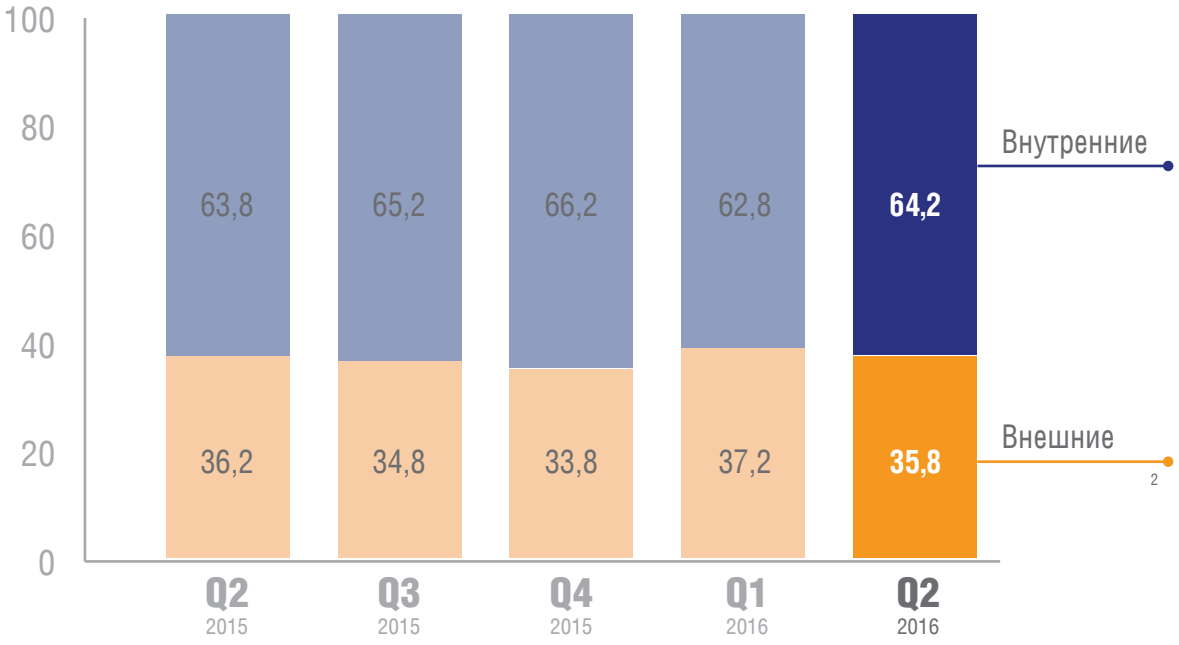
Инцидент считается критичным, если в результате него возможны и высоковероятны следующие события:

- 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 на сумму более 1 млн рублей в результате действий внутренних сотрудников или киберпреступников.

Общие показатели по инцидентам

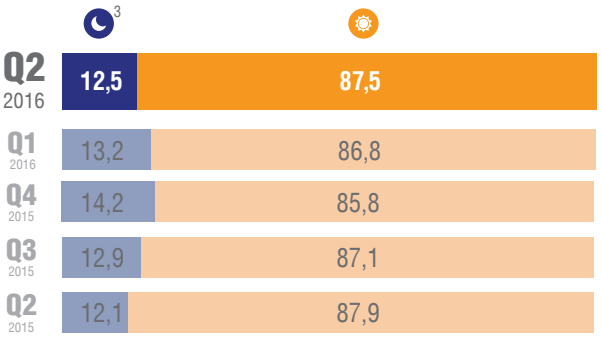
Q2 2016

Распределение инцидентов по внешним и внутренним

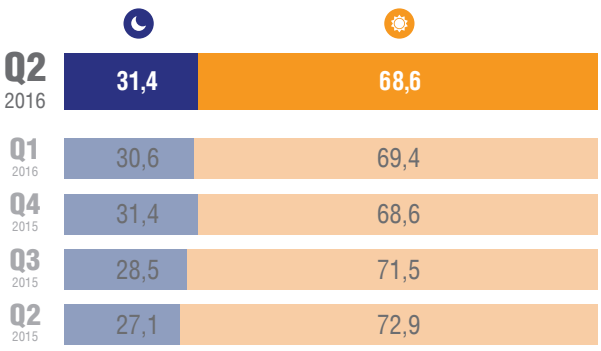


Распределение количества инцидентов по времени суток

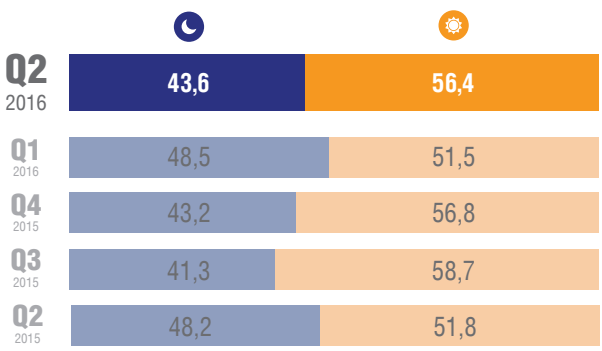
Время суток:



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.

Выводы по общим показателям по инцидентам

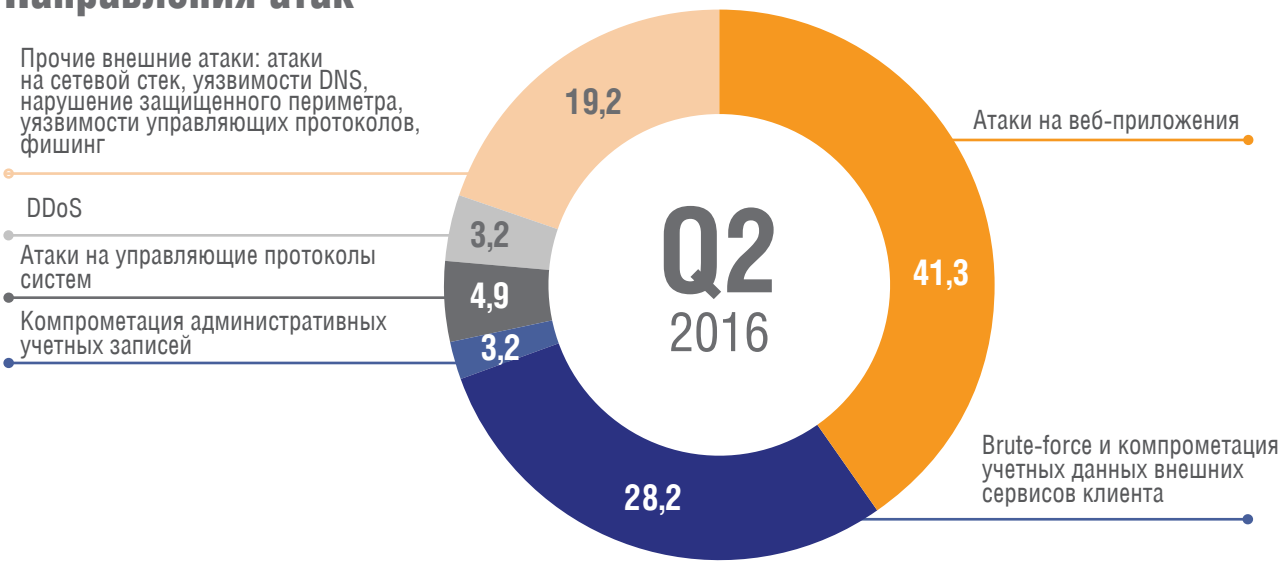
Как и следовало из отчета за предыдущий период, доля критичных ночных инцидентов в Q2 2016 незначительно повысилась и достигла значения 31,4% по сравнению с 30,6% в Q1 2016. Их уровень остается очень высоким и равен значению данного показателя в Q4 2015. Такая ситуация выглядит аномальной, ведь в Q2 2015 доля внешних критичных инцидентов была всего 27,1%.

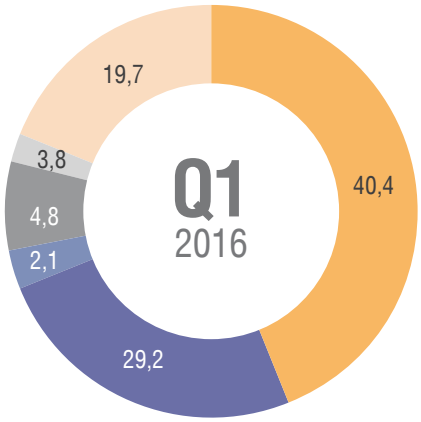
Распределение критичных внешних инцидентов отражает рост дневной активности событий ИБ, связанных с преодолением периметра компаний-клиентов, до значений Q3 и Q4 2015. Отмечается высокий уровень дневных критичных внешних инцидентов по сравнению с Q1 2016, а аналитики JSOC прогнозируют коррекцию данного показателя в ближайшем будущем.

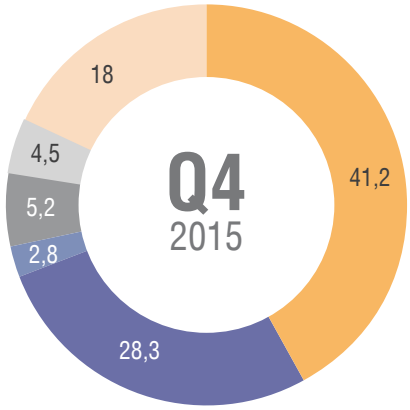
Общее распределение дневных и ночных инцидентов остается в привычном для первой половины года коридоре и примерно соответствует значениям аналогичного периода Q2 2015.

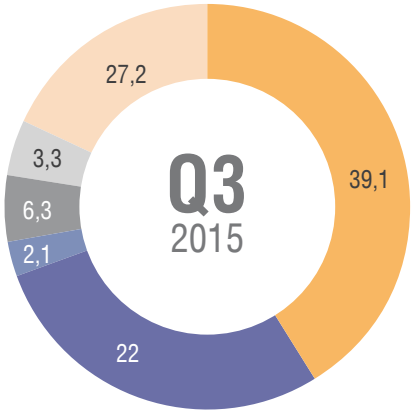
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся сотрудниками компании-клиента. «Простые атаки», а именно, действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не влекущие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей – из отчета исключены.

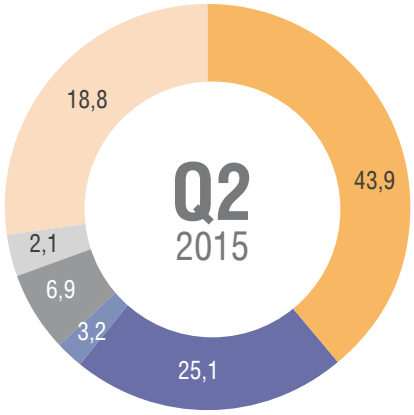
Направления атак











Особенности внутренних инцидентов во втором квартале 2016 г.:

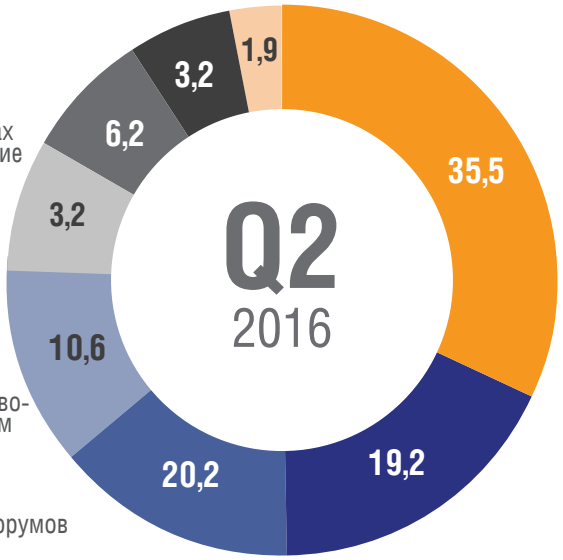
- Во втором квартале 2016 г. зарегистрирован всплеск инцидентов, связанных с подключением устройств прямого доступа в сеть Интернет (3G-4G модемы, телефон как модем и т.д.). Если в Q2 2015 было всего 14,3% подобных случаев от общего числа каналов утечек, то в Q2 2016 уже 21,8%.
- На протяжении года отмечается уверенная тенденция к снижению доли утечек информации посредством печати документов. Так, процент утечек через печать снизился практически вдвое - с 12,2% в Q3 2015 до 6,5% в Q2 2016.
- Как и в предыдущие периоды, более 70% утечек реализуются посредством электронной почты, выгрузки на веб-ресурсы и копирования данных на съемные носители. Рекомендуем обращать пристальное внимание на указанные каналы утечек и принимать превентивные меры и средства контроля для повышения безопасности конфиденциальной информации.

Внутренние инциденты

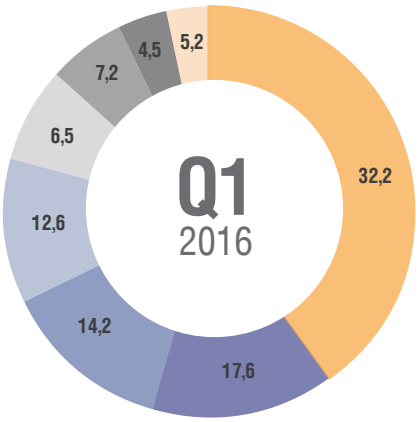
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников компаний-клиентов Solar JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных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

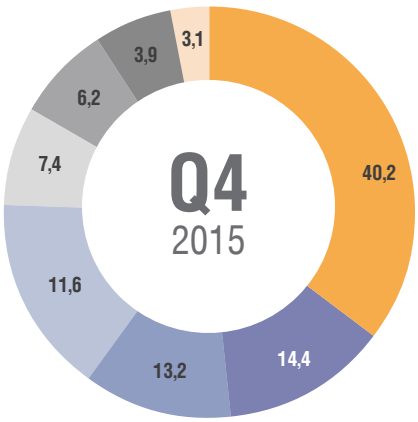
Направления атак

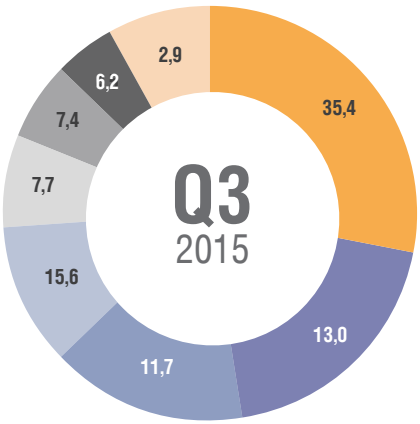
- Утечки конфиденциальных данных
- Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер
- Нелегитимные работы под привилегированными учетными записями: внутренние пользователи
- Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критичных бизнес-систем
- Нарушение политик доступа в интернет, в том числе использование TOR-клиентов, анонимайзеров и посещение хакерских форумов

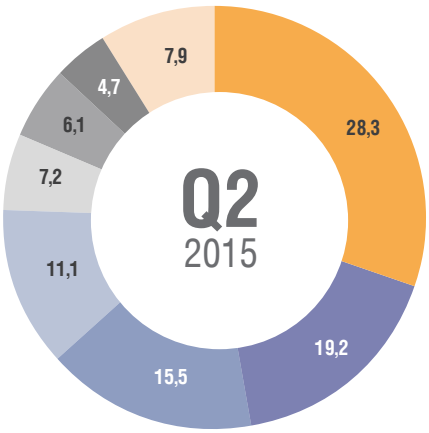


- Вирусные атаки, включая массовые вирусные заражения, действия ransomware и поведенческое выявление zero-day
- Прочее
- Компрометация внутренних учетных записей

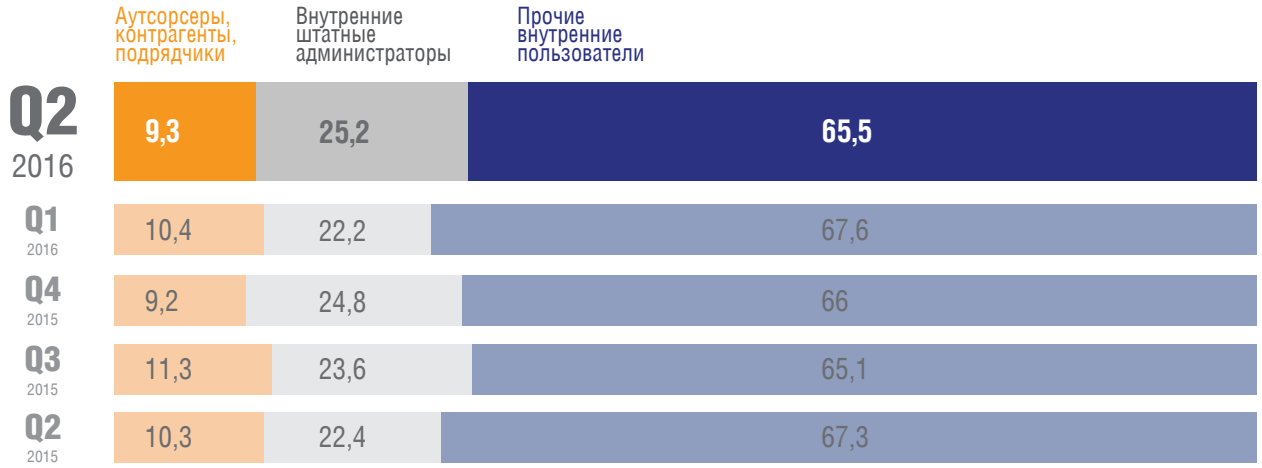




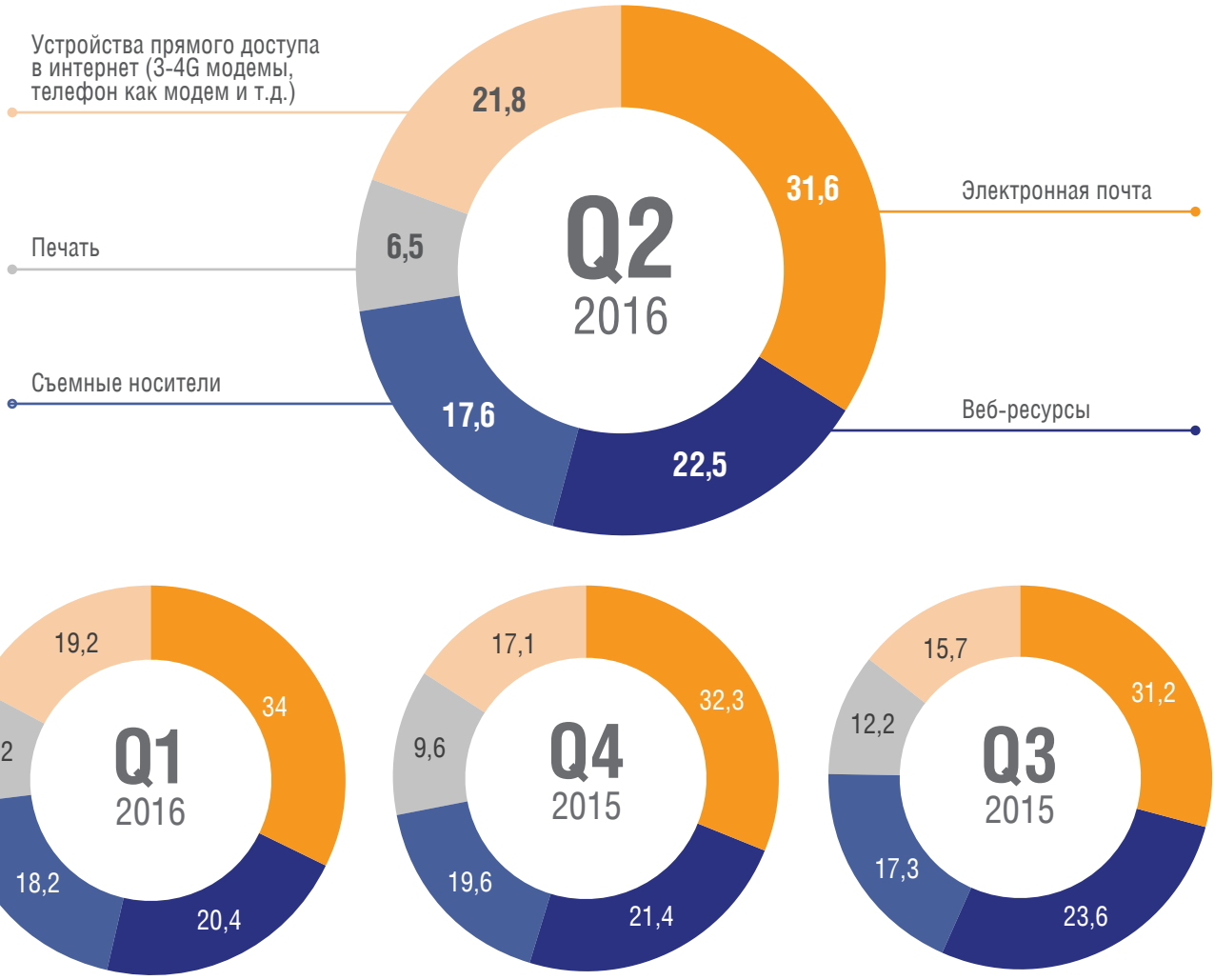




Инициаторы внутренних инцидентов



Распределение инцидентов по каналам утечек



Результаты использования информации об угрозах от FinCERT

За второй квартал 2016 командой Solar JSOC было получено 25 информационных бюллетеней от FinCERT, содержащих технические данные о зарегистрированных атаках, используемом способе проникновения и вредоносном коде, различных сетевых и хостовых индикаторах компрометации систем. Информация из каждого бюллетеня в течение 3 часов заносится в системы контроля защищенности и мониторинга инцидентов для проведения проверки и выявления подозрительных хостов в инфраструктуре подключенных компаний-клиентов.

По результатам отработки информационных бюллетеней FinCERT в Q2 2016 командой Solar JSOC была собрана следующая статистика:

- Признаки наличия сетевых индикаторов обнаружены по 12 бюллетеням в 29 подключенных компаниях (одни бюллетени встречались в нескольких компаниях), причем 7 случаев были определены как подтвержденные инциденты с проведенными дальнейшими расследованиями.

- Признаки наличия хостовых индикаторов обнаружены по 7 бюллетеням в 24 подключенных компаниях, причем только 4 случая определены как ложные срабатывания.

Из выявленных и подтвержденных инцидентов в 2 случаях оперативное взаимодействие команды Solar JSOC с клиентом позволило существенно минимизировать ущерб. Во всех остальных случаях совместное реагирование со службой клиента позволило целиком предотвратить ущерб от возникшего инцидента.