JSOC Security flash report Q4 2016

Отчет **Solar JSOC Security flash report** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за четвертый 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

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 четвертый квартал 2016 года в Solar JSOC было зафиксировано **67 292 события** с подозрением на инцидент.
- В четвертом квартале 2016 года **доля критичных инцидентов составила 14,8%**, что немного выше аналогичного показателя в Q4 2015 года, равного **12,4%**.
- Среднее время принятия инцидента в работу специалистом Solar JSOC составило **17,6 минуты**. Среднее время на подготовку аналитической справки об инциденте и предоставление рекомендаций составило **26,2 минуты** по критичным инцидентам и с момента обнаружения **75,4 минут** по всем остальным.
- Соблюдение клиентских SLA за четвертый квартал 2016 года составило **98,3%**.
- **71,2%** исследованных событий зафиксировано при помощи основных сервисов ИТ-инфраструктуры (межсетевые экраны и сетевое оборудование, VPN-шлюзы, контроллеры доменов, почтовые сервера) и базовых средства защиты информации (антивирусы, прокси-сервера, системы обнаружения вторжений). Оставшиеся инциденты (**28,8%**) выявляются при помощи сложных интеллектуальных средств мониторинга и защиты информации, использование которых позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвра щать сложные и/или 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.

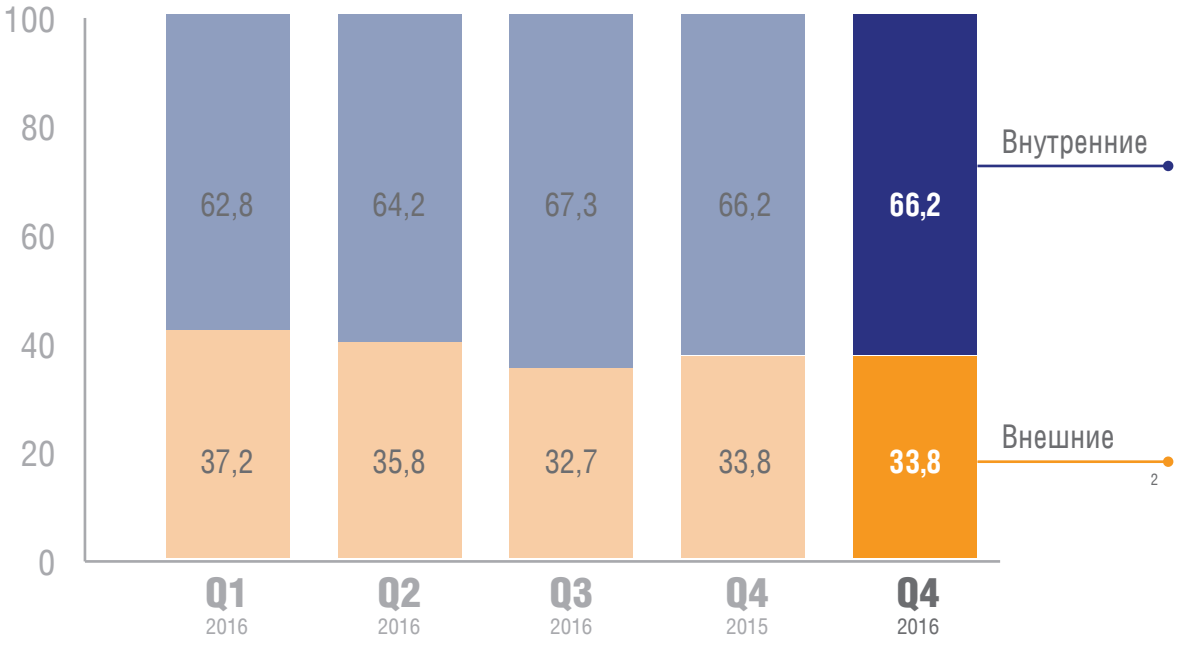
Инцидент считается критичным, если его результатом с высокой степенью вероятности станут следующие события:

- 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 действия внутренних сотрудников или киберпреступников.

Общие показатели по инцидентам

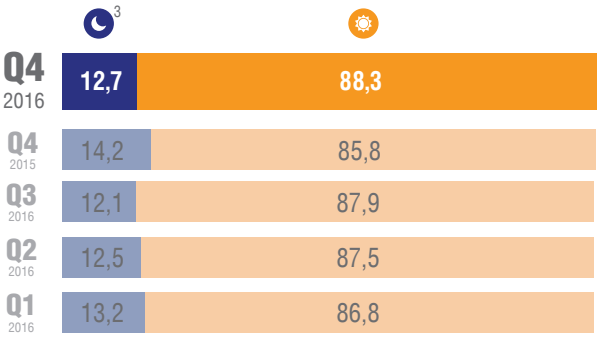
Q4 2016

Распределение инцидентов по внешним и внутренним

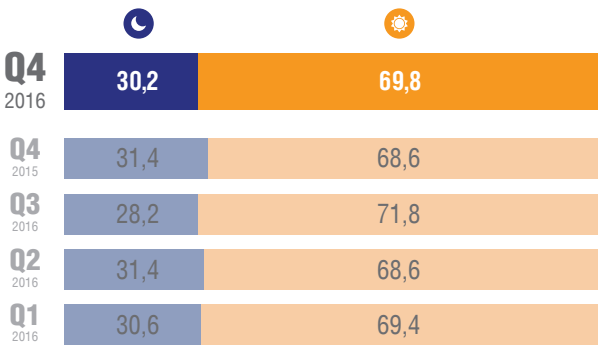


Распределение количества инцидентов по времени суток

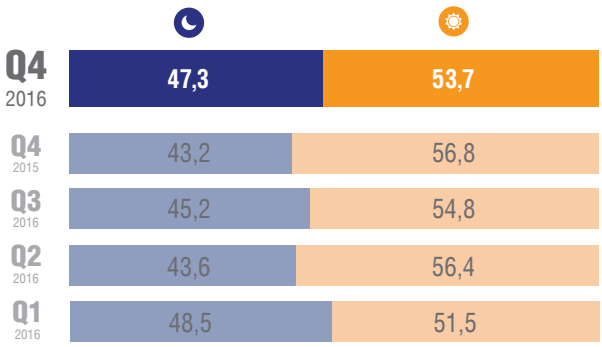
Время суток:



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

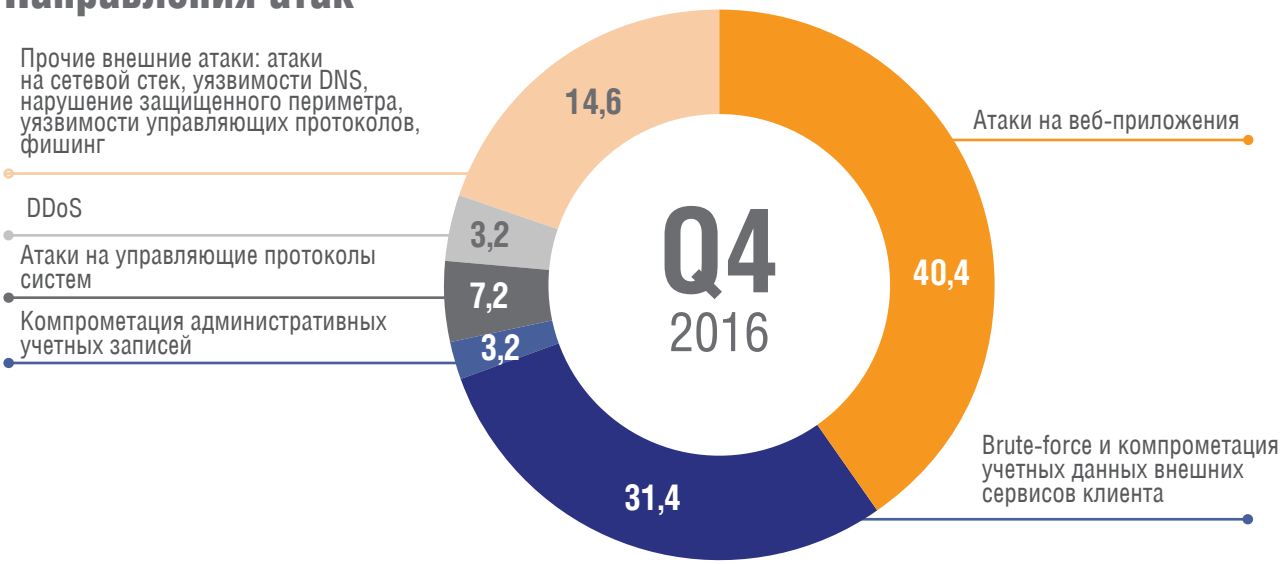
[2] К внутренним пользователям - инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты.

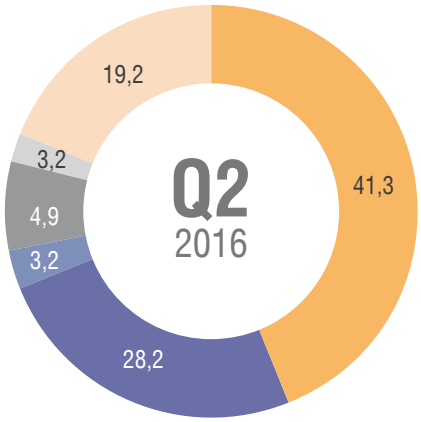
[3] С 21:00 до 08:00 утра по времени расположения офиса и присутствия специалистов информационной безопасности Заказчика.

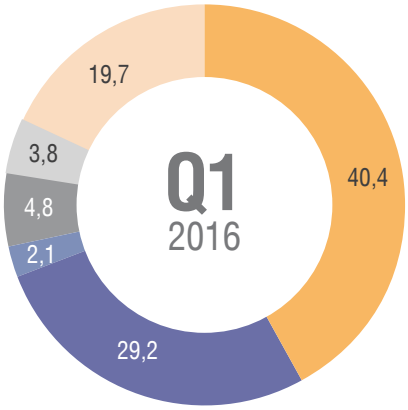
Внешние инциденты

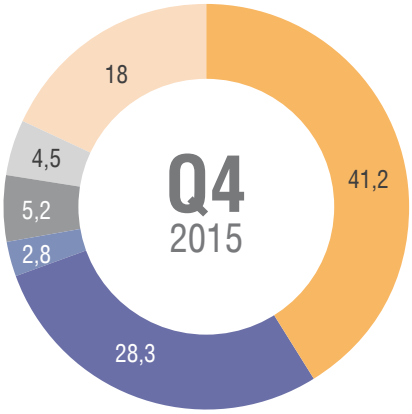
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся внутренними пользователями клиента. «Простые атаки», а именно действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не влекущие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

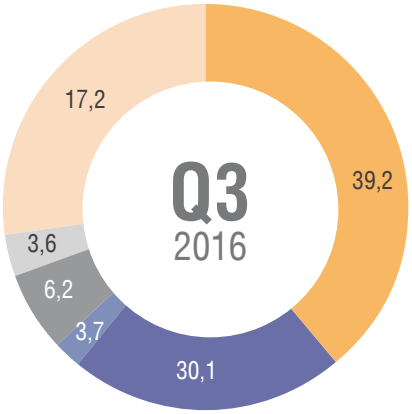
Направления атак











Особенности внешних инцидентов в четвертом квартале 2016 г.:

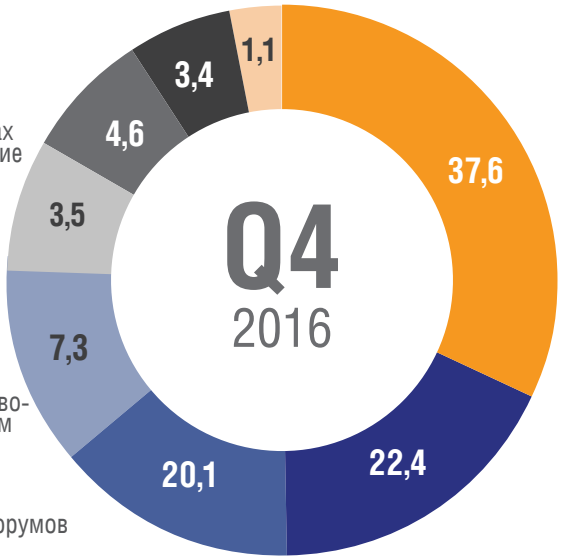
- В дополнение к ранее описанным трендам на атаки веб-приложений и компрометации клиентских учетных записей в Q3 2016 выявлены увеличения доли инцидентов, связанных с компрометацией административных учетных записей и атаками на управляющие протоколы. Так, в Q3 2016 было зарегистрировано 765 случаев компрометации административных учетных записей среди подключенных компаний-клиентов и порядка 1300 инцидентов, связанных с нарушениями использования управляющих протоколов систем и сервисов.
- Некоторое уменьшение продемонстрировали показатели по DDoS-атакам. Более глубокий анализ показал, что данное снижение связано не со снижением активности злоумышленников, а с повышением общей отказоустойчивости инфраструктур клиента и развитием алгоритмов защиты от атак на стороне операторов связи.

Внутренние инциденты

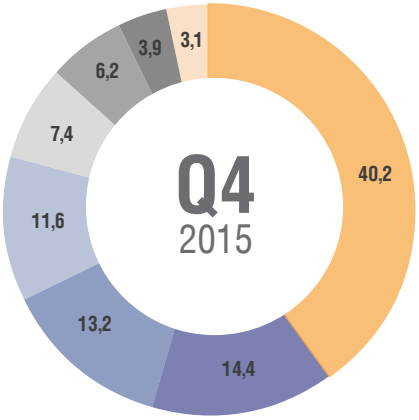
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников компаний-клиентов Solar JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных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

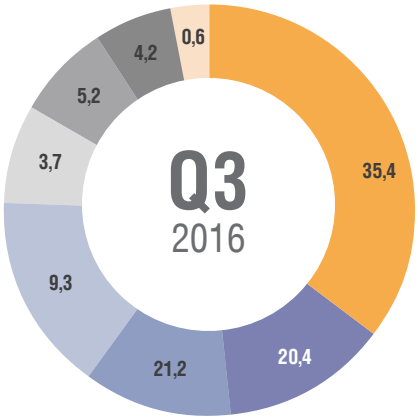
Направления атак

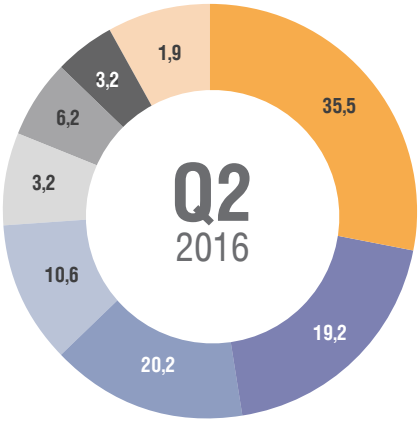
- Утечки конфиденциальных данных
- Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер
- Нелегитимные работы под привилегированными учетными записями: внутренние пользователи
- Нелегитимные изменения 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

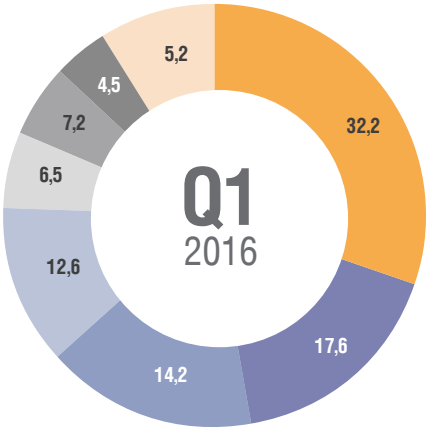


- Вирусные атаки, включая массовые вирусные заражения, действия ransomware и поведенческое выявление zero-day
- Прочее
- Компрометация внутренних учетных записей

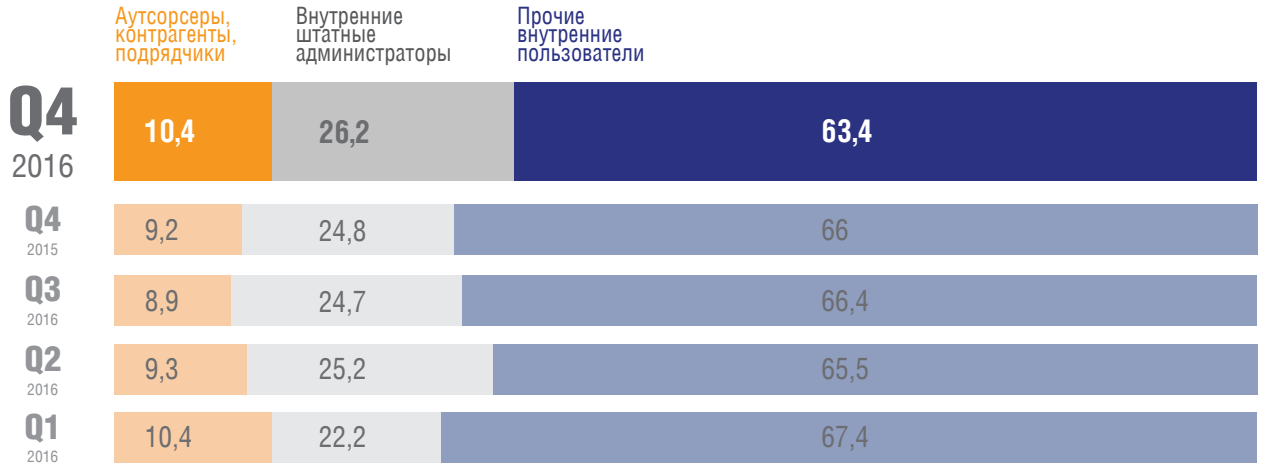




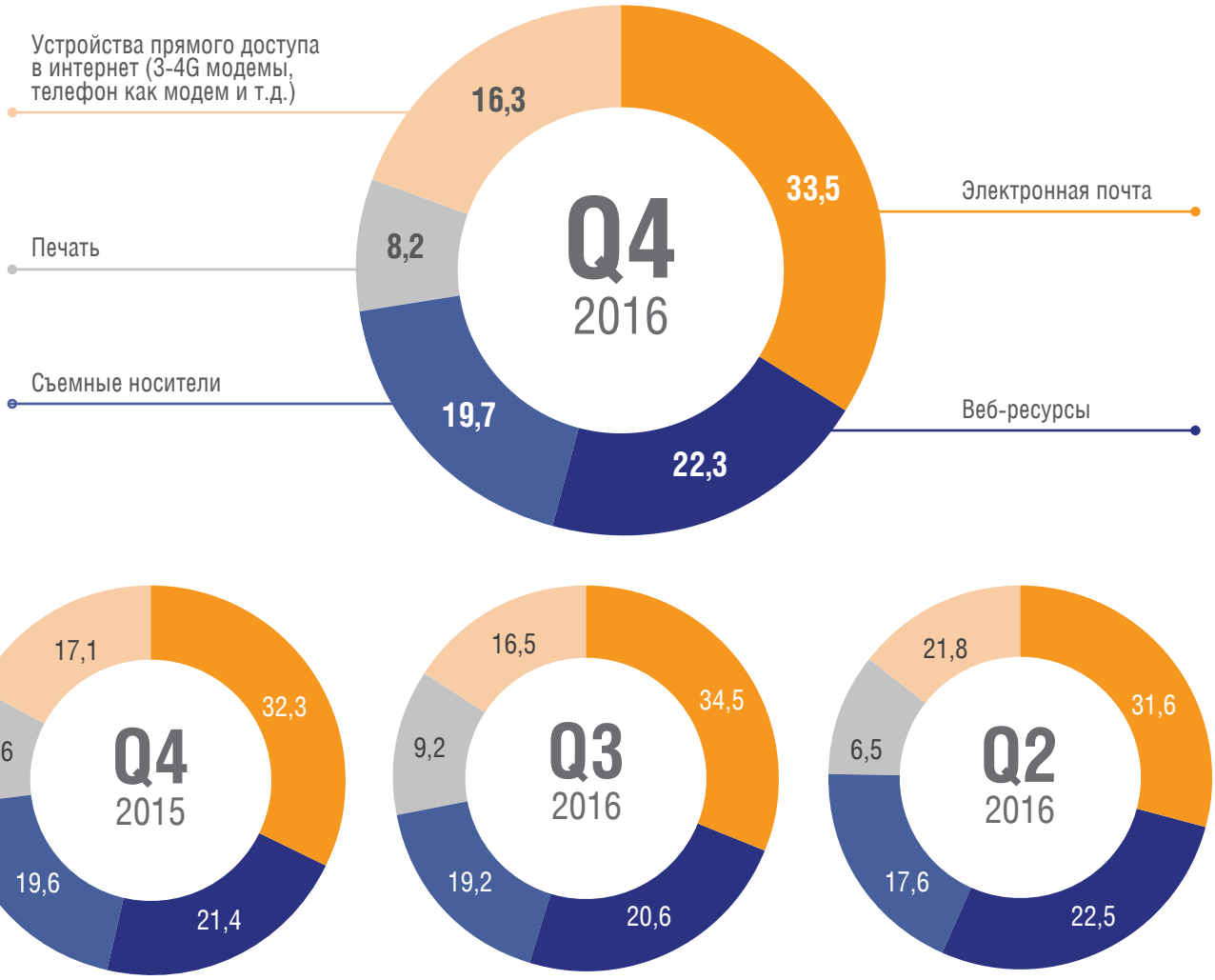




Инициаторы внутренних инцидентов



Распределение инцидентов по каналам утечек



Результаты использования информации об угрозах от FinCERT

За четвертый квартал 2016 командой Solar JSOC было получено 14 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 Q4 2016 командой Solar JSOC была собрана следующая статистика:

- Признаки наличия сетевых индикаторов обнаружены по 8 бюллетеням в 22 подключенных компаниях (одни бюллетени встречались в нескольких компаниях), причем 9 случаев были определены как подтвержденные инциденты с проведенными дальнейшими расследованиями

- Признаки наличия хостовых индикаторов обнаружены по 11 бюллетеням в 12 подключенных компаниях, причем только 2 случая определены как ложные срабатывания