JSOC Security flash report

второе полугодие 2017 года

Отчет **Solar JSOC Security flash report** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC[1] за второе полугодие 2017 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

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

2017
второе полугодие

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 исключительно информационным 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

- Во втором полугодии 2017 средний суточный поток событий ИБ, обрабатываемых SIEM-системами и используемыми Solar JSOC для оказания сервиса, составил **8,243 миллиардов событий (в первом полугодии 2017 – 6,156 миллиардов).**
- Всего за второе полугодие 2017 года в Solar JSOC было зафиксировано **231 623 событий с подозрением на инцидент.** За год их число выросло на 77%.
- Во втором полугодии 2017 года **доля критичных инцидентов** составила **15,5%,** то есть **критичным был каждый 6 инцидент**.
  С каждым годом доля критичных инцидентов неуклонно растет. Так, в первом полугодии 2015 года этот показатель составлял 8,1%, в первом полугодии 2017 – уже 17,2%. Небольшое снижение наблюдалось лишь в конце прошедшего года.
- С 2014 года число атак на компании увеличилось в среднем на **26%**.
- Среднее время принятия инцидента в работу специалистом Solar JSOC с момента выявления составило **14,2 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций по критичным инцидентам составило **22,4 минуты и 83,4 минут** – по всем остальным с момента возникновения инцидента.
- Соблюдение клиентских SLA за второй/третий квартал 2016 года составило **99,2%**.
- **74,3%** (в первом полугодии – 66,9%) исследованных событий зафиксировано при помощи основных сервисов ИТ-инфраструктуры и средств обеспечения базовой безопасности: межсетевые экраны и сетевое оборудование, VPN-шлюзы, контроллеры доменов, почтовые сервера, базовые средства защиты (антивирусы, прокси-сервера, системы обнаружения вторжений), операционные системы. Это свидетельствует о том, что полноценная эксплуатация и качественная настройка даже базовых средств защиты способно серьезно повысить уровень информационной безопасности организации. Увеличение показателя в первую очередь связано с развитием внутреннего контента Solar JSOC по аудиту журналов операционных систем, что позволило повысить количество и глубину анализа событий.

SOLAR SECURITY
software&services

Методология

- При этом стоит отметить, что оставшиеся инциденты **(25,7%)**, 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.
- Большая часть всех инцидентов **(86,7%)** происходила днем, однако, если говорить о критичных внешних инцидентах, то в **58,7%** случаев они происходили ночью. Это самый высокий показатель за последние четыре года.
- Если сравнить распределение общего числа критичных инцидентов по времени, можно увидеть, что они также все чаще (в **68,8%**) происходят ночью.
- Внешние злоумышленники чаще всего атакуют веб-приложения организаций (32,3%), в 22,8% они прибегают к brute-force и компрометации учетных данных внешних сервисов клиента, еще в 22,1% случаев – пытаются внедрить в организацию вредоносное ПО.
- Во второй половине 2017 года атаки еще чаще, чем раньше (**65% против 54%** в первом полугодии 2017), начинались с внедрения вредоносного ПО в инфраструктуру компании через социальную инженерию: пользователи открывали вредоносные вложения и проходили по фишинговым ссылкам. Этот рост произошел почти полностью за счет распространения программного обеспечения для майнинга криптовалют.
  При этом стоит отметить отраслевую специфику. Так, в банках майнинговое ПО чаще всего обнаруживается на рабочих станциях, куда оно доставляется в рамках пакетов вредоносного ПО через почту или зараженные сайты. За пределами финансового сектора ситуация обстоит иначе: в среднем **в каждой третьей организации** мы фиксируем инциденты, когда майнеры на серверном оборудовании компании устанавливают непосредственно сотрудники ИТ-департамента.
- Число инцидентов, связанных с вирусами-шифровальщиками, снизилось примерно на треть. Разумеется, на это косвенно повлияло сокращение числа массовых атак, однако это факт также может свидетельствовать о смещении фокуса злоумышленников с деструктивного влияния на информационные системы организаций в сторону более прямой монетизации атак (например, использования тех же майнеров).
- Инциденты, связанные с действиями внутренних злоумышленников, распределились следующим образом: утечки конфиденциальных данных – **48,2%**, компрометация внутренних учетных записей – 22,6%, нарушение политик доступа в интернет – 8,2%.
- Во второй половине 2017 года существенно (**с 25,6% до 31,3%**) возросло количество инцидентов, виновниками которых были ИТ-администраторы компаний. Сюда относятся и утечки конфиденциальной информации, и несоблюдение политик информационной безопасности ИТ-подразделением, что зачастую вызвано слабым контролем над ним или умением ИТ-специалистов обходить DLP-системы.

Методология

Классификация инцидентов по критичности

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

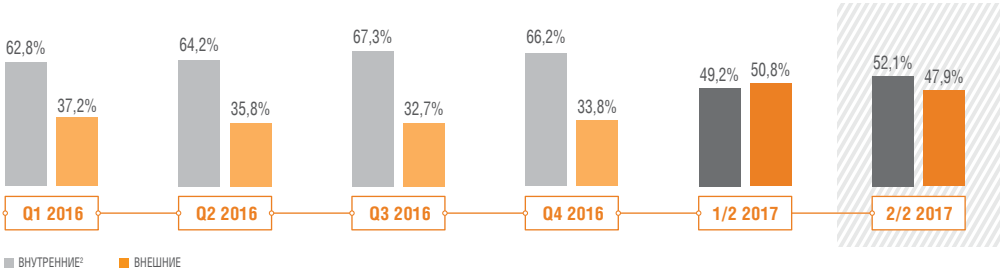
Инцидент считается критичным, если он с высокой вероятностью приведет к следующим событиям:

- 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.

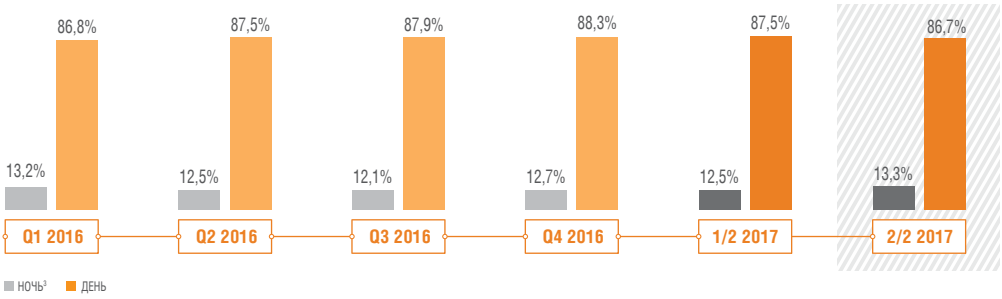
2017
второе полугодие

Общие показатели по инцидентам

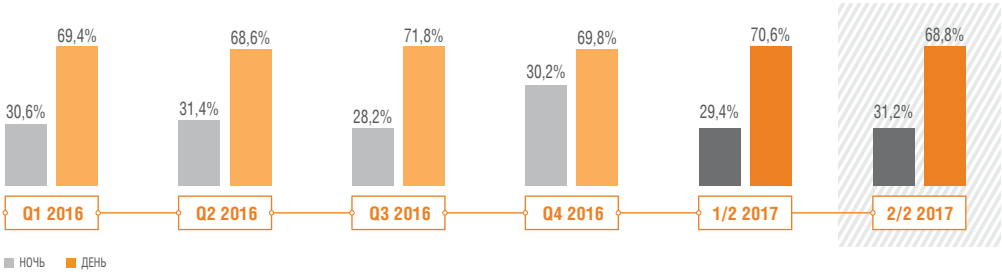
Распределение инцидентов по внешним и внутренним



Распределение общего числа инцидентов по времени суток



Распределение критичных инцидентов по времени суток



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 по времени расположения офиса присутствия специалистов информационной безопасности Заказчика

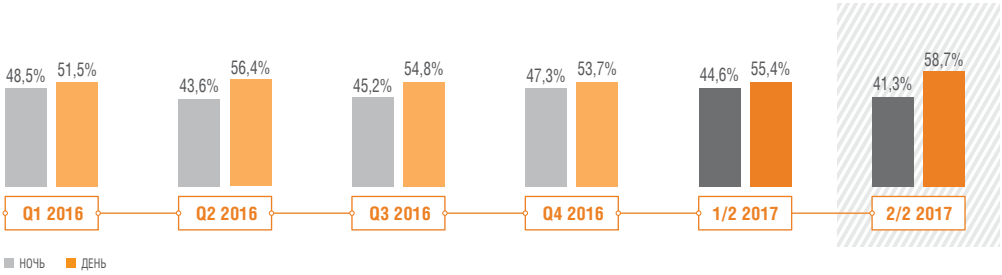
2017
второе полугодие

Общие показатели по инцидентам

Данные за 4 года демонстрируют медленную, но достаточно стабильную тенденцию к смещению критичных инцидентов к ночному времени. Если во второй половине 2014 года распределение критичных инцидентов по времени суток составляло примерно 74/26 (день/ночь), то сейчас оно примерно равно 69/31. С учетом общей стабильности данного показателя, смещение на 5 п.п. представляется достаточно серьезным.

Этот же тренд подтверждается и следующей метрикой – распределением критичных внешних инцидентов по времени суток. Она всегда демонстрировала наиболее серьезное смещение в сторону ночного времени, что вполне объяснимо: с большой вероятностью ночной инцидент детектируют не сразу, и у киберпреступников будет больше времени для закрепления в инфраструктуре или даже для проникновения в целевые сегменты, позволяющие монетизировать атаку. Однако, как бы ни была велика доля критичных внешних инцидентов, происходящих ночью, к концу 2017 года этот показатель достиг пиковых значений, не фиксировавшихся раньше.

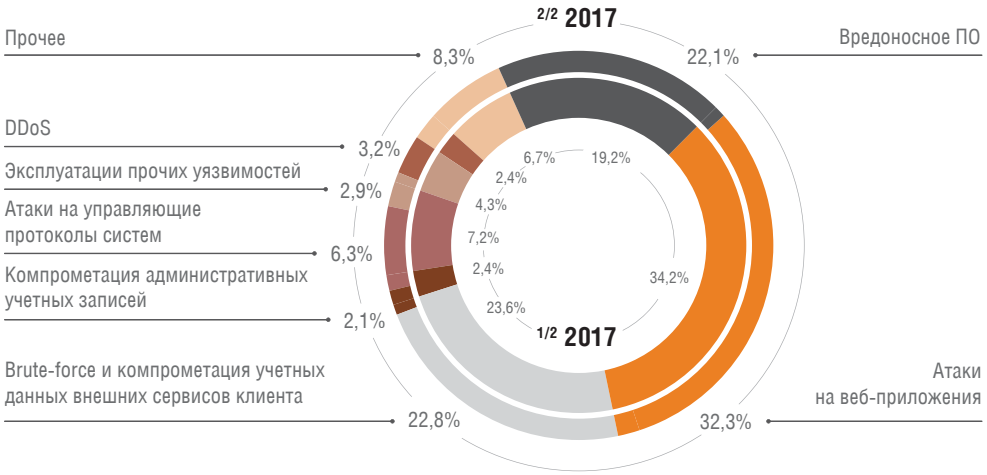
Распределение критичных внешних инцидентов по времени суток



Внешние инциденты

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

Направления атак



Kill Chain

Начиная с 2017 года, мы выделяем в качестве самостоятельного объекта исследования атаки, состоящие из нескольких последовательных шагов, формирующих Kill Chain. Такие атаки не завершаются на этапе получения доступа к конкретной подсистеме, а характеризуются последовательными попытками злоумышленника как можно глубже закрепиться в инфраструктуре и контролировать ее для получения финансовой или иной выгоды.

Наиболее распространенной является такая модель атаки, при которой после фазы первого проникновения в сеть компании злоумышленники пытаются выявить наиболее уязвимый сервер инфраструктуры, например, сервера со старыми необновленными версиями операционной системы. Захватив контроль над ним, злоумышленники в кратчайшие сроки получают доступ к привилегированным учетным записям сети (технологические учетные записи, записи ИТ-администраторов), из-под которых они могут скрытно получать доступ к большому количеству объектов инфраструктуры.

SOLAR SECURITY
software&services

Внешние инциденты

В абсолютном большинстве случаев Kill Chain сводится к этому алгоритму, варьируются лишь способы проникновения злоумышленника в инфраструктуру. Во второй половине 2017 года в 8% случаев проникновение в инфраструктуру осуществлялось с помощью вредоносного ПО, которое доставлялось на машину пользователя через зараженные флеш-носители, либо вследствие компрометации хоста за пределами корпоративной сети. В 10% случаев первым шагом служила атака на веб-приложение (например, онлайн-банк), в 17% – на управляющие протоколы систем, и в 65% – путем внедрения в организацию вредоносного программного обеспечения через email или фишинговые ссылки.

Напомним, в первом полугодии 2017 это распределение выглядело следующим образом: в 11% случаев первым шагом служила атака на веб-приложение; в 13% вредоносное ПО доставлялось на машину пользователя через зараженные флеш-носители, либо хост был скомпрометирован за пределами корпоративной сети; в 22% были атакованы управляющие протоколы систем (в том числе с использованием уязвимости Shellshock, известной с сентября 2014 года); в 54% злоумышленники использовали вредоносное программное обеспечение, доставляемое в инфраструктуру через email-вложения или фишинговые ссылки.

Внешние инциденты

Статистика демонстрирует существенное смещение доли проникновения в инфраструктуру с использованием уязвимостей управляющих протоколов в пользу ВПО. Мы видим три предпосылки для данного тренда:

- Принятие 187-ФЗ и его подзаконных актов способствовало тому, что различные организации энергетического и государственного сектора провели инвентаризацию периметра и цифровых активов. Итогом этих мероприятий стало выявление и закрытие старых неучтенных сервисов или критических уязвимостей периметра, что повысило общий уровень защищенности.
- По итогам массовых атак первой половины прошлого года во многих организациях были внедрены компенсирующие меры ИБ, положительно повлиявшие на уровень защиты от атак на управляющие протоколы систем.
- Продолжающееся развитие инструментария ВПО, которое все чаще модифицируется и дорабатывается хакерскими группировками, в сочетании с простотой его доставки в инфраструктуру. Возможность «широковещательной» атаки сразу по нескольким организациям делает этот механизм все более привлекательным для злоумышленников.

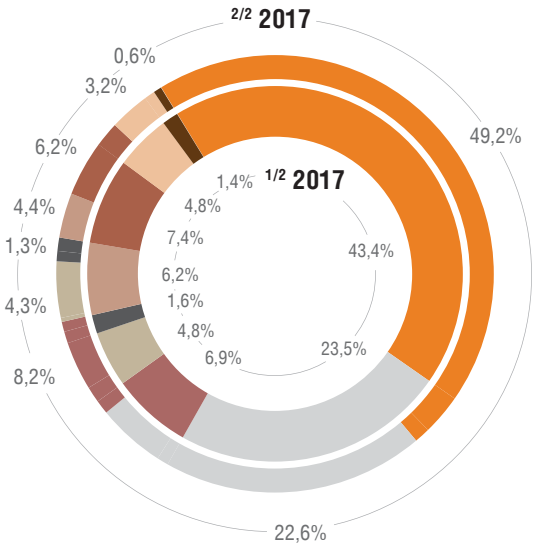
Интересные наблюдения:

- Заметный рост числа инцидентов с вредоносным программным обеспечением связан с фактами выявления утилит для майнинга в инфраструктурах заказчиков. При этом стоит отметить отраслевую специфику. Так, в банках майнинговое ПО чаще всего обнаруживается на рабочих станциях и доставляется в рамках пакетов вредоносного ПО через почту или зараженные сайты. За пределами финансового сектора ситуация обстоит иначе: в среднем в каждой третьей организации мы фиксируем инциденты, когда непосредственно сотрудники ИТ-департамента устанавливают майнеры на серверном оборудовании компании.
- Фиксируем снижение числа инцидентов, связанных с вирусами-шифровальщиками, примерно на треть. Разумеется, на это косвенно повлияло сокращение числа массовых атак, однако это факт также может свидетельствовать о смещении фокуса злоумышленников с деструктивного влияния на информационные системы организаций в сторону более прямой монетизации атак.

Внутренние инциденты

Направления атак

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



- Утечки конфиденциальных данных
- Компрометация внутренних учетных записей
- Нарушение политик доступа в интернет
- Использование Remote Admin Tools или инструментов туннелирования трафика
- Использование хакерских и потенциально вредоносных утилит
- Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критичных бизнес систем
- Нелегитимные работы под привилегированными учетными записями: внутренние сотрудники
- Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер
- Прочее

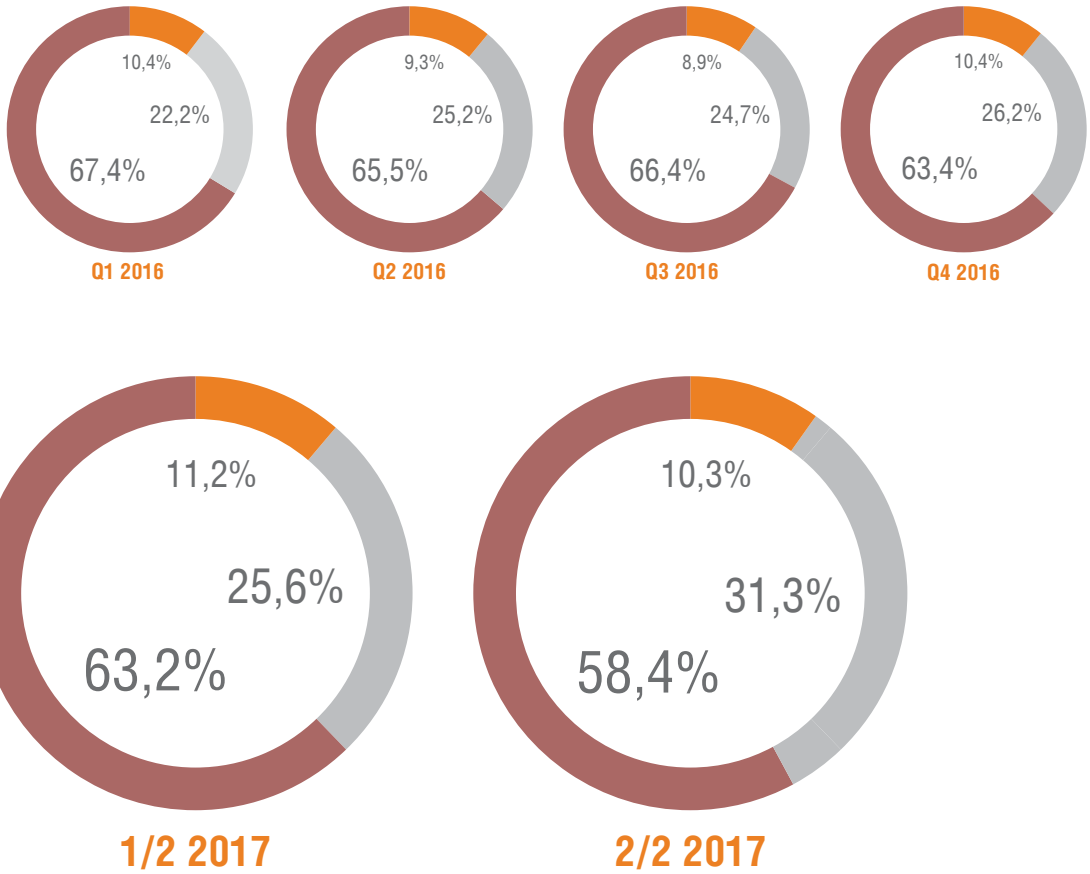
Интересные наблюдения:

- Стабильный рост во второй половине года показывает число инцидентов, связанных с утечками конфиденциальной информации. Основная причина, на наш взгляд, состоит в желании сотрудников, находящихся под угрозой увольнения, сохранить свои наработки и тем самым повысить свою ценность в глазах других потенциальных работодателей. К концу 2017 года они составляли почти половину всех внутренних атак.
- Продолжает увеличиваться количество инцидентов, связанных с нарушением политик доступа в интернет. В большей части это касается использования VPN-сервисов и анонимайзеров. Не в последнюю очередь мы связываем данный факт с государственным ужесточением доступа и расширением списка запрещенных сайтов на территории РФ.

2017
второе полугодие

Внутренние инциденты

Инициаторы внутренних инцидентов



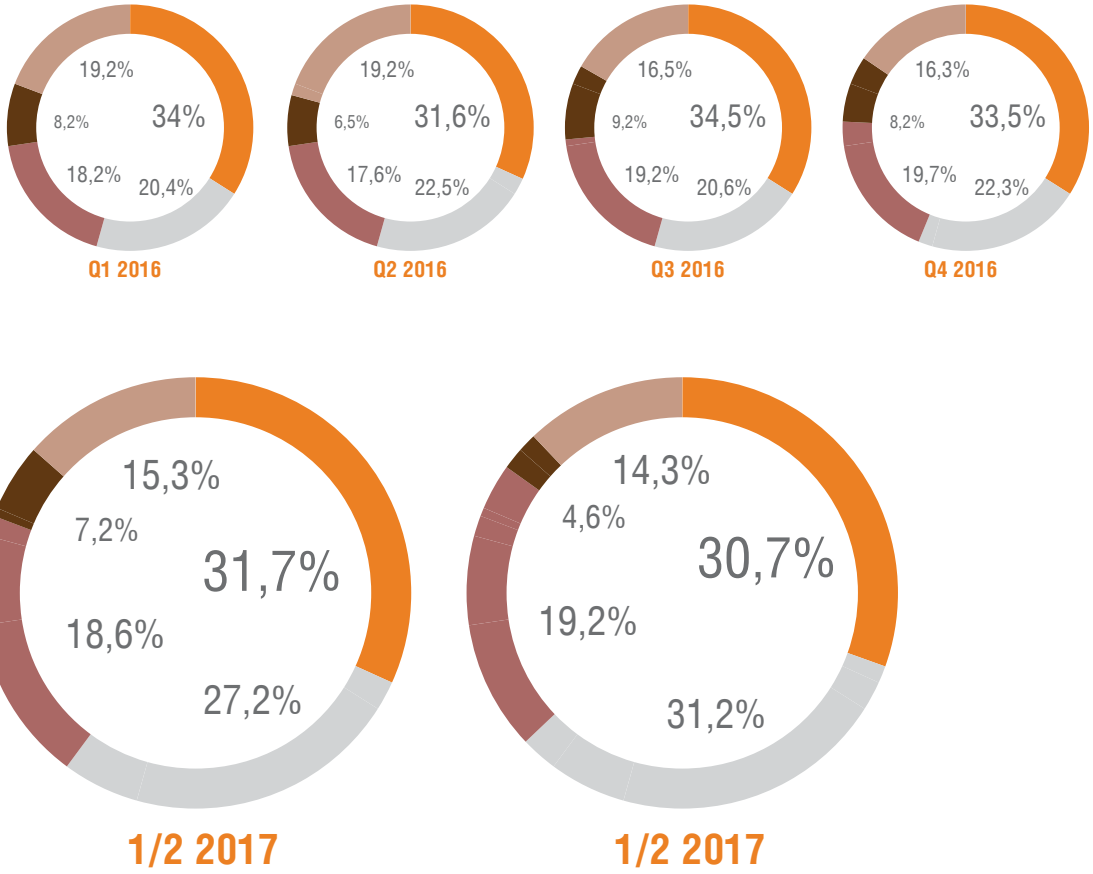
- Аутсорсеры, контрагенты, подрядчики
- Внутренние штатные администраторы
- Прочие внутренние пользователи

Во второй половине 2017 года существенно возросло количество инцидентов, виновниками которых были ИТ-администраторы компаний. Сюда относятся и утечки конфиденциальной информации, и несоблюдение политик информационной безопасности ИТ-подразделением, что зачастую вызвано слабым контролем над ним или умением ИТ-специалистов обходить DLP-системы.

2017
второе полугодие

Внутренние инциденты

Распределение по каналам утечек



- Электронная почта
- Веб-ресурсы
- Съемные носители
- Печать
- Устройства прямого доступа в интернет

Тенденция к увеличению числа утечек через веб-ресурсы, на наш взгляд, связана с увеличением количества нарушения политик доступа в интернет с использованием технологий скрытия, таких VPN-сервисы и анонимайзеры. «Защищенность» соединения создает у пользователей мнимое ощущение возможности использования такого канала для кражи конфиденциальных данных.

При этом доля утечек через печать стабильно сокращается. Можно предположить, что объемы данных, которые пользователи намереваются украсть, обычно слишком велики для того, чтобы их отправка на печать осталась незамеченной.

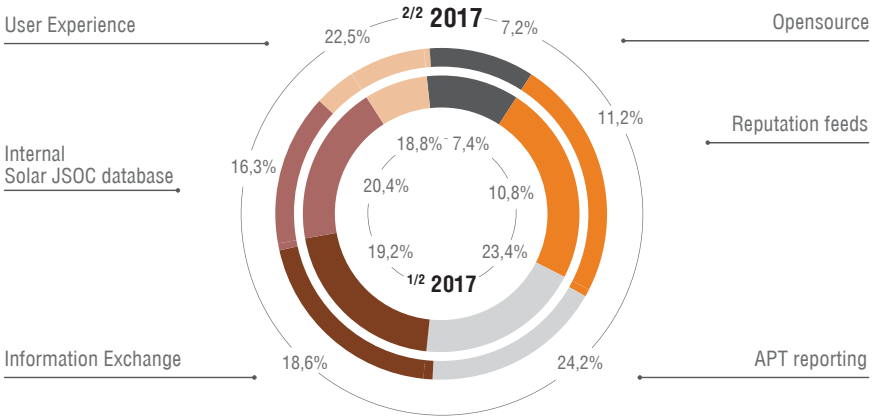
Threat Intelligence

Результаты использования информации об угрозах Threat Intelligence

Источники Threat Intelligence, используемые в Solar JSOC, можно условно разделить на следующие категории:

- Opensource – открытые базы индикаторов вредоносного ПО, серверов управления и фишинговых ссылок. Как правило, в разрезе детектирования с помощью SIEM-платформ актуальность имеют только сетевые индикаторы.
- Reputation feeds – платные подписки на репутационные списки вредоносного ПО, серверов управления и фишинговых ссылок. Как правило, в разрезе детектирования с помощью SIEM-платформ актуальность имеют только сетевые индикаторы.
- APT/IOC reporting – платные подписки на подробные описания 0day вредоносных тел, включающие, в том числе, и описание используемых уязвимостей, и хостовые индикаторы вредоносного ПО.
- Information Exchange – информация, полученная в рамках информационных обменов с государственными, ведомственными и иностранными центрами реагирования на инциденты (CERT).
- Internal Solar JSOC database – индикаторы, полученные в результате собственных исследований Solar JSOC или расследований инцидентов.
- User experience – информация, полученная напрямую от пользователей клиентов (успешное противодействие социальной инженерии, детектирование фишинговых рассылок и т.п.).

Распределение по долям инцидентов, детектированных с помощью разных типов Threat Intelligence



Статистика показывает, что правильное использование бесплатных источников информации о TI может повысить защищенность компании и устойчивость к массовым атакам. Но не менее половины инцидентов выявляется только при помощи платных коммерческих подписок. Изменение долей, в первую очередь, связано с внутренними изменениями в Solar JSOC, в том числе, усилением работы в рамках внутренней вирусной аналитики и развитием сценариев, позволяющих выявлять вирусные атаки по косвенным признакам.