SOLAR SECURITY
software&services

Solar JSOC Security flash report

первое полугодие 2017 года

Отчет **Solar JSOC Security flash report** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за первое 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 реализовывал угрозы информационной безопасности.

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

Оглавление

2017
первое 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 только информативным материалом и не претендует на то, что приведенные данные полностью отражают все угрозы ИБ для компаний российского рынка. Команда Solar JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации.

Сводная статистика за отчетный период

- Средний суточный поток событий ИБ, обрабатываемых SIEM-системами и используемых Solar JSOC для оказания сервиса, составил **6,156 миллиардов**.
- Всего за первое полугодие 2017 года в Solar JSOC было зафиксировано **172 477 событий** с подозрением на инцидент, что примерно **на 28% больше**, чем в первом полугодии 2016 года.
- В первом полугодии 2017 года доля критичных инцидентов составила **17,2%**, в первом-втором квартале 2016 года этот показатель составлял **10,6% - 11,2%**. Таким образом, если в 2016 году критичным был каждый 9 инцидент, то теперь – уже каждый 6. Предполагается, что такая динамика связана с общим повышением интенсивности массовых и нацеленных атак на организации.
- Среднее время с момента выявления до принятия инцидента в работу специалистом Solar JSOC составило **18,2 минуты**. Среднее время с момента возникновения инцидента до получения заказчиком аналитической справки и рекомендаций составило **29,4 минуты** по критичным инцидентам и **72,8 минут** – по всем остальным.
- Соблюдение клиентских SLA за первое полугодие 2017 года составило **98,8%**.
- **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 серверы, базовые средства защиты (антивирусы, прокси-серверы, системы обнаружения вторжений). Это свидетельствует о том, что полноценная эксплуатация и качественная настройка даже базовых средств защиты способны серьезно повысить уровень информационной безопасности организации.
- При этом стоит отметить, что оставшиеся инциденты (**33,1%**), выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации, критичной для информационной и экономической безопасности компании-клиента, что позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные таргетированные атаки.

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 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.

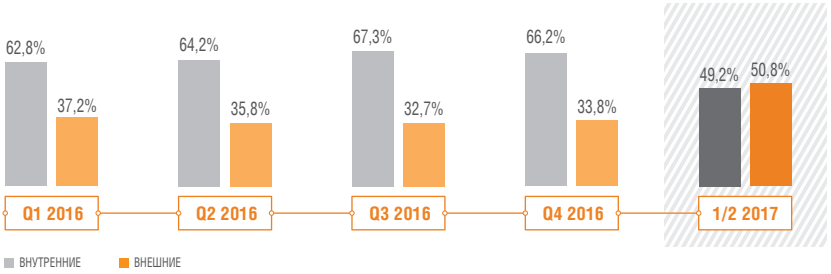
Изменение в классификации инцидентов:

- С первого квартала 2017 года инциденты, связанные с вирусными заражениями (почта, веб и т.д.), в отчетах Solar JSOC отнесены к внешним инцидентам, так как все чаще они являются признаком не халатности пользователя, а интереса злоумышленников к организации и ее инфраструктуре.

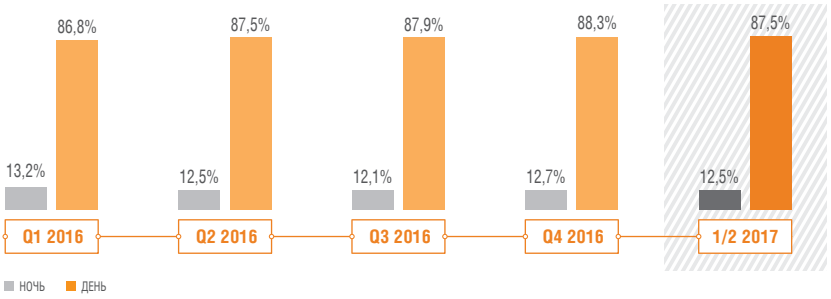
2017
первое полугодие

Общие показатели по инцидентам

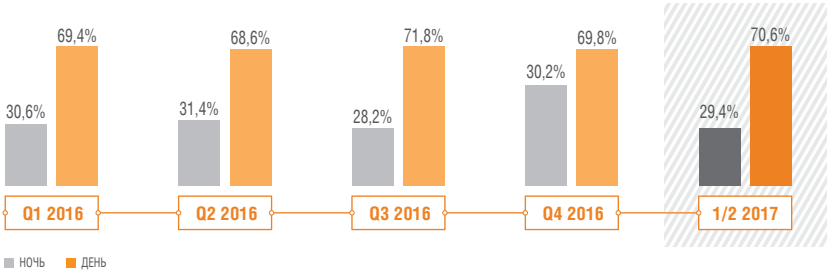
Распределение инцидентов по внешним и внутренним



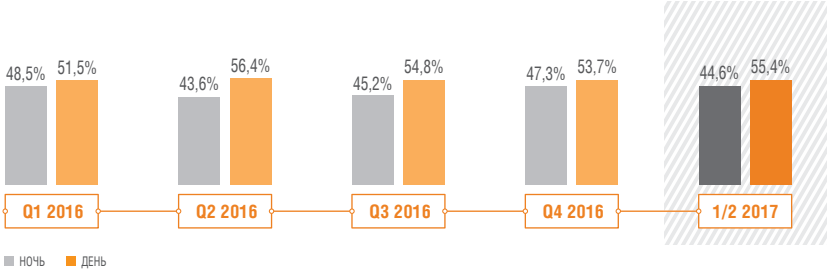
Распределение общего числа инцидентов по времени суток



Распределение критичных инцидентов по времени суток



Распределение критичных внешних 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

SOLAR SECURITY
software&services

Инциденты информационной безопасности и регуляторные требования

Данный раздел показывает, какая часть инцидентов была выявлена благодаря тому, что компания следует требованиям регуляторов, изложенным в рамках того или иного требования или стандарта.

Применительно к финансово-кредитным организациям мы рассматривали инциденты в разрезе требований стандарта PCI DSS.

Применительно к государственным и промышленным компаниям – в разрезе методических рекомендаций по эксплуатации ведомственных и корпоративных центров ГосСОПКА.

Все инциденты

Финансовый сектор – инциденты, предусмотренные стандартом PCI DSS, составляют **9,2%** от общего количества.

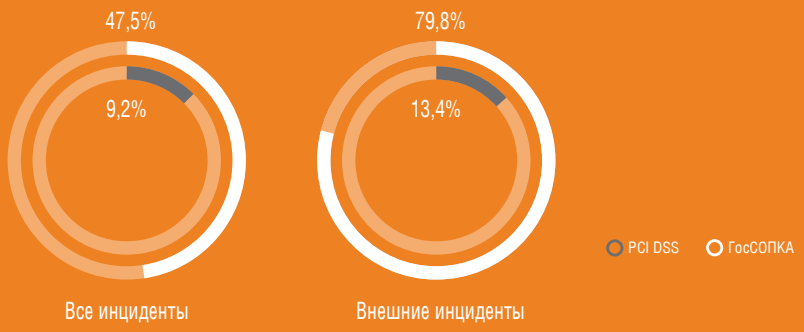
Государственные и промышленные компании – инциденты, предусмотренные методическими рекомендациями, составляют **47,5%** от общего количества.

Внешние инциденты

Финансовый сектор – инциденты, предусмотренные стандартом PCI DSS, составляют **13,4%** от общего количества.

Государственные и промышленные компании – инциденты, предусмотренные методическими рекомендациями, составляют **79,8%** от общего количества.

Доля инцидентов, выявленных благодаря соблюдению требованию регуляторов



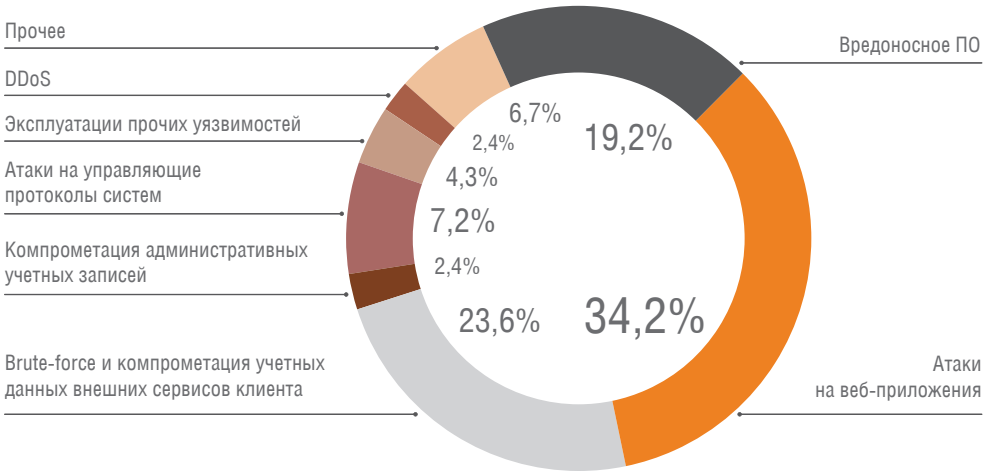
Данный показатель можно считать **маркером эффективности отраслевых стандартов**, поскольку он отражает полноту предписаний регуляторов. Как можно видеть из данных выше, методические рекомендации по эксплуатации ведомственных и корпоративных центров ГосСОПКА позволяют выявить большинство внешних атак. Поскольку стандарт в принципе устанавливает требования к мерам защиты от внешнего злоумышленника, такой результат можно считать очень хорошим.

PCI DSS, в свою очередь, регулирует меры защиты как от внешнего, так и от внутреннего нарушителя. Однако фокус стандарта на конкретных сегментах и бизнес-процессах не позволяет давать полноценный обзор безопасности банковской организации, поэтому соблюдение требований стандарта позволяет выявить меньше десятой части всех инцидентов в финансово-кредитных организациях.

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



В отдельную категорию мы выделяем атаки, состоящие из нескольких последовательных шагов зломышленников, формирующих **Kill Chain**. Данные атаки не завершаются на этапе первого успеха по получению доступа к конкретной подсистеме и доступным на ней данным, а характеризуются последовательными попытками злоумышленника как можно глубже закрепиться в инфраструктуре с тем, чтобы контролировать ее для получения финансовой или прочей выгоды.

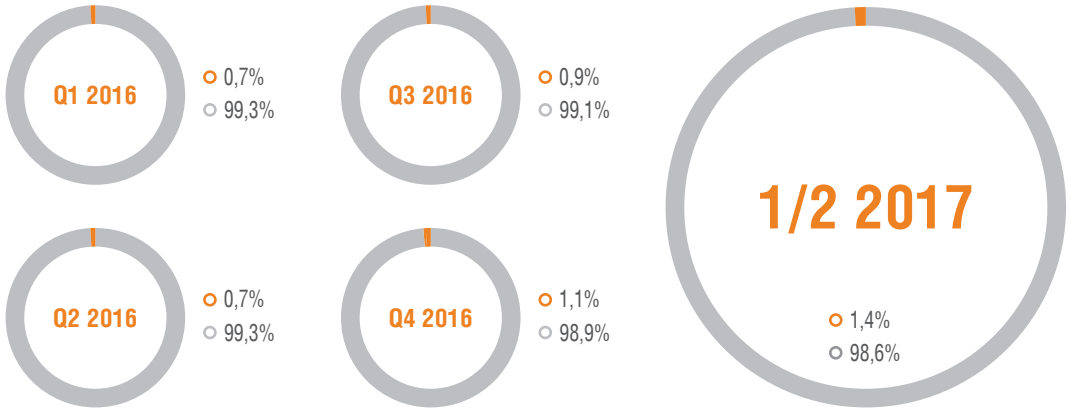
Kill Chain (англ. – «убийственная цепочка») – последовательность действий злоумышленника, осуществляющего проникновение в информационную систему. В первом полугодии 2017 года аналитики Solar JSOC чаще всего (в 87% случаев) сталкивались со следующей моделью атаки: после фазы первого проникновения в сеть компании (статистика описана ниже, см. стр. 7) злоумышленники пытаются выявить наиболее уязвимый сервер инфраструктуры (зачастую используя сканирование сети как промежуточный инструмент). В качестве такого уязвимого узла могут выступать серверы с необновленными версиями операционной системы. Злоумышленники стараются захватить контроль над сервером, чтобы в кратчайшие сроки получить доступ к привилегированным учетным записям сети (технологическим учетным записям, записям ИТ-администраторов), из-под которых они смогут скрытно получать доступ к большому количеству объектов инфраструктуры.

Внешние инциденты

В 13% случаев первым шагом служила атака на веб-приложение (например, онлайн-банк), в 25% – на управляющие протоколы систем (в том числе использование уязвимости Shellshock, известной с сентября 2014 года), в 62% – внедрение в организацию вредоносного программного обеспечения через email-вложения или фишинговые ссылки.

Однако зачастую те или иные этапы развития атаки оказываются еще проще в реализации: например, пароли от привилегированных учетных записей обнаруживаются на файловых серверах или в конфигурации скриптов управления системным ПО в открытом виде. Не редки случаи, когда пароли от технологических учетных записей прописываются на уровне контроллера домена в комментариях (пометках) к самой УЗ и доступны для чтения всей организации, что, безусловно, упрощает злоумышленникам задачу по получению доступа к ним.

Классификации атак



SOLAR SECURITY
software&services

Внешние инциденты

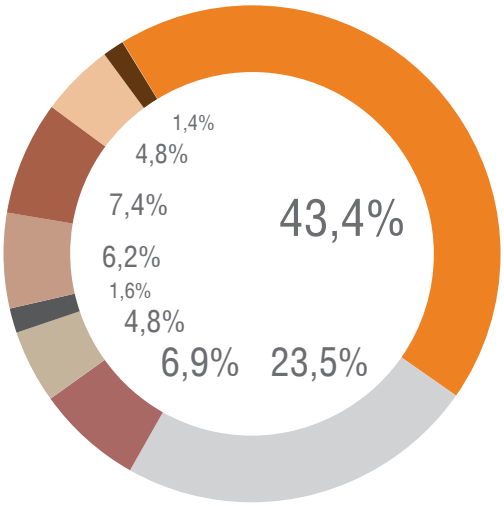
Интересные наблюдения:

- В среднем в течение месяца в общем доступе в сети Интернет публикуется от 2 до 5 сервисов заказчиков с критичными уязвимостями, не устранявшимися около года. Такие публичные сервисы позволяют злоумышленникам без особой подготовки и сложных инструментов проникнуть в корпоративную сеть компании и развивать атаку на критичные системы. Из них 2/3 публикуются администраторами ненамеренно, без ведома служб информационной безопасности, тем самым создавая существенный риск компрометации инфраструктуры.
- Тренд к росту числа вирусов-шифровальщиков не сдает позиций. Однако если раньше аналитики чаще имели дело с вредоносным ПО, чьей единственной функцией является шифрование данных на зараженной рабочей станции, то теперь шифрование, как правило, является лишь одной из функций. Все чаще ей сопутствуют keylogger и возможность удаленного управления зараженной рабочей станцией. Таким образом, инструментарий злоумышленников становится более многозадачным.
- Отдельно хотелось бы подчеркнуть, что, несмотря на массовые атаки Wannacry и Petya, цифры по внешним инцидентам демонстрируют высокий, но не драматический рост. Причина состоит в том, что массовые атаки на российские компании происходят регулярно, но, как правило, остаются вне поля зрения СМИ.
- Снизилось количество случаев компрометации учетных данных удаленного доступа. Ранее первым шагом атаки на компанию часто был взлом учетных записей ее сотрудников в публичных почтовых сервисах (Mail.ru, Yandex.ru, Gmail.com), поскольку пользователи часто устанавливают один и тот же пароль для различных учетных записей. Постепенное внедрение механизмов двухфакторной аутентификации и усложнению алгоритмов доступа в российских компаниях позволило снизить эффективность этого метода атаки.

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

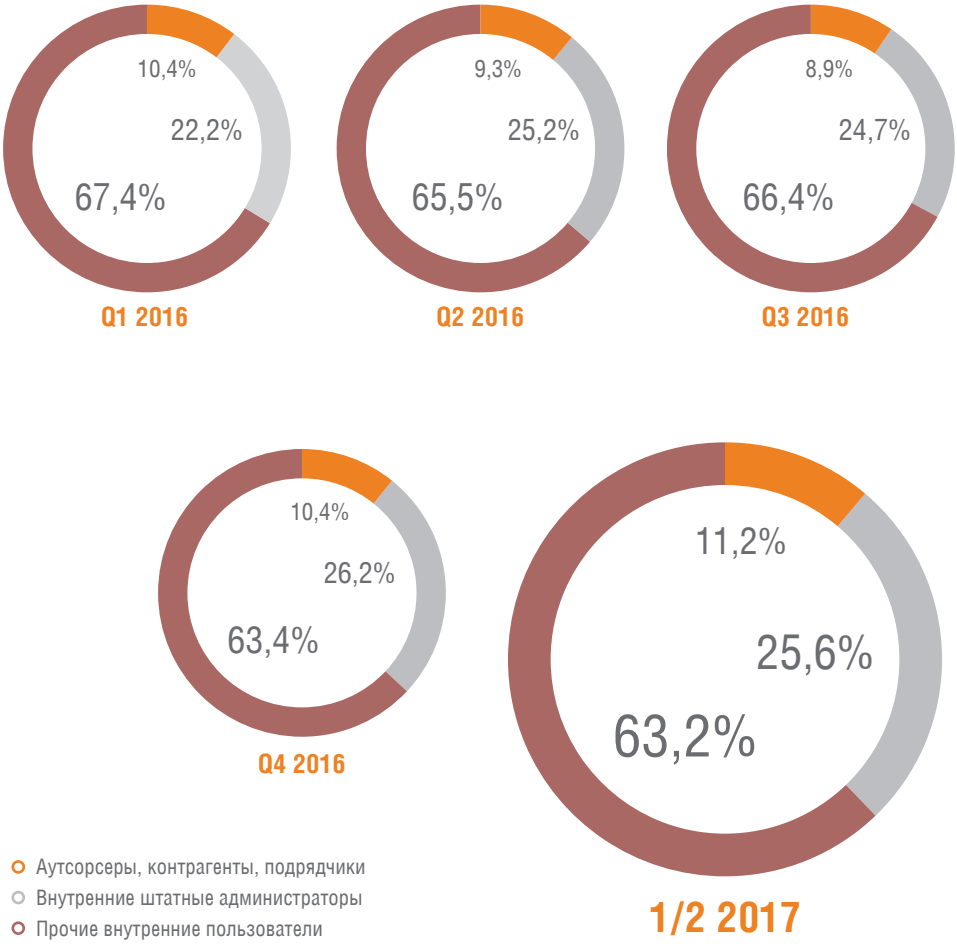
Интересные наблюдения:

- Несмотря на то, что учетные записи удаленного доступа достаточно редко подвергаются компрометации, количество инцидентов, связанных с удаленной работой подрядчиков, растет. По нашим наблюдениям это связано с ростом популярности сервисов ИТ-аутсорсинга при невысоком уровне информационной безопасности в ИТ-аутсорсерах.
- Информационная образованность пользователей растет, но не в том ключе, который хотели бы видеть офицеры безопасности: в среднем раз в два месяца у заказчиков Solar JSOC фиксируются попытки использования рядовыми сотрудниками вредоносных или хакерских утилит. Например, утилит, позволяющих получить информацию о паролях пользователей (procdump, mimikatz), систем сканирования сети и поиска уязвимостей и т.д. Помимо желания нанести прямой вред компании, сотрудниками зачастую двигает обыкновенное любопытство.

2017
первое полугодие

Внутренние инциденты

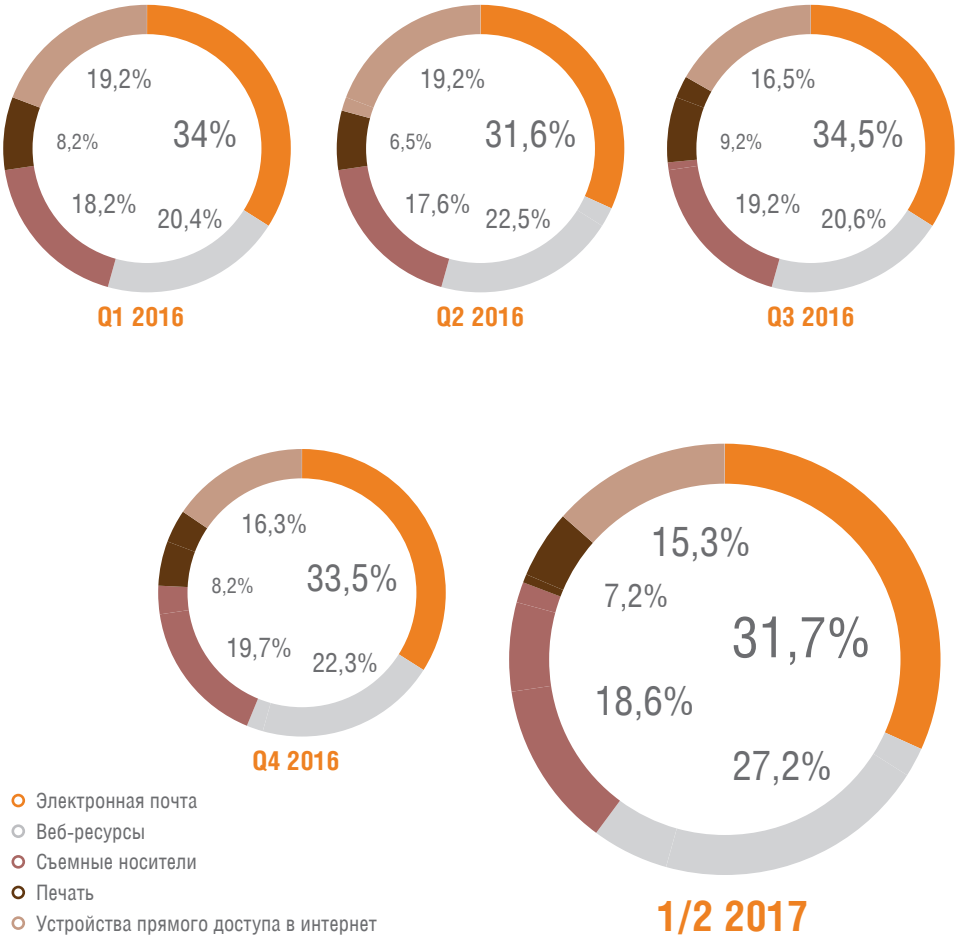
Инициаторы внутренних инцидентов



Мы видим, что в течение года доля инцидентов, виновниками которых были рядовые сотрудники компании, стабильно снижалась за счет прироста числа нарушителей из числа администраторов и внешних подрядчиков. Это можно объяснить ростом популярности обучающих мероприятий для сотрудников по повышению security awareness. Благодаря им компаниям удалось избежать части непредумышленных нарушений политик информационной безопасности.

Внутренние инциденты

Распределение по каналам утечек



В данном разрезе мы наблюдаем два тренда: повышение числа утечек через веб-ресурсы и снижение – через электронную почту и устройства прямого доступа. По нашему мнению, это может быть связано с распространением **блокировок сайтов на уровне законодательства**. Все чаще на рабочих местах сотрудников встречается ПО, которое позволяет обходить блокировки для выполнения функциональных задач. Параллельно оно дает возможность обращаться к веб-ресурсам (файлообменникам, почтовым серверам), ранее закрытым для доступа с рабочего места. Получение таких «скрытых» возможностей и влияет на используемые сотрудниками каналы.

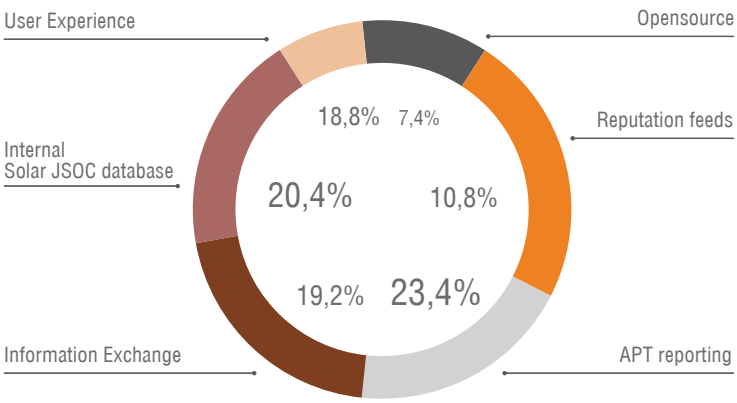
Threat Intelligence

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.).

Статистика по использованию разных типов Intelligence в детектировании инцидентов.



Статистика показывает, что правильное использование бесплатных источников информации о TI может повысить защищенность компании и устойчивость от массовых атак. Но не менее половины инцидентов выявляется только при помощи платных коммерческих подписок.