SOLAR JSOC SECURITY FLASH REPORT

Первое полугодие 2018 года

Ростелеком-Solar

Solar JSOC security flash report первое полугодие 2018 года

Отчет Solar JSOC security flash report основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за первое полугодие 2018 года. В документе отражена сводная информация о выявленных инцидентах по различным категориям. Отчет демонстрирует, кто, как, в какое время и с использованием каких векторов и каналов атаковал российские компании.

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

Оглавление

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

Методология

Общие положения

Solar JSOC Security flash report базируется на анализе инцидентов, выявленных командой Solar JSOC как в рамках оказания своих регулярных услуг мониторинга и реагирования на кибератаки, 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 информационным материалом и не претендует на то, что приведенные данные полностью отражают все угрозы информационной безопасности 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 JSOC для оказания сервиса, составил 28 миллиардов.

- Всего за первое полугодие 2018 года в Solar JSOC было зафиксировано 357 706 событий с подозрением на инцидент, что в два раза больше, чем в первом полугодии 2017 года (172 477). За первое полугодие 2016 года было выявлено 123 549 событий с подозрением на инцидент. Как можно видеть, год от года увеличивается не только число событий с подозрением на инцидент, но и темп прироста.

- В первом полугодии 2018 года доля критичных инцидентов составила 18,7%, в первом полугодии 2017 года критичными были признаны 17,2%, в первом полугодии 2016 года – 10,9%. Таким образом, если в 2016 году критичным был каждый 9 инцидент, то теперь – уже каждый 5. Это рекордная отметка за последние 4 года. 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 17,3 минуты. Среднее время с момента возникновения инцидента до получения заказчиком аналитической справки и рекомендаций составило 22,6 минуты по критичным инцидентам и 71,4 минут – по всем остальным.

[2] Здесь и далее сравниваются показатели за аналогичные периоды разных лет, т.е. первое полугодие с первым, второе – со вторым. Исследователи считают такую методику наиболее корректной ввиду ежегодно наблюдаемой тенденции к росту числа инцидентов во второй половине года и снижению – в первой.

- 71,2% 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 (28,9%), 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 (88,5%) происходила днем, однако, если говорить о критичных инцидентах, когда организацию атаковали извне, то почти в половине случаев (48,9%) они происходили ночью. Это самый высокий показатель с начала 2014 года.

- Почти в полтора раза выросло количество атак, направленных на получение контроля над инфраструктурой. Злоумышленники стремятся к долгосрочному и незаметному присутствию в ней с целью детального исследования и получения как можно более глубокого доступа к информационным и технологическим системам.

- В ходе атаки киберпреступники чаще всего пытаются взломать веб-приложения организаций (33,6%), заразить серверы и рабочие станции пользователей вредоносным ПО (22,5%) или подобрать пароли к учетным записям на внешних сервисах компании (в «личных кабинетах», системах файлового обмена с контрагентами и т.д.), в том числе с помощью простого перебора (21,7%).

- В первой половине 2018 года сложные внешние кибератаки еще чаще, чем раньше (71% против 62% в первом полугодии 2017), начинались с внедрения вредоносного ПО в инфраструктуру компании через социальную инженерию: пользователи открывали вредоносные вложения и проходили по фишинговым ссылкам. Без преувеличения, на данный момент фишинговые атаки представляют собой одну из ключевых угроз для информационной безопасности организаций.

- Инциденты, связанные с действиями внутренних злоумышленников, распределились следующим образом: утечки конфиденциальных данных – 42,1%, компрометация внутренних учетных записей – 22,6%, нарушение политик доступа в интернет – 9,3%.

- В первой половине 2018 года в 60,5% случаев виновниками внутренних инцидентов становились рядовые сотрудники компаний, в 28% – администраторы ИТ-систем, в 11,9% - аутсорсеры, контрагенты или подрядчики компаний.

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 / Mission Critical.

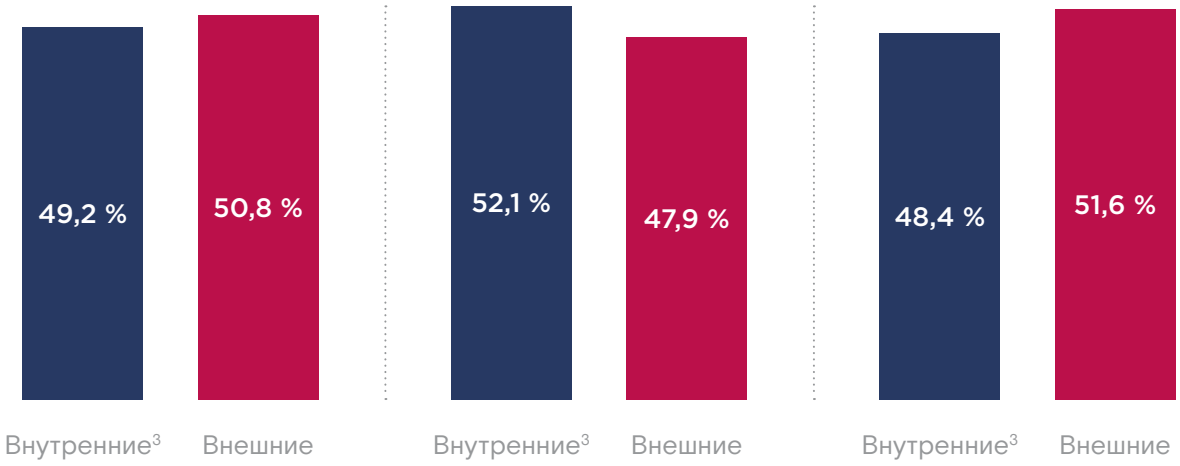
- Повреждение, потеря или компрометация критичной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам.

- Прямые финансовые потери на сумму более 1 млн рублей.

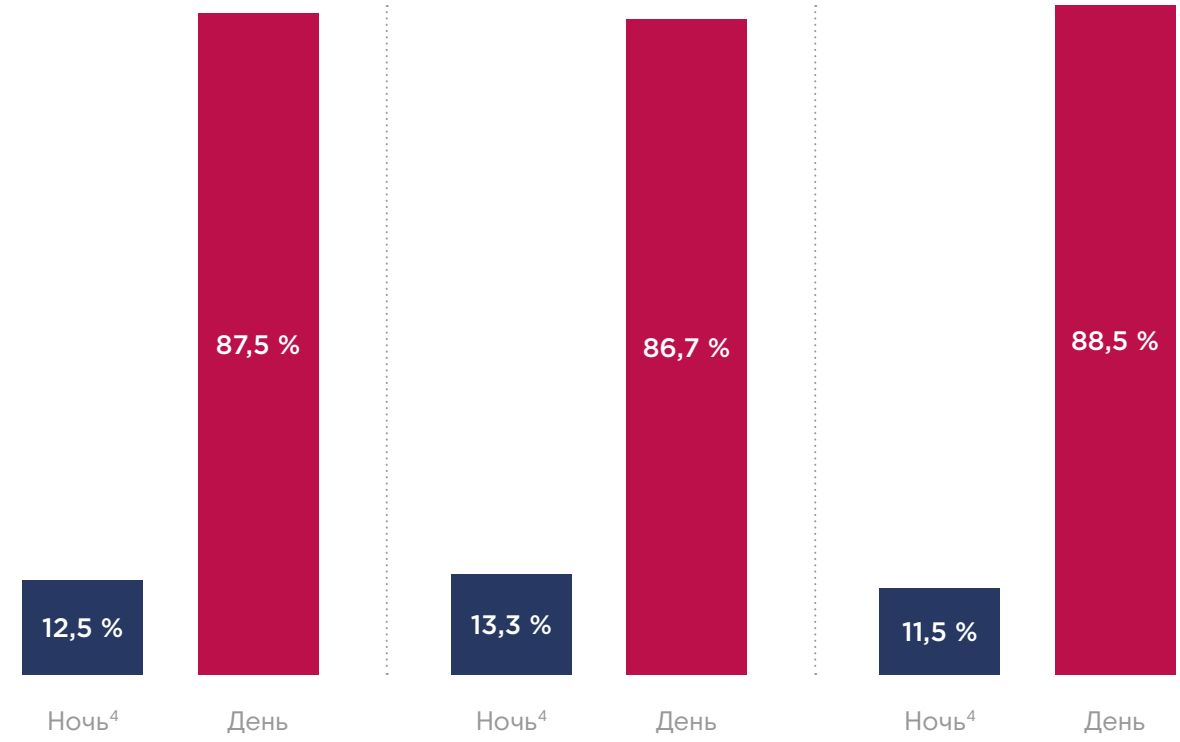
Общие показатели по инцидентам

Первая половина 2017 года	Вторая половина 2017 года	**Первая половина 2018 года**

Распределение инцидентов по внешним и внутренним



Распределение общего числа инцидентов по времени суток

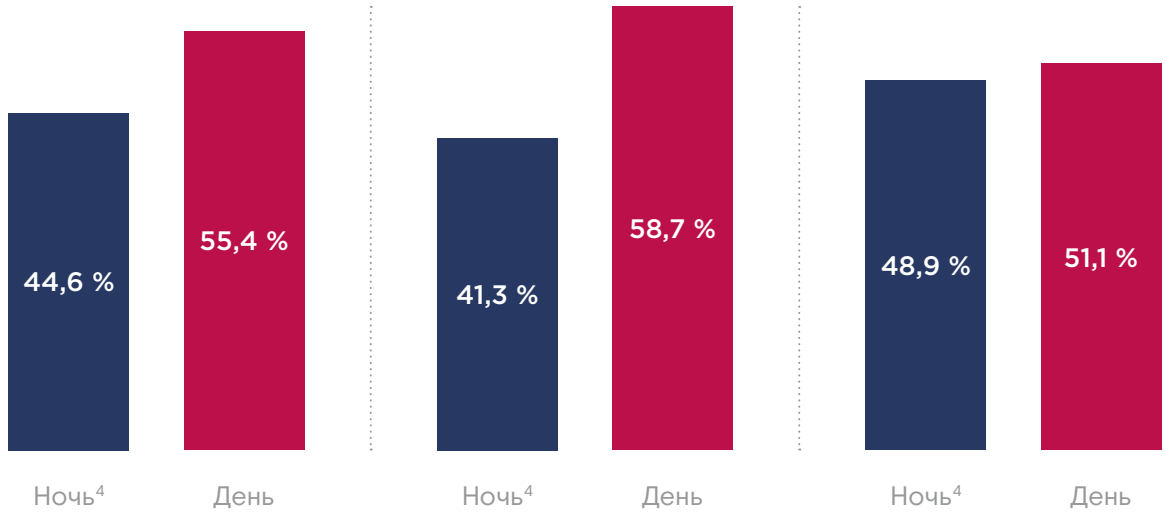


[3] К внутренним пользователям-инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты.

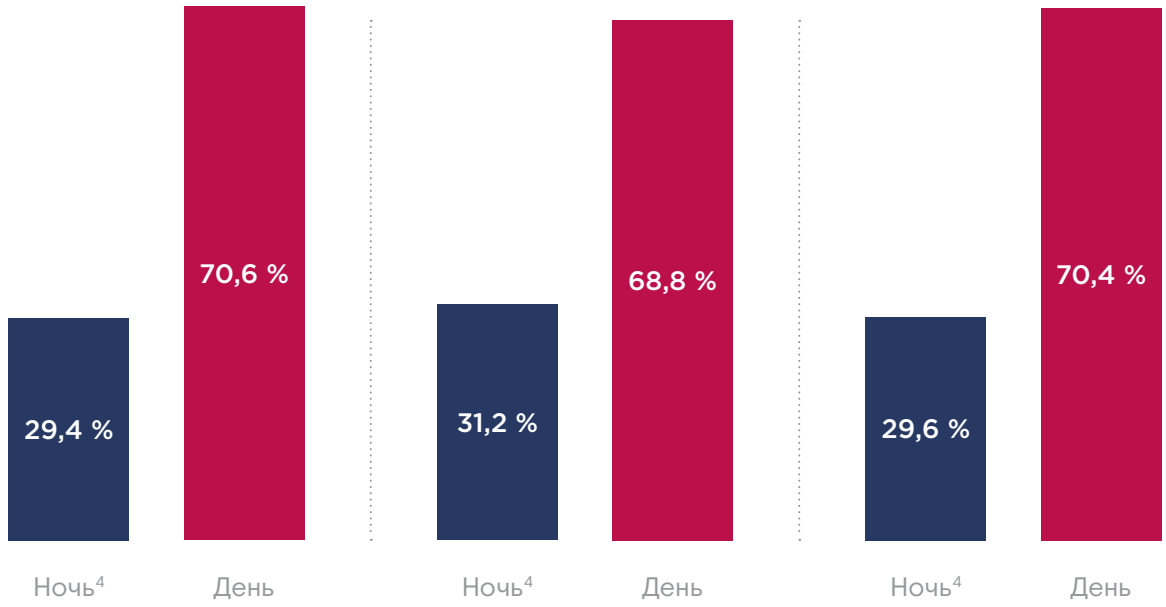
[4] С 21:00 до 8:00 утра по времени расположения офиса присутствия специалистов информационной безопасности Заказчика

Первая половина 2017 года	Вторая половина 2017 года	**Первая половина 2018 года**

Распределение критичных внешних инцидентов по времени суток



Распределение критичных инцидентов по времени суток



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

[4] С 21:00 до 8:00 утра по времени расположения офиса присутствия специалистов информационной безопасности Заказчика

Цели атак – ключевые тренды

В этом году в отчет впервые включено распределение атак по целям злоумышленника. Определение итоговой цели зависит от действий киберпреступника в инфраструктуре, функциональных возможностей вредоносного ПО, внедренного в компанию, и т.д. Аналитика учитывает как внешние, так и внутренние атаки.

- Существенно (почти на 50% по сравнению с аналогичным периодом прошлого года) выросло количество атак, направленных на получение контроля над инфраструктурой. Злоумышленники стремятся к долгосрочному и незаметному присутствию в ней с целью детального исследования и получения как можно более глубокого доступа к информационным и технологическим системам.

- На 10% выросло количество атак, направленных на кражу денежных средств. Однако стоит отметить, что развитие информационного обмена в рамках сообщества все чаще позволяет пресечь атаки на ранних стадиях и не позволить киберпреступникам вывести денежные средства из организаций.

- Заметен сильный тренд к уменьшению числа «хулиганских» кибератак, таких как дефейс или компрометация публичных сайтов, порча и уничтожение данных. Их количество снизилось на 45% по отношению к первому полугодию 2017 года. Вероятными причинами можно считать снижение активности от «злоумышленников-любителей» в связи с вступлением в силу федерального закона и большую нацеленность профессионалов на монетизацию услуг.

- Существенно развивается инструментарий атакующих: в среднем за неделю мы фиксируем появление 5-6 новых инструментов для реализации атаки, причем все чаще для их разработки используются легитимные элементы операционной среды либо популярные средства удаленного администрирования и управления операционными системами.

Внешние инциденты

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

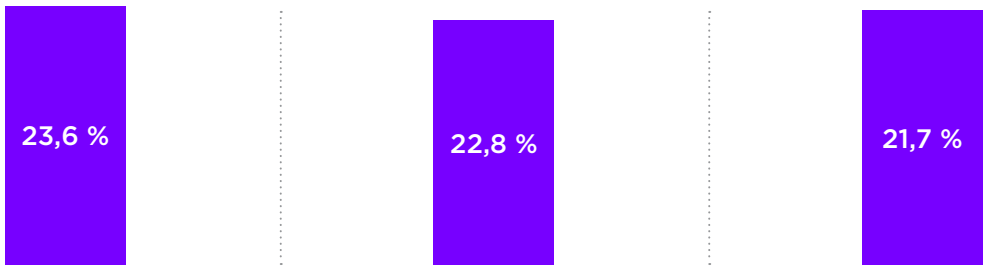
Направления атак

Первая половина 2017 года	Вторая половина 2017 года	**Первая половина 2018 года**

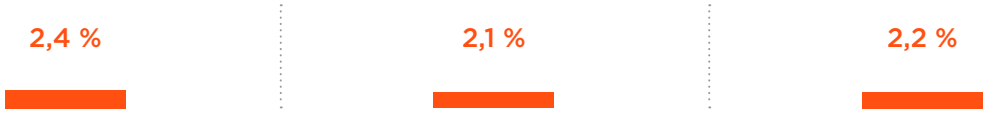
Вредоносное ПО

Атаки на веб-приложения

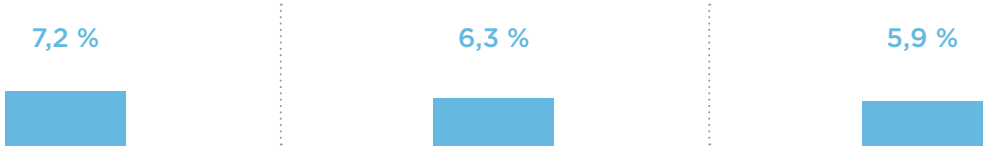
Brute force и компрометация учетных данных внешних сервисов клиента



Компрометация административных учетных записей

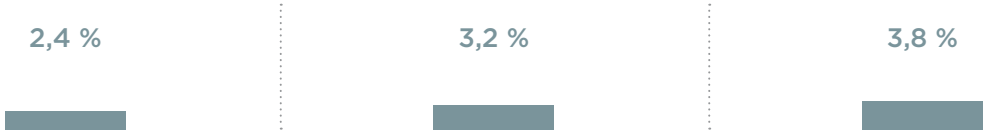


Атаки на управляющие протоколы систем

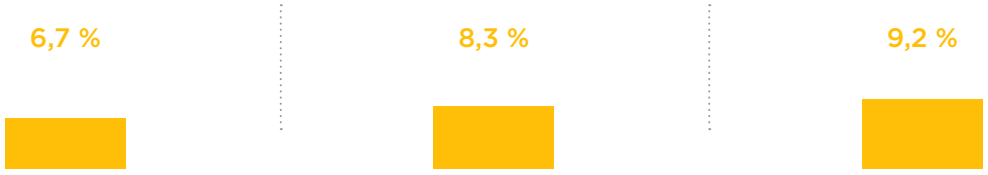


Эксплуатации прочих уязвимостей

DDoS



Прочие внешние атаки: атаки на сетевой стек, уязвимости DNS, нарушение защищенного периметра, фишинг



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 проникновения в сеть компании злоумышленники пытаются выявить наиболее уязвимый сервер инфраструктуры, например, сервера с не обновленными 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. В абсолютном большинстве случаев Kill Chain сводится к этому алгоритму, варьируются лишь способы проникновения злоумышленника в инфраструктуру.

Во первой половине 2018 года в 3% 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 20% случаев использовалась атака на веб-приложение (например, онлайн-банк), в 6% – на управляющие протоколы систем, и в 71% – путем внедрения в организацию вредоносного программного обеспечения через email или фишинговые ссылки.

Инструменты киберпреступников для проникновения в инфраструктуру компаний

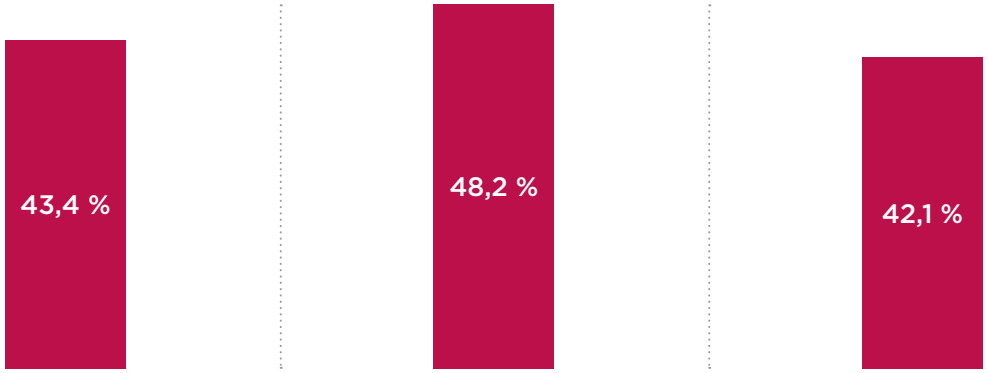
Внутренние инциденты

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

Направления атак

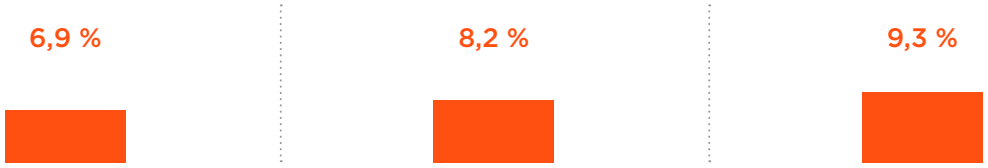
Первая половина 2017 года	Вторая половина 2017 года	**Первая половина 2018 года**

Утечки конфиденциальных данных

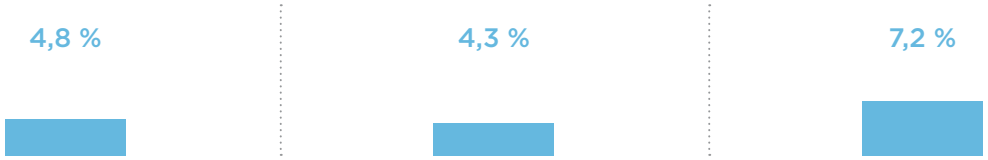


Компрометация внутренних учетных записей

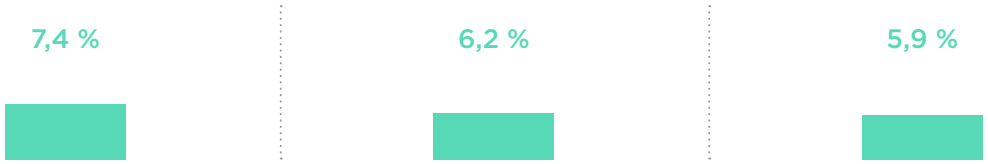
Нарушение политик доступа в Интернет, в том числе использование TOR-клиентов, использование анонимайзеров и посещение хакерских форумов



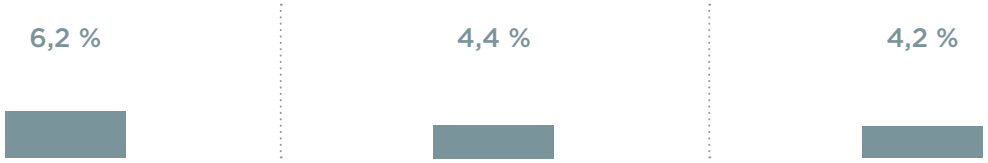
Использование Remote Admin Tools или инструментов туннелирования трафика



Нелегитимные работы под привилегированными учетными записями

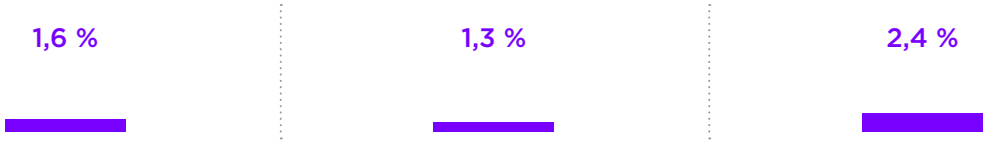


Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критичных бизнес систем



Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер

Использование хакерских и потенциально вредоносных утилит



Прочее

Инициаторы внутренних инцидентов

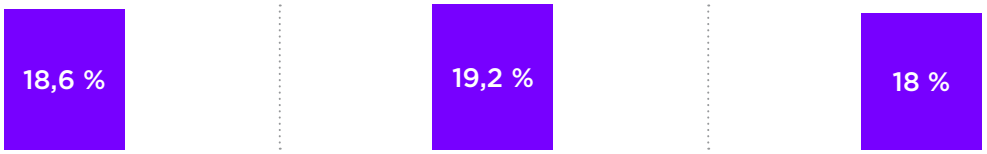
Распределение по каналам утечек

Первая половина 2017 года	Вторая половина 2017 года	**Первая половина 2018 года**

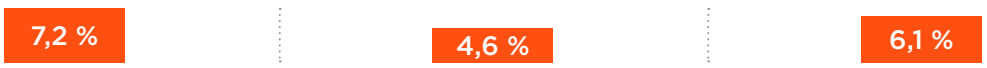
Электронная почта

Веб-ресурсы

Съемные носители



Печать



Устройства прямого доступа в интернет (3-4G модемы, телефон как модем и т.д.)

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.

- 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.).

Ниже приведена статистика по использованию разных типов Intelligence в детектировании инцидентов.

Тип Intelligence	Доля инцидентов, детектированных с помощью TI
Opensource	8,4%
Reputation feeds	20,1%
APT reporting	17,6%
Information Exchange	24,5%
Internal JSOC database	20,2%
User Experience	9,2%

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.