JSOC Security flash report Q1 2016

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

Ключевые выводы

1. 70% атак реализуются через незакрытые уязвимости web-сервисов и слабые парольные политики бизнес-систем.

2. Количество критичных внешних инцидентов, происходящих в ночное время, продолжает расти и составляет уже 48,5%.

3. В Q1 2016 отмечается некоторое снижение числа DDoS-атак по сравнению с Q4 2015, но их уровень более чем в 2 раза выше, чем в аналогичном периоде Q1 2015.

4. Информационные бюллетени FinCERT позволили выявить 13 подтвержденных инцидентов, из которых в 9 случаях совместное реагирование со службой клиента позволило целиком предотвратить ущерб от атаки.

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

© Solar Security
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 первый квартал 2016 года в Solar JSOC было зафиксировано **54 726 событий** с подозрением на инцидент, в то время как за аналогичный период 2015 года их количество составило только 34 743. Прирост за год составил 58%, что обусловлено подключением новых клиентов к сервисам Solar JSOC в 2015 году и запуску новых сценариев мониторинга инцидентов в ранее подключенных организациях.
- В первом квартале 2016 года доля критичных инцидентов составила 10,6%, что ниже аналогичного показателя в **Q4 2015 года, равного 12,4%**. Это связано с общим снижением бизнес-активности подключенных компаний в начале года.
- Среднее время принятия инцидента в работу специалистом JSOC с момента выявления составило **18,6 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций по критичным инцидентам составило **22,5 минуты и 84,2 минуты** по всем остальным с момента возникновения инцидента.
- Соблюдение клиентских SLA за первый квартал 2016 года составило **98,8%**. Данная метрика постоянно поддерживается на высоком уровне и не опускалась ниже **98,3%** за весь 2015 год.
- **56,3%** 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 **(43,7%),** 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.

Классификация инцидентов по критичности

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

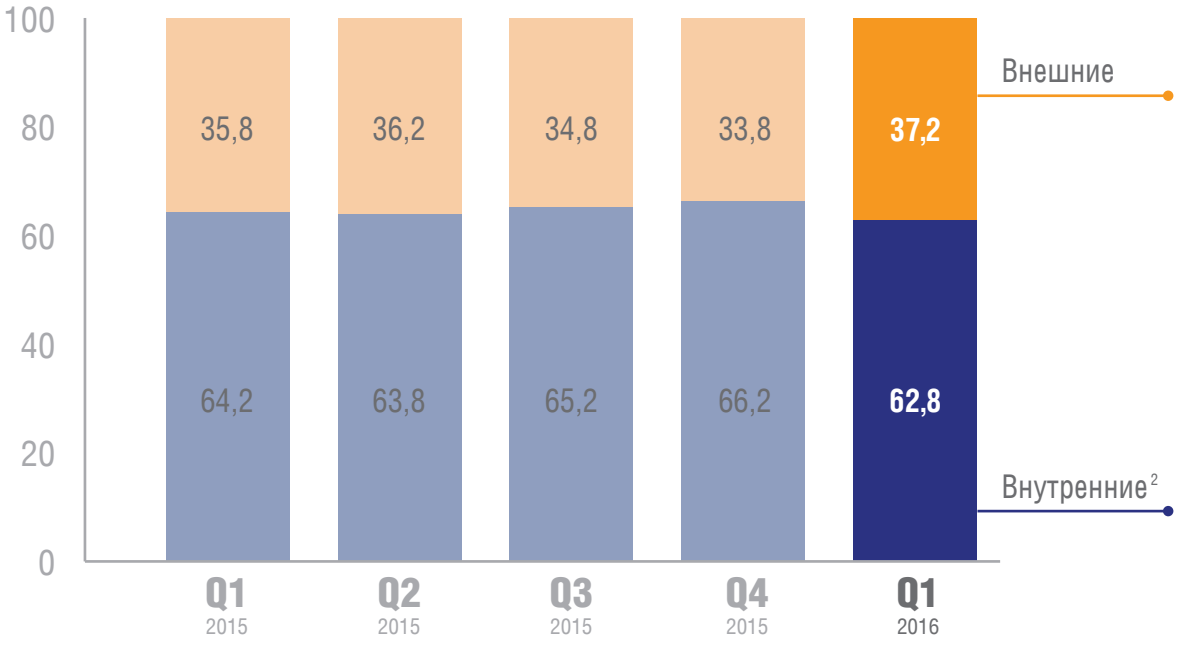
Инцидент считается критичным, если в результате него возможны и высоковероятны следующие события:

- 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

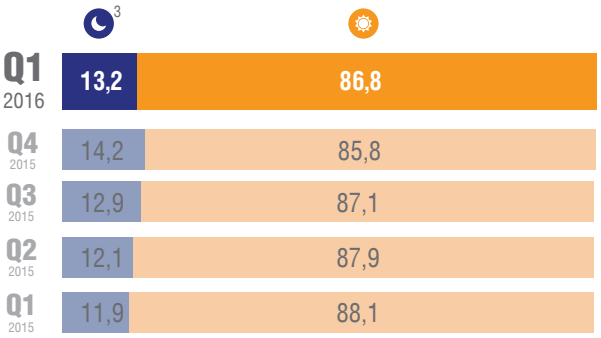
Q1 2016

Распределение инцидентов по внешним и внутренним

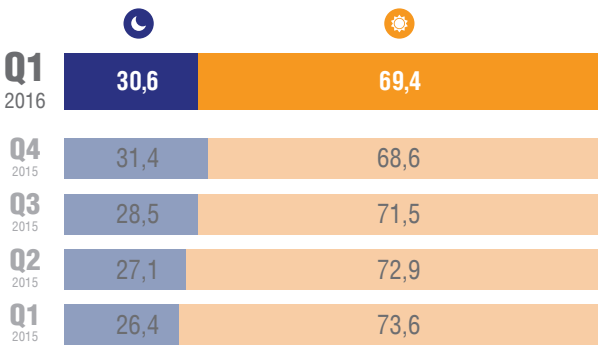


Распределение количества инцидентов по времени суток

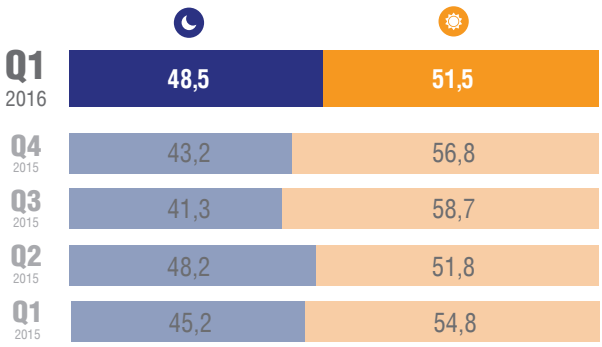
Время суток:



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.

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

Общие показатели по инцидентам

В первом квартале 2016 года отмечается существенный рост количества внешних инцидентов – с 33,8% в Q4 2015 до 37,2% в Q1 2016, что в абсолютных значениях означает: число событий с подозрением на инцидент, обрабатываемых 1 линией Solar JSOC, увеличилось на 2 981. Проведенные в Q4 2015 года внутренние мероприятия по численному и методологическому усилению команды дежурных линий Solar JSOC обеспечили соблюдение клиентских SLA.

Доля критичных ночных инцидентов продолжает оставаться на высоком уровне: на протяжении периода с Q1 2015 до Q1 2016 их уровень повышается. Незначительная коррекция с 31,4% в Q4 2015 до 30,6% в Q1 2016 лишь отражает сезонный характер данного показателя, а аналитики Solar JSOC ожидают продолжения незначительного роста доли критичных ночных инцидентов в 2016 году.

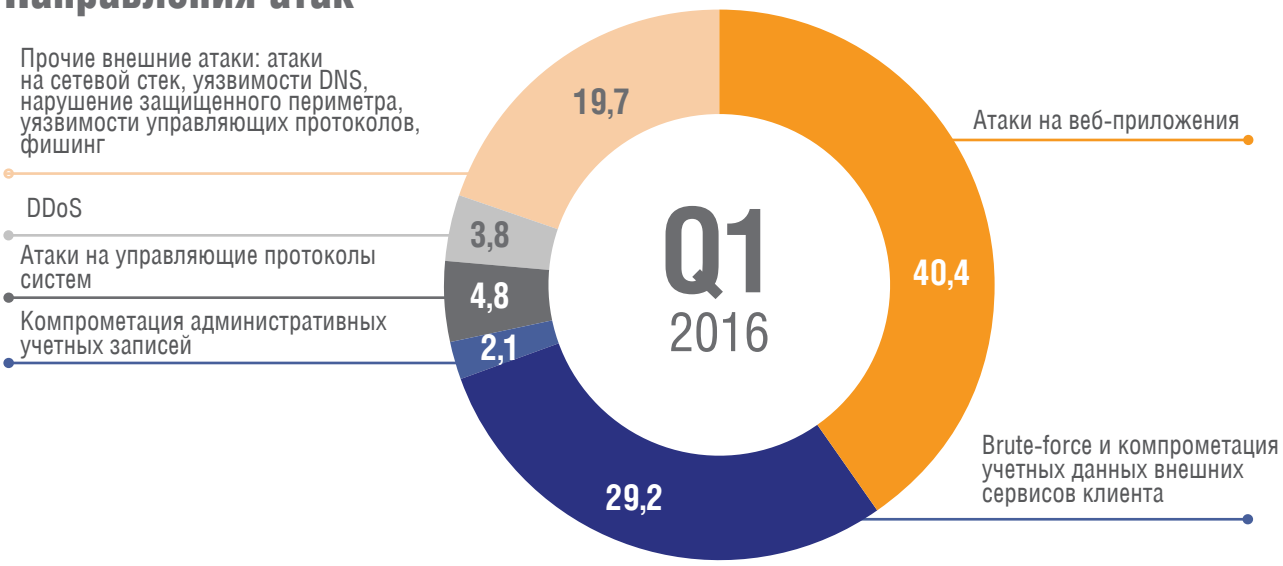
Количество ночных критичных внешних инцидентов продолжает расти и составляет уже 48,5%. Это тревожная ситуация для большинства компаний-клиентов, так как зачастую требует оперативной реакции в нерабочее время и задействования ресурсов как ИБ-, так и ИТ-департаментов.

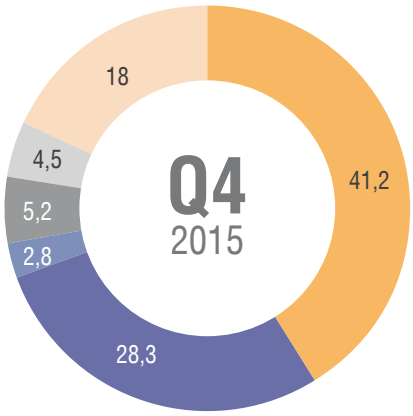
Внешние инциденты

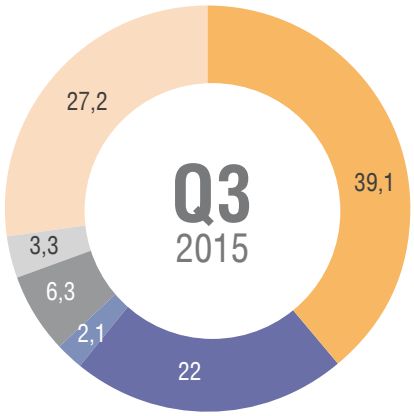
Q1 2016

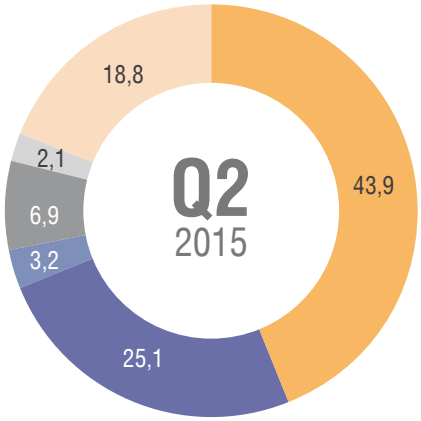
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся сотрудниками компании-клиента. «Простые атаки», а именно, действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не влекущие к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

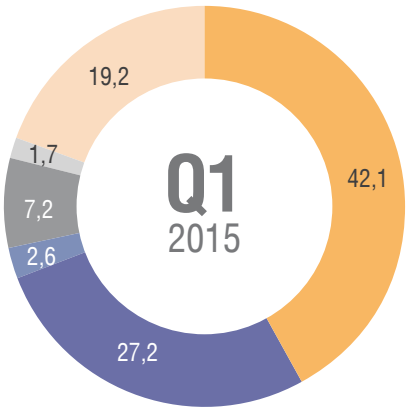
Направления атак











Особенности внешних инцидентов в первом квартале 2016 г.:

- Вектор внешних атак на инфраструктуры компаний-клиентов направлен на взлом web-приложений и лишь немного скорректировался в сторону компрометации учетных данных внешних сервисов. По-прежнему порядка 70% атак реализуются через незакрытые уязвимости web-сервисов и слабые парольные политики бизнес-систем.

- В Q1 2016 отмечается некоторое снижение числа DDoS атак по сравнению с Q4 2015, но их уровень более чем в 2 раза выше, чем в аналогичном периоде Q1 2015. Аналитики Solar JSOC связывают локальный тренд снижения с сезонными факторами, а общий тренд на повышение – с простотой, эффективностью и дешевизной организации DDoS-атак.

- Отмечается незначительный рост числа прочих внешних атак, сигнализирующий об интересе злоумышленников к применению специальных техник и творческого подхода к реализации атак.

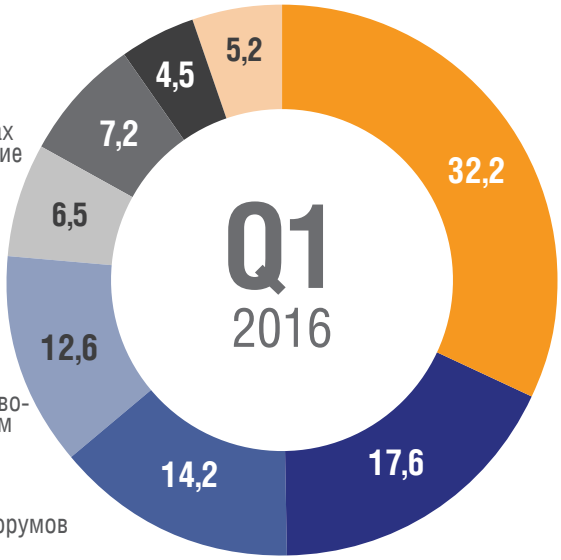
Аналитики Solar JSOC прогнозируют сохранение тренда на повышение числа DDoS-атак на инфраструктуры компаний-клиентов и акцентируют внимание на необходимости своевременной защиты для успешного и оперативного отражения подобных атак. Уязвимости web-приложений будут под прицелом большинства векторов угроз, так как их эксплуатация является самым распространенными способом получения доступа к информационным ресурсам компаний.

Внутренние инциденты

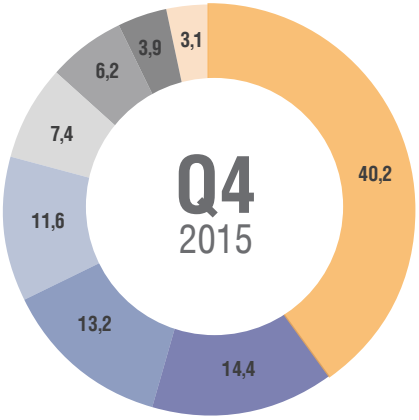
В данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников компаний-клиентов Solar JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных данных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

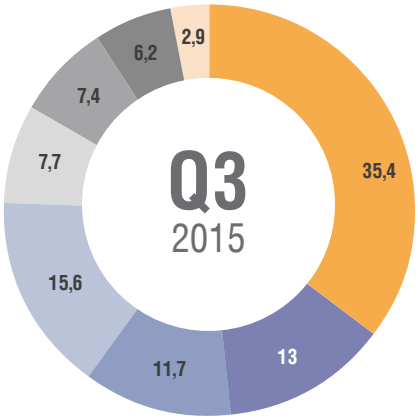
Направления атак

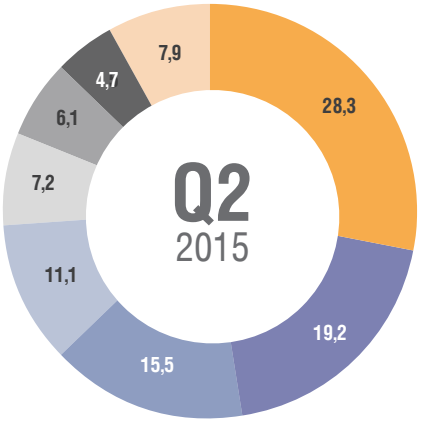
- Утечки конфиденциальных данных
- Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер
- Нелегитимные работы под привилегированными учетными записями: внутренние пользователи
- Нелегитимные изменения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

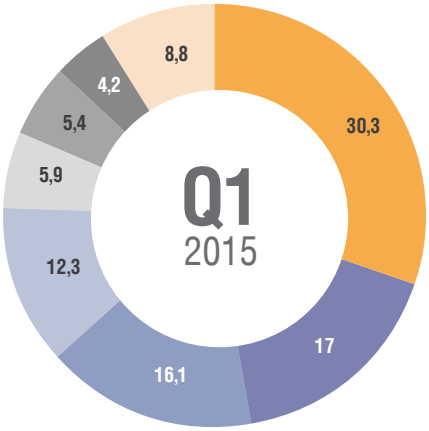


- Вирусные атаки, включая массовые вирусные заражения, действия ransomware и поведенческое выявление zero-day
- Прочее
- Компрометация внутренних учетных записей

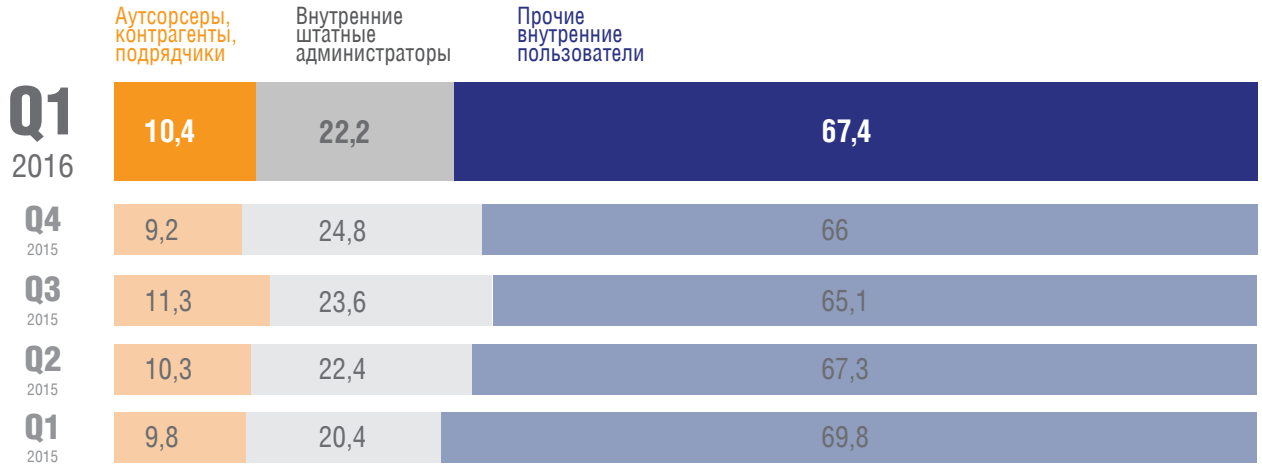




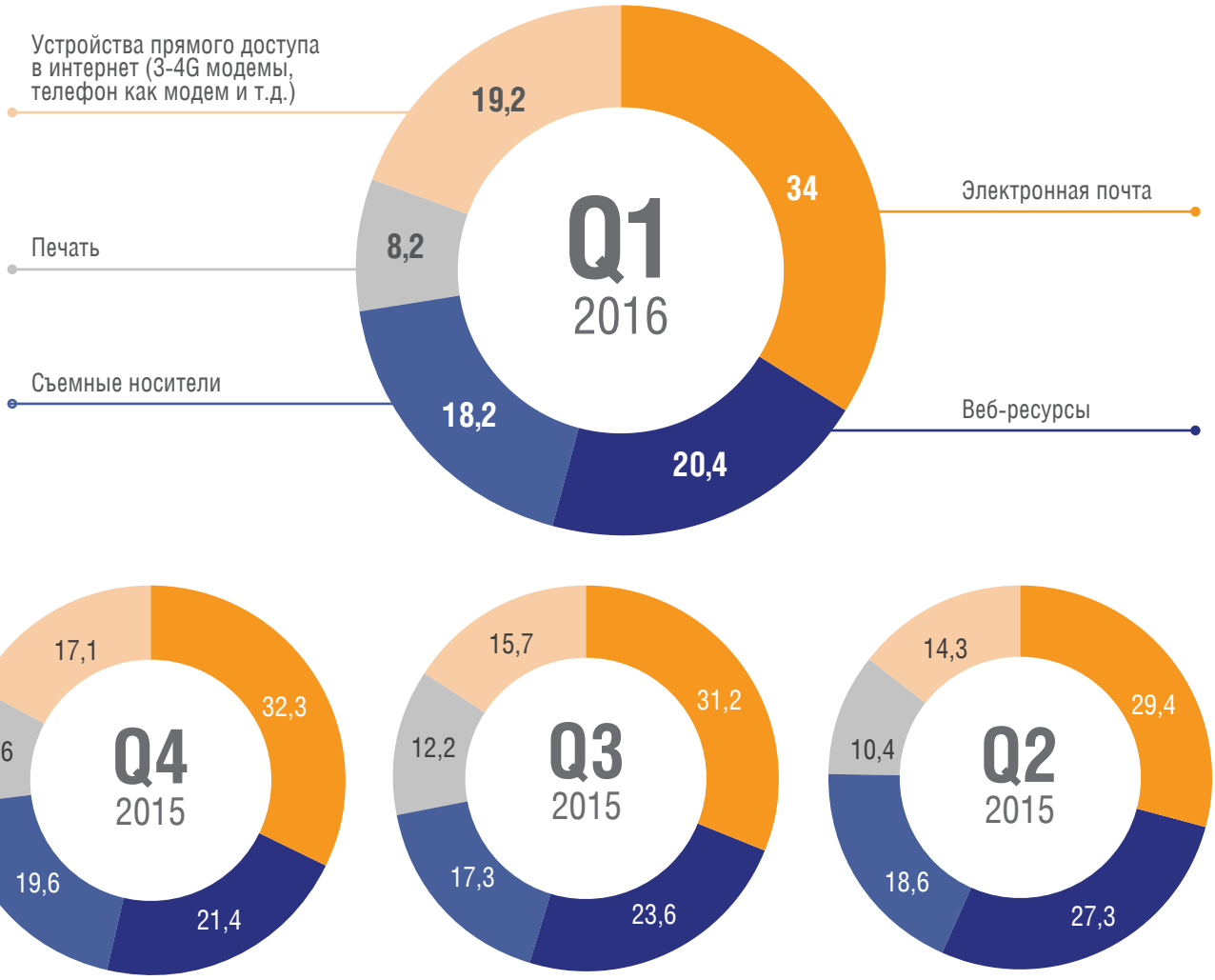




Инициаторы внутренних инцидентов



Распределение инцидентов по каналам утечек



Особенности внутренних инцидентов в первом квартале 2016 г.:

- Наблюдается снижение доли утечек конфиденциальных данных по сравнению с Q4 2015 и возвращение на уровень Q1 2015. Аналитики Solar JSOC связывают это с наличием годовых циклов в ведении бизнеса, так что на протяжении всего 2016 года доля утечек будет расти и может составить до 40-45% от всех внутренних инцидентов к концу года. Рекомендуется уделять проблеме утечек данных повышенное внимание, так как они зачастую наносят серьезный ущерб компании.

- Несмотря на некоторый спад в Q4 2015 доля инцидентов, связанных с нелегитимной работой из-под привилегированных учётных записей, в Q1 2016 снова повысилась. Данный вектор угроз популярен среди сотрудников, имеющих повышенные полномочия в ИБ- и ИТ-системах, и поэтому требует особого контроля со стороны бизнеса и ключевых руководителей.

- Штатные сотрудники и администраторы являются инициаторами инцидентов в 89,6% зарегистрированных в Solar JSOC случаях. При этом доля нарушений со стороны подрядчиков, контрагентов и аутсорсинговых компаний сохраняется на уровне 10-11%. Важно подписывать с внешними компаниями, получающими доступ к ресурсам компании, не только соглашения о конфиденциальности, но и вводить технические меры контроля и мониторинга их действий. Хорошей практикой должно стать прописывание ответственности контрагентов за нарушения политик ИБ обслуживаемой компании.

Результаты использования информации об угрозах от FinCERT

За первый квартал 2016 командой Solar JSOC было получено 34 информационных бюллетеня 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 4 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 Q1 2016 командой Solar JSOC была собрана следующая статистика:

- Признаки наличия сетевых индикаторов обнаружены по 15 бюллетеням в 26 подключенных компаниях (одни бюллетени встречались в нескольких компаниях), причем 4 случая были определены как подтвержденные инциденты с проведенными дальнейшими расследованиями.
- Признаки наличия хостовых индикаторов обнаружены по 12 бюллетеням в 16 подключенных компаниях, причем только 7 случаев определены как ложные срабатывания.

Из 13 выявленных и подтвержденных инцидентов в 9 случаях совместное реагирование со службой клиента позволило целиком предотвратить какой-либо ущерб от возникшего инцидента. В оставшихся 4 случаях, связанных с работой вирусов-шифровальщиков, оперативное взаимодействие команды Solar JSOC с клиентом позволило существенно минимизировать ущерб (сузить область фактического шифрования данных, минимизировать время на восстановление данных из резервных копий).

Ключевые выводы

- 70% атак реализуются через незакрытые уязвимости web-сервисов и слабые парольные политики бизнес-систем.
- Количество критичных внешних инцидентов, происходящих в ночное время, продолжает расти и составляет уже 48,5%.
- В Q1 2016 отмечается некоторое снижение числа DDoS-атак по сравнению с Q4 2015, но их уровень более чем в 2 раза выше, чем в аналогичном периоде Q1 2015.
- Информационные бюллетени FinCERT позволили выявить 13 подтвержденных инцидентов, из которых в 9 случаях совместное реагирование со службой клиента позволило целиком предотвратить ущерб от атаки.

JSOC

Solar JSOC – первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ, являющийся провайдером сервисов безопасности (MSSP).

На всех этапах мониторинга и реагирования на инциденты ИБ Solar JSOC обеспечивает защиту клиентских данных. Обеспечение безопасности реализовано как на физическом, так и на информационном уровне с помощью средств разграничения доступа, аудита работы специалистов Solar JSOC, контроля целостности и защиты данных при передаче. Solar JSOC сертифицирован по требованиям PCI DSS, что подтверждает зрелость процессов обеспечения безопасности.

Уже более десятка клиентов получают аутсорсинговые услуги Solar JSOC. Сервис по мониторингу инцидентов был запущен в 2013 году, став первым подобным коммерческим центром в России. Сейчас в штате Solar JSOC более 30 специалистов дежурной смены, аналитиков и экспертов, которые обрабатывают более 100 000 событий с подозрением на инциденты в год.

Сервисы Solar JSOC

- Мониторинг инцидентов
- Контроль защищенности
- Противодействие кибепреступности
- Эксплуатация систем ИБ
- Анализ кода приложений
- Анти-DDoS
- Защита web-приложений

О компании Solar Security

Solar Security – это команда, создающая продукты и сервисы, позволяющие выстроить вертикаль управления и мониторинга ИБ, начиная с низкоуровневых инцидентов и заканчивая системами стратегической аналитики и ситуационными центрами по информационной безопасности.

Solar Security – это команда с двадцатилетним опытом разработки продуктов и собственная исследовательская лаборатория по анализу и прогнозированию инцидентов информационной безопасности. Наши знания позволяют гарантировать нашим клиентам уверенность в контроле над ситуацией в постоянно меняющемся мире внутренних и внешних киберугроз.

Solar Security – это продукты и сервисы, удобные в использовании и простые в восприятии. Они упрощают работу сотрудников ИБ, повышая их эффективность. Мы делаем технологии доступными руководителям и сотрудникам подразделений информационной безопасности, позволяя им выбрать удобный канал доставки в виде сервиса, приложения и комплексной системы.

Этот отчет был подготовлен компанией Solar Security исключительно в целях информации. Содержащаяся в настоящем отчете информация была получена из источников, которые, по мнению компании Solar Security, являются надежными, однако компания Solar Security не гарантирует точности и полноты информации для любых целей. Информация, представленная в этом отчете, не должна быть истолкована, прямо или косвенно, как информация, содержащая рекомендации по инвестициям. Все мнения и оценки, содержащиеся в настоящем материале, отражают мнение компании на день публикации и подлежат изменению без предупреждения. Компания Solar Security не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования любой третьей стороной информации, содержащейся в настоящем отчете, включая опубликованные мнения или заключения, а также за последствия, вызванные неполнотой представленной информации. Информация, представленная в настоящем отчете, получена из открытых источников либо предоставлена упомянутыми в отчете компаниями. Дополнительная информация предоставляется по запросу.