JSOC Security flash report Q3 2015

Отчет **JSOC Security flash report Q3 2015** основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за третий квартал 2015 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 утечек реализовывал угрозы ИБ.

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

Оглавление

Ключевые выводы

1. Подтверждена прямая взаимосвязь между ростом доли внутренних инцидентов и экономическими факторами. С усилением экономической неустойчивости доля внутренних инцидентов стабильно увеличивается. Эта тенденция хорошо видна на данных Q4'14-Q1'15 и в Q3'15

2. На протяжении трех кварталов 2015 года наблюдается устойчивый рост числа утечек по каналу печати и устройств прямого доступа (3/4G USB-модемы, Wi-Fi точки доступа смартфонов)

3. В Q3'15 впервые за 2015 год отмечено существенное снижение числа инцидентов, связанных с вирусными заражениями, ransomware и с компрометацией учетных записей пользователей. Мы связываем это с усилением технических политик ИБ и применением внутренними службами ИБ рекомендаций, выданных Solar JSOC

4. В Q3'15 наблюдается снижение доли атак на веб-приложения. Это связано с ростом прочих внешних атак, например, фишинга и уязвимостей протоколов. Пока сложно предсказать, долгосрочная ли это тенденция

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 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 российского рынка. Команда Solar JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации.

Сводная статистика за отчетный период

- Всего за третий квартал 2015 года в Solar JSOC было зафиксировано **54 578** событий с подозрением на инцидент, что на **14 %** выше, чем аналогичный показатель в Q2'15.
- Доля критичных инцидентов составила **8,2 %** от общего числа.
- Среднее время принятия инцидента в работу специалистом Solar JSOC с момента выявления составило **22,5 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций клиенту Solar JSOC по критичным инцидентам составило **29,2 минуты** и **89,6 минуты** по всем остальным.
- Соблюдение клиентских SLA за третий квартал составило **99,3 %**.
- **63,4 %** исследуемых событий зафиксировано при помощи основных сервисов инфраструктуры и базовой безопасности: межсетевые экраны и сетевое оборудование, VPN, AD, почтовые серверы, базовые средства защиты (антивирусы, прокси-серверы, IPS).
- При этом стоит отметить, что оставшиеся инциденты (**36,6 %**), выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации и критичность для информационной и экономической безопасности клиента. Информация по данным инцидентам позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные, таргетированные инциденты.

Классификация инцидентов по критичности

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

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

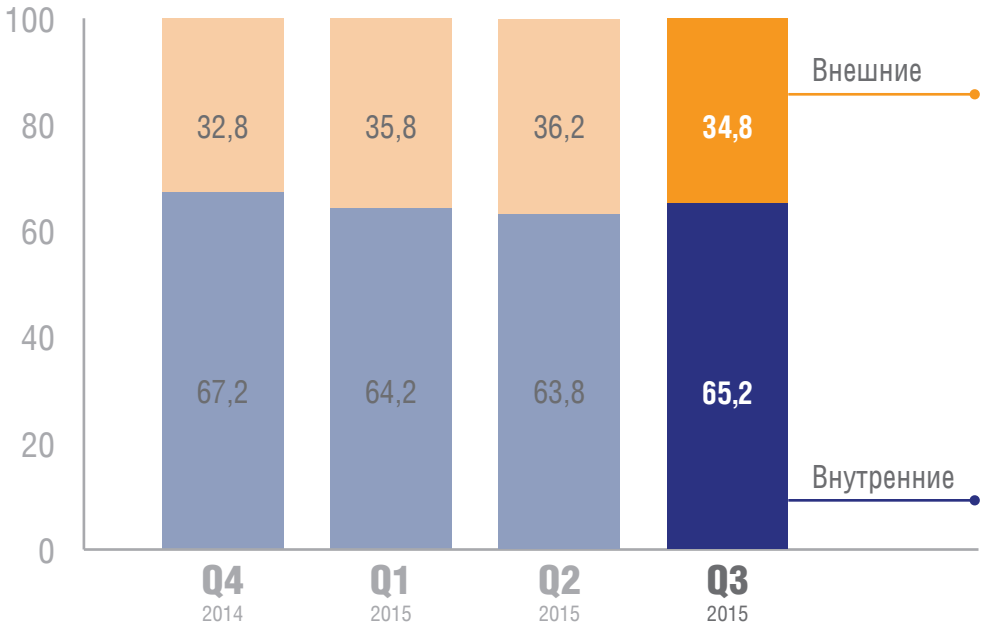
- длительное прерывание (более получаса) или остановка функционирования систем и сервисов клиента, относящихся к категориям Business и Mission Critical;
- повреждение, потеря или компрометация критичной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам;
- прямые финансовые потери в результате действий внутренних сотрудников или киберпреступников суммой более 1 млн рублей.

Общие показатели по инцидентам

Q3 2015

Распределение инцидентов по внешним и внутренним[1]

в %-ном соотношении от общего числа:



Распределение количества инцидентов по времени суток

Общее распределение по времени суток (в %):

Q3 2015	12,9	87,1
Q2 2015	12,1	87,9
Q1 2015	11,9	88,1
Q4 2014	11,1	88,9

Распределение по критичным инцидентам (в %):

Q3 2015	28,5	71,5
Q2 2015	27,1	72,9
Q1 2015	26,4	73,6
Q4 2014	26,8	73,2

Распределение по критичным внешним инцидентам (в %):

Q3 2015	41,3	58,7
Q2 2015	48,2	51,8
Q1 2015	45,2	54,8
Q4 2014	47,1	52,9

Ночь
С 21:00 до 08:00 по времени расположения офиса заказчика

День
С 08:00 до 21:00 по времени расположения офиса заказчика

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

Ключевые выводы по общим показателям по инцидентам

- Как и на протяжении всего года по-прежнему сохраняется распределение между внутренними и внешними инцидентами в пропорции 65/35. Это объясняется устоявшимся среди клиентов Solar JSOC соотношением выполняемых на сетевом и прикладном уровнях действий внутренними сотрудниками и внешними подрядчиками, аутсорсерами, контрагентами. Доля хакерских внешних атак не оказывает существенного влияния на подобные макропоказатели, но отражается в других разделах по распределению угроз, которые будут представлены в разделе отчета «Внешние инциденты».
- Стоит обратить внимание на изменение соотношения критичных внешних инцидентов по времени суток: дневных внешних инцидентов стало почти на 7% больше. В первую очередь это связано с повышением активности внешних легитимных категорий пользователей, таких как подрядчики, разработчики, службы эксплуатации и аутсорсеры. Такой тренд можно считать сезонным и в Q4'2015 года прогнозируется сохранение или повышение доли критичных внешних инцидентов.
- Тем не менее доля ночных критичных внешних инцидентов сохраняется на очень высоком уровне и сопоставима с дневной активностью, что говорит о целесообразности и необходимости круглосуточного мониторинга инцидентов.

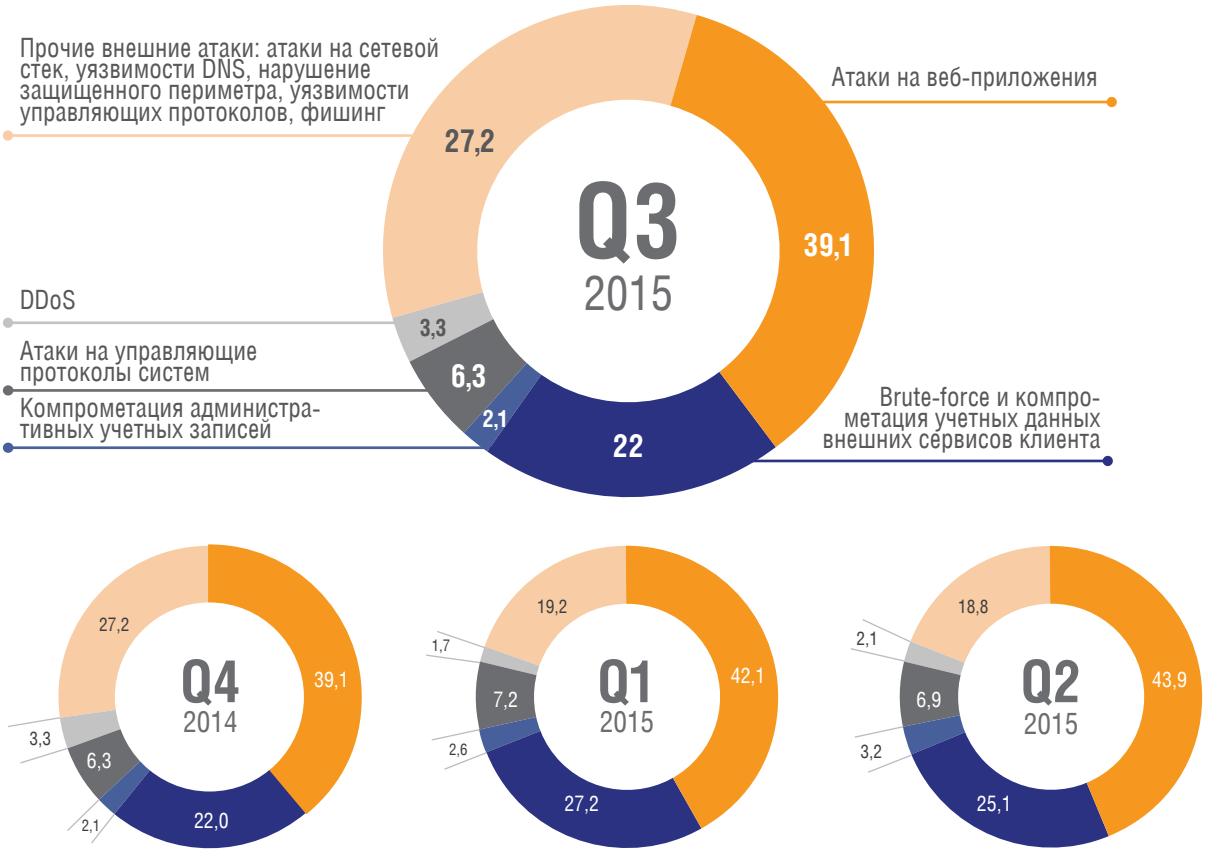
Внешние инциденты

Q3 2015

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 приводящие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей – из отчета исключены.

Направления атак в %-ном соотношении от общего числа:



Особенности внешних инцидентов в третьем квартале 2015 г.

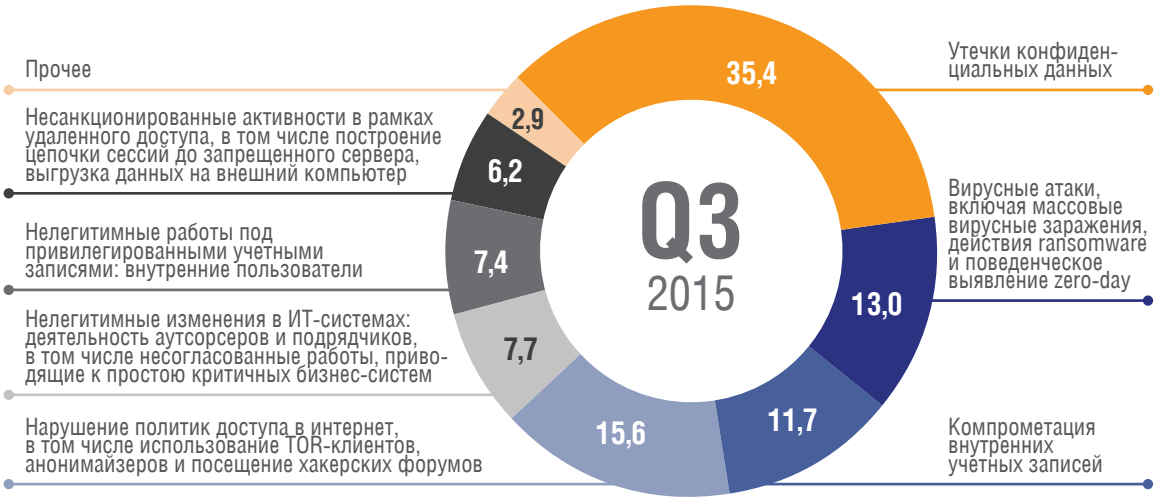
- В течение всего 2015 года наблюдается уверенный рост числа DDoS-атак. По мнению аналитиков Solar JSOC это связано с ростом влияния конкуренции и бизнес-активности, обычно нарастающих к концу календарного года.
- Замечено уменьшение доли атак на веб-приложения до уровней Q3-Q4 2014 года, равно как и снижение уровня угроз, связанных с подбором паролей и компрометацией учетных данных внешних сервисов клиентов.
- Вместе с тем почти всё снижение по первым двум направлениям угроз нашло своё отражение в росте прочих внешних атак, например, фишинге и уязвимостях протоколов. Такие атаки принято относить к фазам разведки и начальной стадии проникновений в инфраструктуру клиентов Solar JSOC.
- Зафиксирована высокая активность очередного варианта вируса Corkow – более 40 российских компаний стали целью злоумышленников. Уже на ранней стадии Solar JSOC зарегистрировал множественные атаки на инфраструктуры клиентов, что позволило остановить распространение вируса и предотвратить финансовые последствия для организаций.

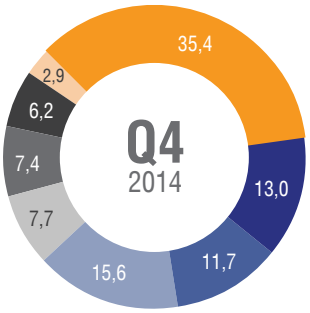
Внутренние инциденты

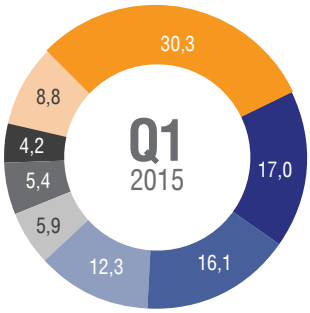
Q3 2015

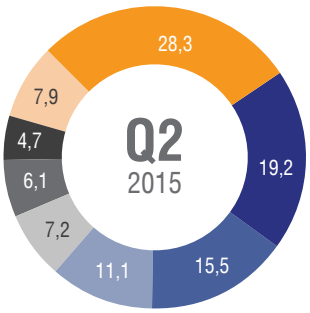
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников клиентов Solar JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных данных сотрудников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

Направления атак в %-ном соотношении от общего числа:









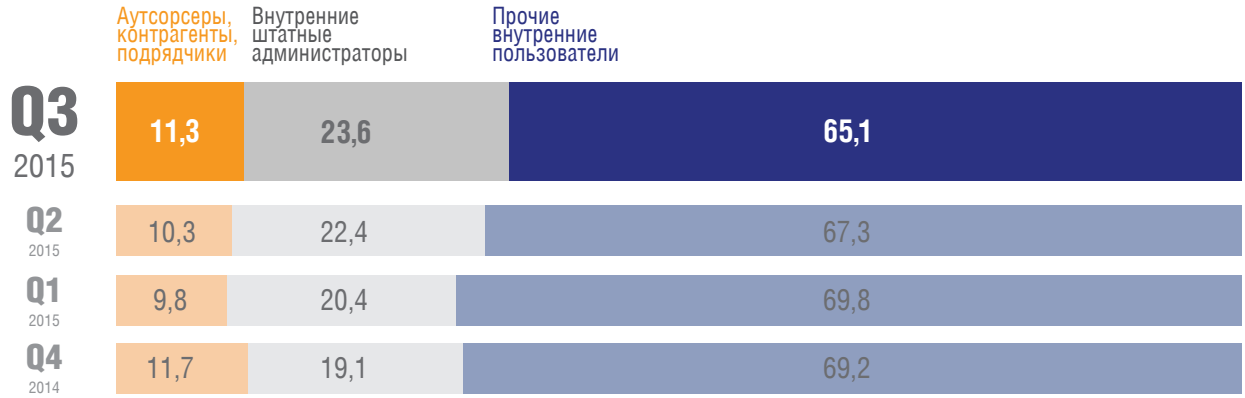
Особенности внутренних инцидентов в третьем квартале 2015 г.

- Впервые за 2015 год замечено существенное снижение числа инцидентов, связанных с вирусными заражениями, ransomware, а также с компрометацией учетных записей пользователей. Мы связываем это с усилением мер защиты ИБ в подключенных компаниях: от ужесточения ряда внутренних политик ИБ до внедрения дополнительных систем анализа вложений в почтовой переписке и при http-передаче. Такое направление деятельности свойственно многим службам ИБ, которые являются клиентами Solar JSOC, поэтому мы прогнозируем дальнейшее снижение доли такого типа атак.
- Не так радужно выглядит ситуация по многим другим направлениям: почти каждый вектор, так или иначе связанный с целенаправленной реализацией внутренним пользователем угроз информационной безопасности, вырос на 2-7%. Такое поведение говорит в целом об ухудшении климата внутри компаний и о желании пользователей намеренно нарушить безопасность информационных активов.

Внутренние инциденты

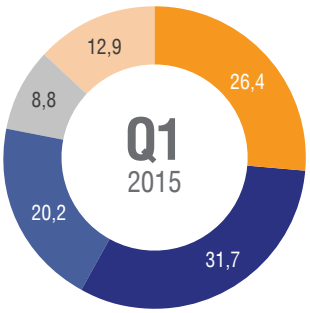
Q3 2015

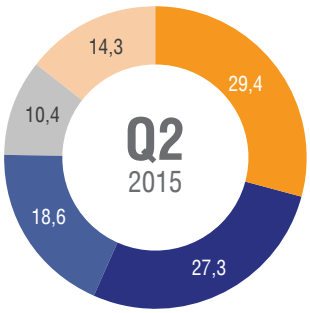
Инициаторы внутренних инцидентов в %-ном соотношении от общего числа:



Распределение инцидентов по каналам утечек

в %-ном соотношении от общего числа:





Данные за период Q4 2014 отсутствуют (ранее не публиковались)

Особенности внутренних инцидентов в третьем квартале 2015 г.

- Отмечается стабильный рост использования устройств прямого доступа в интернет, что соотносится со снижением зарегистрированных утечек через веб-ресурсы. Очевидно, что особое внимание нужно уделять выявлению фактов использования подобных устройств, так как это существенно снижает эффективность мониторинга и уменьшает защищенность корпоративных ресурсов.
- Повышение клиентами Solar JSOC уровня информационной безопасности в части использования съемных носителей далеко не всегда останавливает внутренних пользователей от нарушений принятых политик и норм ИБ. Так, например, снижение доли съемных носителей в качестве канала утечек пропорционально увеличивает долю нарушений при печати или использовании электронной почты.

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

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.