Solar JSOC Security Report
Итоги 2019 года

rt-solar.ru

Ростелеком
Солар

Solar JSOC Security Report

Исследование кибератак на российские организации в 2019 г.

Отчет Solar JSOC Security Report основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за 2019 год. В документе отражена сводная информация о выявленных инцидентах по различным категориям. Отчет демонстрирует, как, в какое время и с использованием каких векторов и каналов атаковали российские компании.

Solar JSOC Security Report предназначен для информирования служб ИТ и ИБ о текущем ландшафте угроз и основных трендах кибератак.

Оглавление

О компании «Ростелеком-Солар»

«Ростелеком-Солар», компания группы ПАО «Ростелеком», – национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

Solar JSOC – первый российский центр мониторинга и реагирования на кибератаки, лидер российского рынка Security Operations Center (SOC).

Список сервисов Solar JSOC:

- Мониторинг, реагирование и анализ инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Сервисы ГосСОПКА (государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)
- Комплексный контроль защищенности
- Техническое расследование инцидентов ИБ
- Построение SOC или его частных процессов

Методология

Solar JSOC Security Report составлен на основе анализа инцидентов, выявленных командой Solar JSOC в 2019 году. В фокус внимания экспертов попало более 100 компаний и организаций из разных отраслей экономики: госсектор, финансы, нефтегазовая отрасль, энергетика, телекоммуникации, крупный ритейл. Все компании представляют сегмент large enterprise и enterprise со средним количеством сотрудников от 1000 человек, оказывают услуги в разных регионах страны и, как правило, являются крупнейшими в отрасли по своему региону или по стране в целом.

Совокупно в рамках оказания сервиса заказчикам Solar JSOC обеспечивает контроль и выявление инцидентов для:

Более 1200

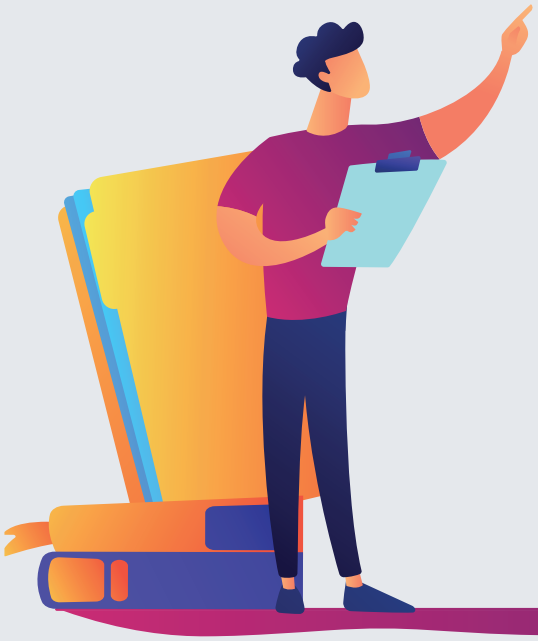
внешних сервисов,
опубликованных в сети Интернет

Более 400 000

сотрудников разных коммерческих и государственных организаций

Более 40 000

серверов общего, прикладного и инфраструктурного назначения



В отчете мы используем следующие ключевые понятия:

Событие информационной безопасности (ИБ) – выявленное состояние системы, указывающее на возможное нарушение политики безопасности, отказ или нарушение мер защиты, или прежде неизвестная ситуация, которая может угрожать безопасности.

Инцидент – появление одного или нескольких нежелательных событий ИБ, которые с высокой долей вероятности могут скомпрометировать бизнес-процессы компании или непосредственно угрожают ее информационной безопасности.

Критичный инцидент – инцидент, который может напрямую повлиять на ключевые бизнес-процессы и информационные ресурсы компании. В частности, привести к остановке работы систем более, чем на полчаса, компрометации критичной информации и учетных записей или прямым финансовым потерям на сумму более 1 млн рублей.

Внешняя кибератака – инциденты, причиной которых становились действия лиц, не являющихся внутренними пользователями организаций.

Внутренняя кибератака – инциденты, причиной которых становились действия внутренних сотрудников организаций.

Внутренние пользователи – все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты.

Одним из ключевых факторов, влияющих на методологию исследования, является проактивность сервисов Solar JSOC, которые позволяют выявлять действия злоумышленников на самых ранних стадиях, до проникновения в инфраструктуру. Это накладывает определенные ограничения на проведение оценки финансового ущерба организации (в силу отсутствия фактических потерь), а также идентификацию целей злоумышленника: направлены ли его действия на получение финансовой выгоды, сбор чувствительной информации, закрепление в инфраструктуре с целью дальнейшей продажи ресурсов, хактивизм или иное. Поэтому при определении целей злоумышленника Solar JSOC использует комбинированную методику, которая опирается на особенности атаки.

При выявлении инцидентов на ранней стадии (до фактического закрепления злоумышленников и развития атаки в инфраструктуре) учитываются используемые техники и методики атаки, функционал используемого вредоносного ПО и его применимость для конкретных целей, атрибуция хакерской группировки и информация о ее типовых целях, информация о схожих атаках (получаемая в рамках информационных обменов или коммерческих расследований инцидентов) с известным ущербом и целями злоумышленников.

При выявлении атаки на фазе распространения (в рамках инцидентов, детектируемых у новых подключаемых заказчиков до момента стабилизации уровня безопасности инфраструктуры) на фактическом перечне скомпрометированных хостов дополнительно учитывается: их территориальная распределенность, функциональное назначение, возможности реализации одной из вышеприведенных целей, а также динамика и вектор движения киберпреступника. Например, если ближайшие шаги злоумышленника после проникновения в инфраструктуру направлены на проникновение на хосты, связанные с финансовыми операциями и выводом денежных средств, то такая атака классифицируется как нацеленная на вывод денежных средств. В случае же если при проведении атаки не задействованы специализированные модули для вывода средств, а ее развитие подразумевает широковещательное получение контроля над различными активами инфраструктуры, то атака классифицируется как нацеленная на захват инфраструктуры.

При выявлении атак на финальной стадии (в рамках расследований инцидентов у новых клиентов, не использующих сервисы мониторинга на момент инцидента) – дополнительно собирается информация о фактическом ущербе, которая в дальнейшем служит ключевым критерием, определяющим вектор атаки.

Из отчета исключены так называемые простые атаки, не ведущие к реальным инцидентам информационной безопасности, – в частности, деятельность автоматизированных систем (бот-сетей), сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей.

Сводная статистика за 2019 год

Среднее время принятия инцидента в работу специалистом Solar JSOC с момента выявления составило 12,2 минуты. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций с момента его возникновения составило 22,8 минуты по критичным инцидентам и 78 минут по остальным.

86,7 млрд составил средний суточный поток событий ИБ, обрабатываемых SIEM-системами и используемых Solar JSOC для оказания сервиса

16% составила доля критичных инцидентов. Это первое за 5 лет снижение данного показателя на годовом периоде

Более 1,1 млн событий с подозрением на инцидент было зафиксировано за 2019 год

99,3% уровень соблюдения клиентских SLA в 2019 году

54,6% событий были зафиксированы с помощью 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). Оставшиеся события информационной безопасности (45,4%) – были выявлены с помощью сложных интеллектуальных средств защиты или анализа событий бизнес-систем, которые позволяют глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные таргетированные атаки. В 2018 году это соотношение составляло 72,1% и 27,9% соответственно. Изменение динамики в сторону увеличения инцидентов, выявляемых с помощью специализированных средств, говорит о том, что атаки злоумышленников стали заметно сложнее и базовые средства защиты все чаще не справляются с их выявлением и предотвращением.

Ключевые тенденции 2019 года

В 2019 году злоумышленники сменили вектор интересов. Виден отчетливый рост **(на 40%)** атак, направленных на получение контроля над инфраструктурой, и снижение **(на 15%)** атак, направленных на кражу денежных средств.

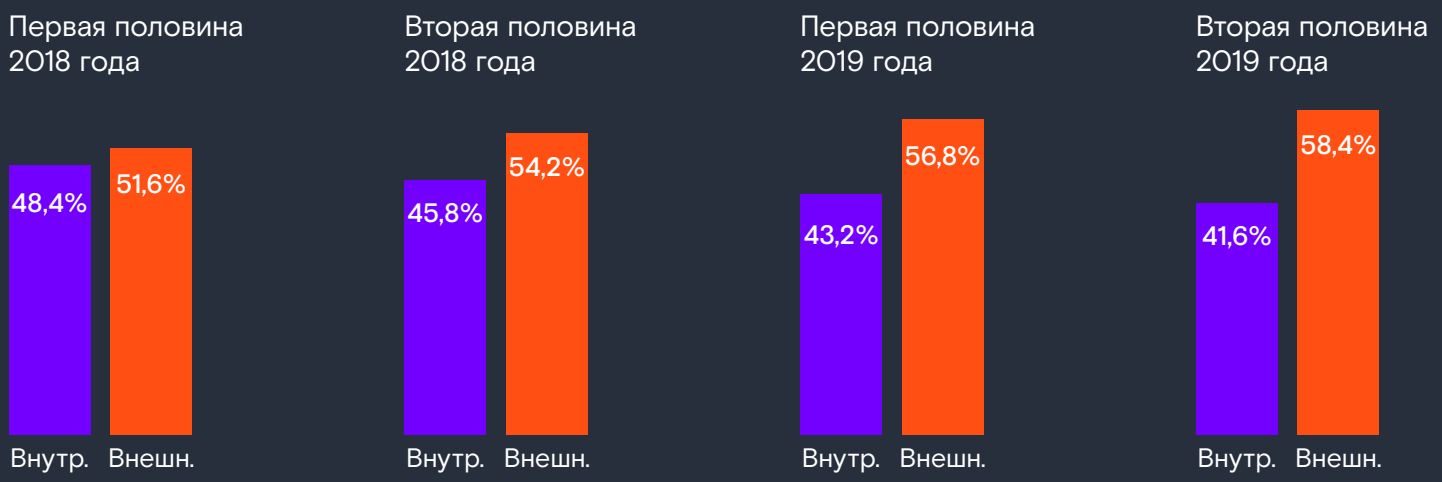
Видна существенная динамика приведения в порядок периметров компаний. Если в 2018 году **более 260 тыс.** российских серверов были подвержены уязвимости EternalBlue, то в 2019 году их число сократилось до **49,7 тыс.** При этом динамика закрытия уязвимостей в России существенно выше средней по миру – российские серверы составляют **менее 5%** от уязвимых в мире. Тем не менее, по оценке Solar JSOC, примерно **40%** уязвимых серверов, принадлежат крупным коммерческим или государственным компаниям. Продолжается рост доли внешних инцидентов от общего числа угроз. Это говорит о том, что внешние злоумышленники стали активнее атаковать компании, тогда как угрозы, исходящие от сотрудников, остались примерно на том же уровне. Если в 2018 году доля внешних кибератак не превышала **54,2%**, то в 2019 году этот показатель достиг **58,4%;**

Если в 2018 году основной функциональностью вредоносного ПО было шифрование данных, то в 2019 оно сменилось на майнинг.

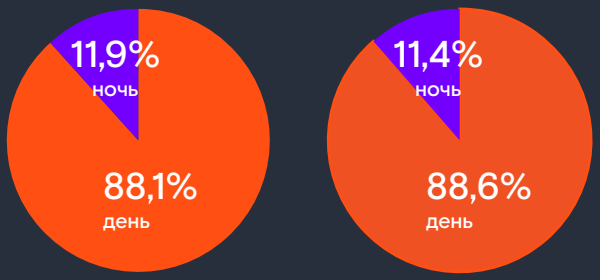
Более 16% атак на объекты КИИ, имели своей целью АСУ ТП или закрытые сегменты. Это связано с их низким уровнем кибергигиены и часто встречающимся смешением корпоративных и технологических сетей. В среднем в процессе мониторинга, аудита защищенности или тестирования на проникновение специалисты «Ростелеком-Солар» выявляют не менее 2 точек смешения открытых и технологических/закрытых сегментов в **95%** компаний организаций.

Общая статистика по инцидентам

Распределение инцидентов по внешним и внутренним



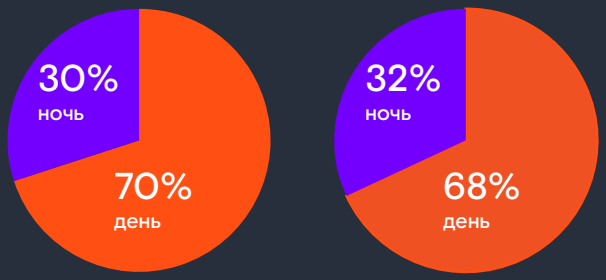
Распределение общего числа инцидентов по времени суток



2018 год

2019 год

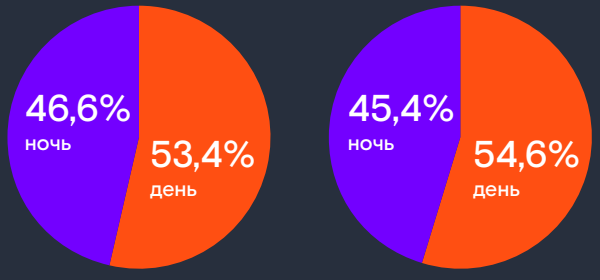
Распределение критических инцидентов по времени суток



2018 год

2019 год

Распределение критических внешних инцидентов по времени суток



2018 год

2019 год

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 критическим, 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 критически важной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам;
- Прямые финансовые потери на сумму более 1 млн рублей.

Внешние инциденты

Направления атак

1-е полугодие 2018

2-е полугодие 2018

1-е полугодие 2019

2-е полугодие 2019

Ключевые тенденции

Стабильный рост показывают атаки, связанные с вирусным ПО **(+11%)**, и атаки на веб-приложения **(+13%)**.

В первом случае этому способствует развитие фишинга как основного способа доставки вредоносного ПО (ВПО). Аналитики Solar JSOC отмечают, что и само ВПО становится более сложным: каждое 5 ВПО, доставляемое на машину пользователя с фишинговыми рассылками, имеет встроенный инструментарий обхода песочницы.

Поводом к увеличению числа атак на веб-приложения служит развитие цифровых порталов и внешних ресурсов в компаниях. Помимо традиционных отраслей – банки и ритейл – все больше веб-ресурсов появляется в энергетике и госсекторе. При этом каждый третий интернет-сайт имеет критическую уязвимость, позволяющую получить привилегированный доступ к серверу (web-shell).

В среднем по стране продолжается падение количества атак, связанных с подбором пароля. С одной стороны, даже небольшие организации повысили сложность парольных политик под влиянием информации о массовых утечках данных. С другой стороны, в крупном бизнесе продолжают развиваться и внедряться альтернативные, беспарольные способы аутентификации пользователей.

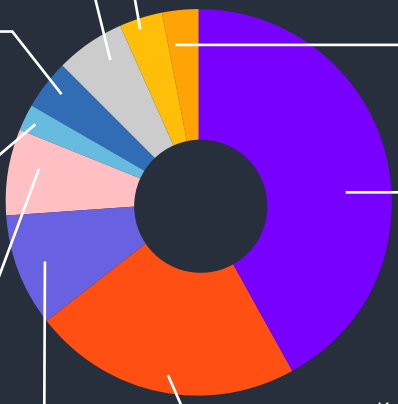
DDoS-атаки при процентном падении доли демонстрируют существенный технологический рост. В 2019 году киберпреступники на **40%** чаще использовали IoT-ботнеты (ботнеты из зараженных устройств интернета вещей) при проведении DDoS-атак, что затрудняло их блокирование и противодействие. Также увеличивается число DDoS-атак, направленных на прикладной уровень, а не на исчерпание полосы.

В 2019 году были выявлены две новые критические уязвимости Windows – BlueKeep и DejaBlue, обе из которых использовали встроенный в систему протокол удаленного доступа RDP. Однако попытки их эксплуатации in the wild встречались нам крайне редко. При этом продолжаются атаки с использованием все более устаревающей уязвимости Eternal Blue. Разница с 2018 годом состоит лишь в том, что теперь злоумышленники стремятся заразить машину жертвы не шифровальщиком, а майнинговым ПО.

Внутренние инциденты

Направления атак

1-е полугодие 2018



5,9%
Нелегитимные работы под привилегированными учетными записями

4,2%
Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критически важных бизнес-систем

2,4%
Использование хакерских и потенциально вредоносных утилит

7,2%
Использование инструментов для удаленного доступа (remote admin tools) или туннелирования трафика

9,3%
Нарушение политик доступа в интернет

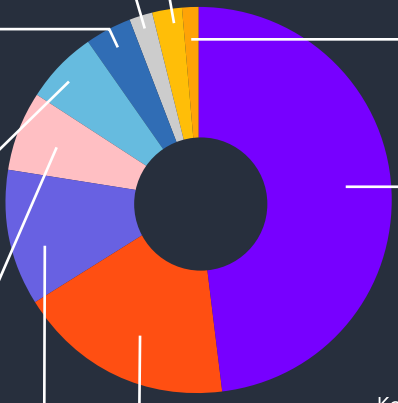
3,4%
Несанкционированные активности в рамках удаленного доступа (VPN), в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер

Прочее 2,9%

42,1%
Утечки конфиденциальных данных

22,6%
Компрометация внутренних учетных записей

2-е полугодие 2018



2,1%
Нелегитимные работы под привилегированными учетными записями

3,8%
Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критически важных бизнес-систем

6,2%
Использование хакерских и потенциально вредоносных утилит

6,5%
Использование инструментов для удаленного доступа (remote admin tools) или туннелирования трафика

11,4%
Нарушение политик доступа в интернет

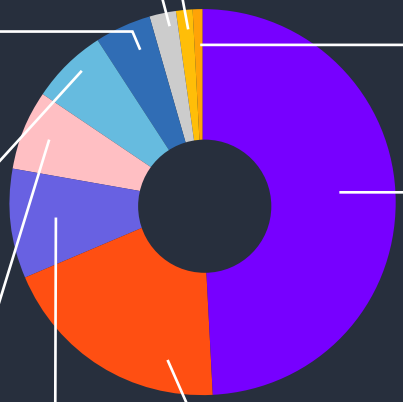
2,5%
Несанкционированные активности в рамках удаленного доступа (VPN), в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер

Прочее 1,2%

48,1%
Утечки конфиденциальных данных

18,2%
Компрометация внутренних учетных записей

1-е полугодие 2019



2,4%
Нелегитимные работы под привилегированными учетными записями

4,5%
Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критически важных бизнес-систем

6,4%
Использование хакерских и потенциально вредоносных утилит

6,8%
Использование инструментов для удаленного доступа (remote admin tools) или туннелирования трафика

9,2%
Нарушение политик доступа в интернет

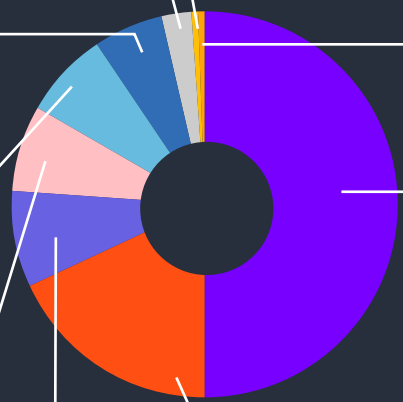
1,3%
Несанкционированные активности в рамках удаленного доступа (VPN), в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер

Прочее 0,7%

49,4%
Утечки конфиденциальных данных

19,3%
Компрометация внутренних учетных записей

2-е полугодие 2019



2,6%
Нелегитимные работы под привилегированными учетными записями

5,6%
Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критически важных бизнес-систем

7,3%
Использование хакерских и потенциально вредоносных утилит

7,2%
Использование инструментов для удаленного доступа (remote admin tools) или туннелирования трафика

8,2%
Нарушение политик доступа в интернет

0,6%
Несанкционированные активности в рамках удаленного доступа (VPN), в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер

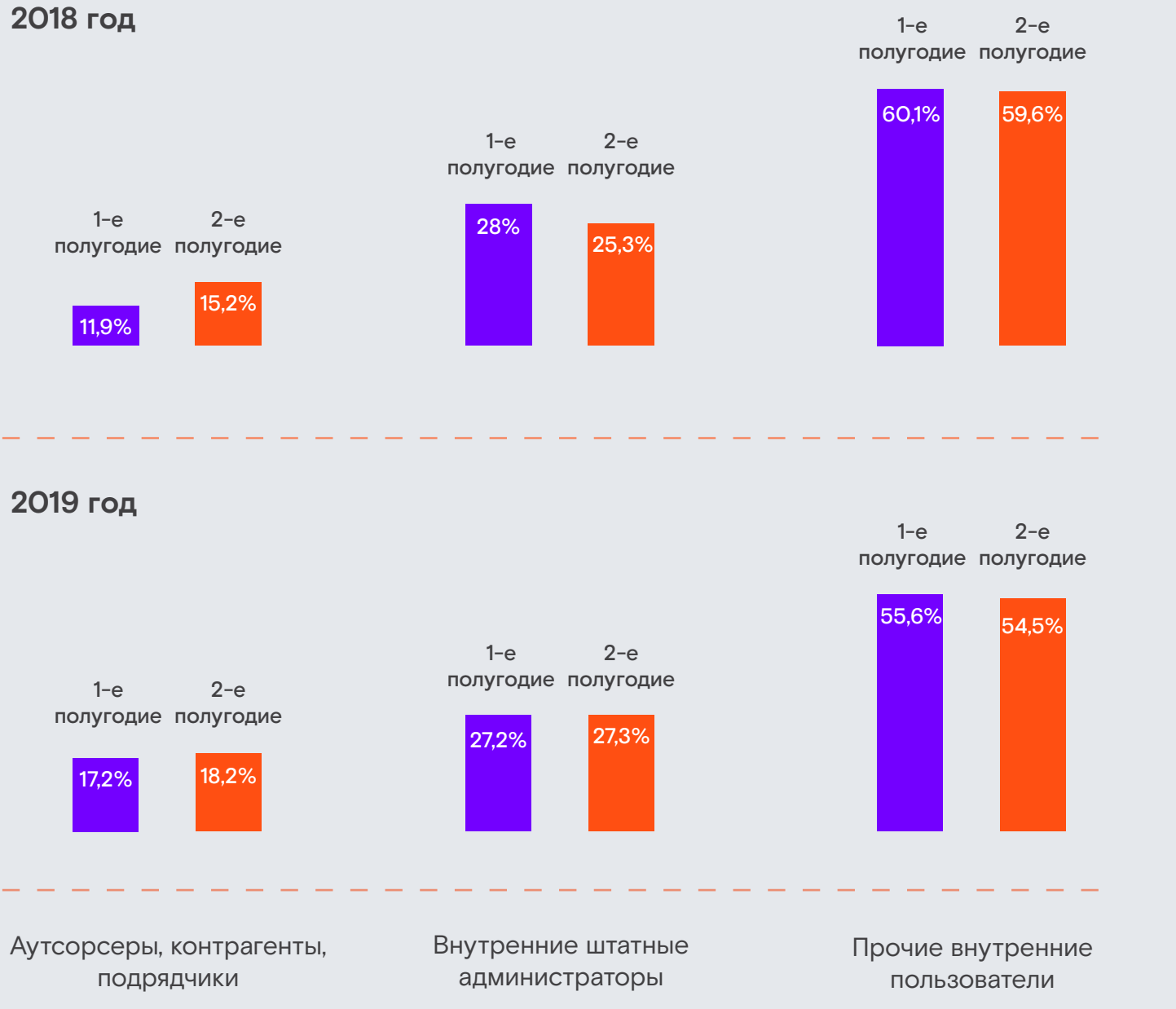
Прочее 0,4%

50,2%
Утечки конфиденциальных данных

17,9%
Компрометация внутренних учетных записей

Не всегда подобные инциденты становятся результатом злонамеренных действий сотрудников. Чаще всего это результат их халатности и нарушения политик информационной безопасности. В среднем каждый восьмой пользователь, который не проходит регулярное обучением основам ИБ, поддается на социальную инженерию: открывает зараженный файл или отправляет свои данные злоумышленникам.

Инициаторы внутренних инцидентов



Многие компании переходят на сервисную модель обслуживания, но при этом не все заказчики понимают, что установленные у них политики информационной безопасности также должны распространяться и на подрядчиков. На этом фоне растет доля инцидентов, происходящих по вине различных подрядчиков и аутсорсеров.

Ключевые тенденции

Существенно снижается количество инцидентов, связанных с нарушением доступа в Интернет. Это косвенно свидетельствует о развитии технологий: многие заказчики провели процедуру миграции со старых межсетевых экранов и прокси-серверов на более совершенные системы.

Продолжается рост числа утечек конфиденциальной информации. Они составляют уже более половины внутренних инцидентов, и в ближайшие годы этот показатель, скорее всего, будет расти.

Обзор инструментов и методов киберпреступников

Цели атак. Ключевые тренды.

На **40%** выросло количество атак, направленных на получение контроля над инфраструктурой. Это позволяет злоумышленникам детально исследовать внутренние процессы, происходящие в организации, получив доступ к информационным и технологическим системам. Сложно определить, как в дальнейшем хакеры используют эти точки входа в инфраструктуры. Это может быть как промышленный шпионаж в интересах конкурентов, так и дальнейшая продажа доступов на черном рынке или даже шантаж организации. Кроме того, в последние годы атаки все чаще направлены на промышленные и энергетические объекты, а также органы госвласти, контроль над инфраструктурой которых критичен для страны в целом.

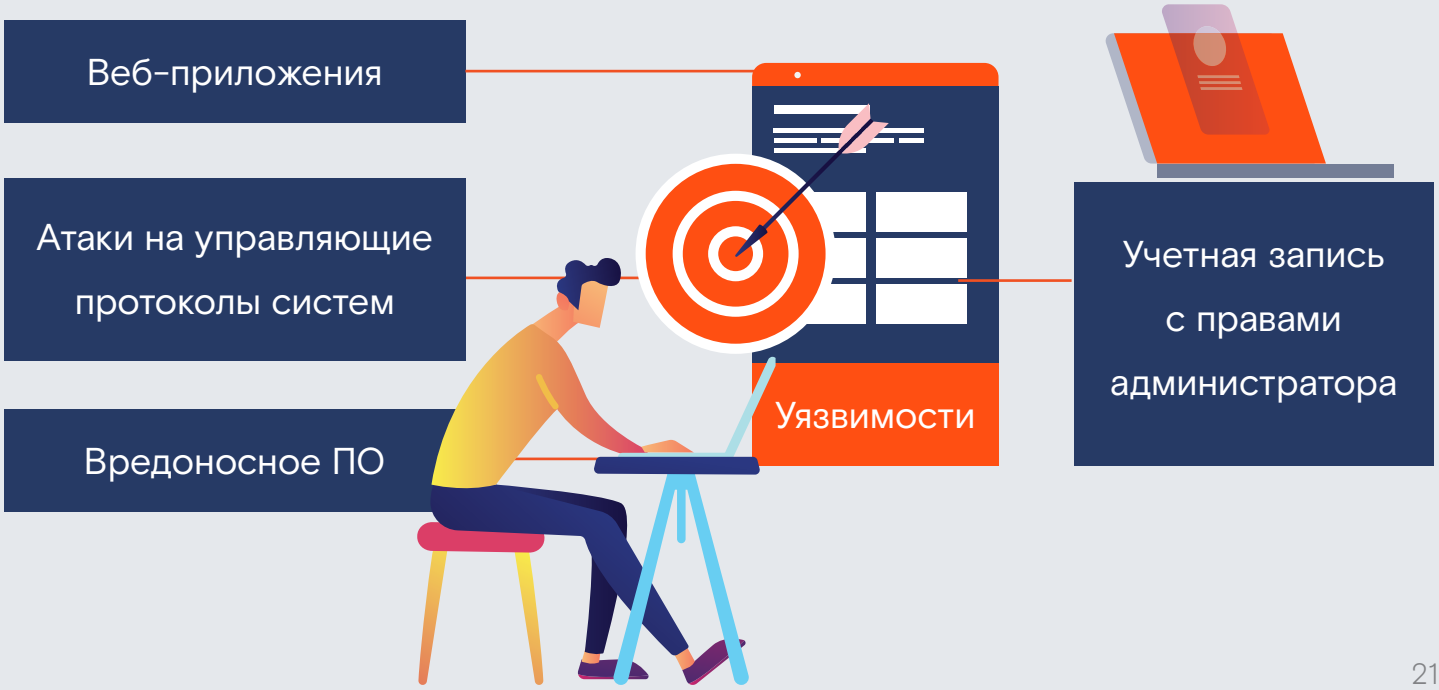
На **15%** относительно 2018 года снизилось количество атак, направленных на кражу денежных средств. Не в последнюю очередь это свидетельствует о существенном развитии уровня информационной безопасности в кредитно-финансовой сфере. Быстрая и прямая монетизация атаки становится все более сложной задачей для киберпреступников, и они переключаются на более доступные цели.

Зафиксировано более десятка фишинговых рассылок с результативностью «пробива» более **100%**: информацию о бесплатных билетах, скидках и акциях к праздникам или «черной пятнице» сотрудники организаций пересылали коллегам и друзьям, вследствие чего охват атаки превзошел ожидания злоумышленников.

Как киберпреступники получают контроль над инфраструктурой

Начиная с 2017 года, мы выделяем в качестве самостоятельного объекта исследования атаки, формирующие Kill Chain – последовательность действий злоумышленника, осуществляющего проникновение в информационную систему. 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.

Чаще всего встречается следующая модель атаки Kill Chain: после первого проникновения в сеть компании злоумышленник сканирует ее, пытаясь найти уязвимый сервер. Если эксплуатация уязвимости прошла успешно, злоумышленник может в короткие сроки получить доступ и к привилегированным учетным записям сети (технологическим учетным записям, записям ИТ-администраторов), из-под которых в свою очередь добраться до остальных объектов инфраструктуры.



Инструменты киберпреступников для проникновения в инфраструктуру компаний

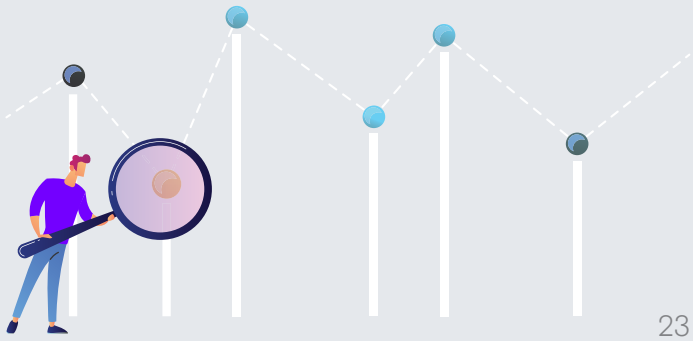
	2018		2019	
	1-е полугодие	2-е полугодие	1-е полугодие	2-е полугодие
Вредоносное ПО, доставляемое на машину пользователя через зараженные флеш-носители либо вследствие компрометации хоста за пределами корпоративной сети	3%	3%	2%	2%
Вредоносное ПО, доставляемое на машину пользователя через вредоносные вложения или фишинговые ссылки в электронных письмах	71%	70%	68%	71%
Атака на веб-приложение	20%	19%	25%	24%
Атака на управляющие протоколы систем	6%	8%	5%	4%

Ключевые тренды развития вредоносного программного обеспечения

В этом разделе мы собрали свои наблюдения и интересные факты о вредоносном программном обеспечении, с которым JSOC CERT сталкивался в 2019 году:

Второй год подряд абсолютным лидером по количеству фишинговых рассылок является банковский троян RTM. Сам троян периодически модифицировался с целью предотвращения обнаружения и повышения надежности работы. Несколько раз он менял «оболочку» (например, на самораспаковывающийся архив, различные вариации оригинальной оболочки) и получил возможность общения с C&C-серверами, расположенными в сети TOR. Кроме того, операторы, распространяющие RTM, стали больше уделять внимание элементам социальной инженерии. Так, если раньше письма приходили от частных лиц, то сейчас все чаще от существующих компаний и организаций.

В течение первого квартала 2019 года фиксировались массовые рассылки шифровальщика Troldesh на крупные российские компании. В письмах содержались архивы с js- или vbs-скриптами, которые после запуска в одну или две итерации заражали систему основным модулем Troldesh. Особенность рассылок была в том, что они производились с различных роутеров, доступных из сети Интернет по административным портам и имеющих слабые аутентификационные данные. В этом случае невозможно было отследить реальный источник рассылок, так как чаще всего обычные роутеры не ведут запись активности в лог-файлы.



Также активными участниками в рассылках 2019 года были хорошо известные сообществу вредоносы класса stealer - Pony, Loki и Hawkeye. Все они в течение года были накрыты одним и тем же пакером, называемым VBInJect (или VBCrypt). Суть технологии защиты вредоносного кода, которую предоставляет VBInJect, состоит в долгой итерационной работе с постоянными проверками виртуального окружения и работы в «песочнице». В течение года мы много раз видели, как благодаря этому функционалу вредоносы обходят даже самые современные технологии защиты – песочницы.

В фишинговых рассылках офисных документов чаще всего использовались технологии запуска кода в виде макросов. На втором месте по популярности – технология DDE (Microsoft Dynamic Data Exchange), которую Microsoft официально отключал в новых версиях своих офисных продуктов, но это никак не повлияло на ее использование злоумышленниками.

Среди уязвимостей Microsoft Office уже на протяжении двух лет подряд наиболее популярными остаются уязвимости в математическом объекте формул CVE-2017-11882 и CVE-2018-0802. Причина в том, что их эксплоиты прочно осели в открытом доступе, и для их использования не требуются глубокие технические знания.

Также потенциальным новым трендом в доставке вредоносного кода можно считать использование стеганографии. Метод, который обычно используют внутренние нарушители для скрытой передачи конфиденциальной информации, стал все чаще применяться внешними злоумышленниками для доставки модулей управления ВПО.

Хотя принято считать, что вредонос Emotet не распространяется в информационном пространстве России, в течение года мы фиксировали ряд атак с использованием данного ВПО. Злоумышленники взламывали общедоступные ресурсы

с уязвимой версией WordPress и располагали на них вредоносные файлы, ссылки на которые рассылались по электронной почте. При этом все вредоносные ссылки имели некоторое сходство: они оканчивались тремя случайными строками, разделенными через дефис (например: http://*.sk/isotope/fa9n-ilztc-raiydwlsg/ и http://*.com/wp-content/uploads/hwqu-5dj22r-chrsl/)

В 2019 году большинство инцидентов, с которыми столкнулись специалисты JSOC CERT, были связаны либо с эксплуатацией уязвимостей публичных веб-ресурсов, либо с относительно простыми аутентификационными данными администраторских панелей веб-ресурсов и терминальных серверов RDP. Так, по нашим данным, если использовать слабый пароль администратора и открыть к этим сервисам доступ из интернета, пройдет менее 5 часов до того, как они будут заражены вредоносным ПО. Чаще всего это будет майнер, шифровальщик или относительно простой вирус, например, Monero Miner, Miner Xmig, Watchbog, Dbg Bot или Scarab.

Выявление атак злоумышленников с помощью сбора и анализа информации об угрозах (Threat Intelligence)

Источники Threat Intelligence (TI), используемые в Solar JSOC:

Opensource – открытые базы индикаторов вредоносного ПО, серверов управления и фишинговых ссылок. Как правило, в разрезе детектирования с помощью SIEM-платформ актуальны 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 актуальны только сетевые индикаторы.

APT/IoC reporting – платные подписки на подробные описания 0-day вредоносных тел, включающие 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.).

Использование различных источников Threat Intelligence в детектировании инцидентов

Источник Threat Intelligence	% от общего количества инцидентов, детектированных с помощью TI
Opensource	7,4 %
Reputation feeds	19,6 %
APT/IoC reporting	20,1 %
Information Exchange	18,7 %
Internal Solar JSOC database	22,4 %
User Experience	11,8 %

Несмотря на существенное расширение списка коммерческих поставщиков информации об угрозах в Solar JSOC (в частности, соглашение с антивирусным вендором ESET, имеющим очень широкое покрытие в мире), соотношение между количеством угроз, выявленных при помощи коммерческих источников, и тех, которые были выявлены при помощи бесплатных источников (информационное взаимодействие, перекрестное опыление информацией заказчиков и т.д.), сохранился на прежнем уровне. Это доказывает важность обмена информацией и детального анализа угроз внутри ИБ-сообщества.

rt.ru
rt-solar.ru

info@rt-solar.ru
+7 (499) 755-07-70