Solar JSOC Security Report 2018 и тренды 2019

rt-solar.ru

Ростелеком
Солар

Solar JSOC Security Report

Исследование кибератак на российские организации в 2018 и начале 2019 гг.

Отчет Solar JSOC Security Report основан на данных, полученных в коммерческом центре мониторинга и реагирования Solar JSOC за 2018 год. 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.

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 в режиме 24*7.
- Контроль защищенности и управление уязвимостями.
- Анализ безопасности состояния конфигураций систем ИБ.
- Техническое расследование инцидентов.
- Практическая оценка защищенности (тестирование на проникновение).
- Управление средствами защиты и предоставление средств защиты по арендной схеме.
- Сервисы повышения осведомленности корпоративных пользователей.
- Специальные сервисы ГосСОПКА (государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации).

Под защитой Solar JSOC находится более 100 крупнейших российских компаний и организаций. Среди них – федеральные ведомства, региональные правительства, крупнейшие финансовые институты, энергетические компании и т.д. В рамках информационного обмена о киберугрозах Solar JSOC активно взаимодействует с ФинЦЕРТ ЦБ РФ и ГосСОПКА ФСБ РФ. Подразделения Solar JSOC расположены в Москве, Нижнем Новгороде, Самаре и Хабаровске. Штат сотрудников центра мониторинга насчитывает более 170 опытных инженеров и аналитиков.

Методология

Solar JSOC Security report базируется на анализе инцидентов, выявленных командой Solar JSOC как в рамках оказания 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.

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

Сводная статистика за 2018 год

Средний суточный поток событий ИБ, обрабатываемых SIEM-системами и используемых Solar JSOC для оказания сервиса, составил **72,2 миллиарда событий**. Это в пять раз больше, чем в 2017 году (14,4 млрд событий). Такой прирост связан с увеличением числа заказчиков Solar JSOC и, как следствие, более широким охватом событий информационной безопасности в российских организациях.

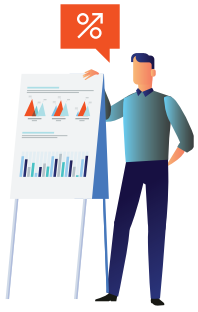
765 000

Всего за 2018 год в Solar JSOC было зафиксировано свыше **765 тысяч событий с подозрением на инцидент**, что на 89% больше, чем в 2017 году

97,4%

Соблюдение клиентских SLA за 2018 год составило **97,4%**

В 2018 году **доля критических инцидентов составила 19%**. Это самый высокий показатель с 2015 года. Увеличение доли критических инцидентов говорит о том, что инструментарий киберпреступников продолжает стремительно совершенствоваться.



Среднее **время с момента выявления инцидента до принятия его в работу** специалистом JSOC **составило 19 минут**. Среднее время с момента возникновения инцидента до предоставления аналитической справки и рекомендаций по его устранению составило 24 минуты по критическим инцидентам и 75 – по остальным.

Ключевые тенденции 2018 года

• Во второй половине 2018 года на 20% выросло количество атак, направленных на получение контроля над инфраструктурой, на 37% – количество атак, направленных на кражу денежных средств.

• Несмотря на ущерб от массовых атак в 2017-2018 гг., многие российские компании не приняли никаких мер защиты. На сегодняшний день 266 294 российских серверов все еще подвержены уязвимости EternalBlue, 953 единицы сетевого оборудования работают с незакрытым протоколом Cisco SMI. Эти организации остаются потенциальными жертвами таких, казалось бы, устаревших атак, как WannaCry или атаки на оборудование Cisco.

• В 2018 году произошел ряд крупных вирусных заражений технологических сетей, изолированных от интернета (сегмент АСУ ТП). Поскольку в таких сетях антивирус обновляется вручную, случайное заражение одного узла приводит к быстрому распространению вируса, а процесс ликвидации угрозы, напротив, длится в несколько раз дольше, чем в корпоративном сегменте.

• Киберпреступники наращивают как сложность инструментария, так и темпы его создания. Так, группировка Cobalt начала рассылку вредоносного ПО, эксплуатировавшего уязвимость CVE-2018-15982, в течение суток с момента появления информации о ней.

• 70% сложных целенаправленных атак начинается с фишинга. В среднем каждый 7-й пользователь, не прошедший курсы повышения осведомленности, поддается на социальную инженерию. Однако этот показатель может варьироваться в зависимости от функционального подразделения компании. В юридической службе жертвой фишинга становится в среднем каждый четвертый сотрудник, в бухгалтерии, финансово-экономической службе и логистике – каждый пятый, в секретариате и службе техподдержки – каждый шестой.

• По сравнению с 2017 годом количество DDoS-атак выросло почти в два раза – на 95%. Во многом это связано с их дешевизной и эффективностью.

• Почти половину внутренних инцидентов информационной безопасности составляют утечки данных.

• 72,1% исследованных событий были зафиксированы 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. Во многом это возможно благодаря развитию системы информационных обменов и CERT, передающих информацию о новых способах атак, видах вредоносного ПО и уязвимостях широкому перечню контрагентов.

• Оставшиеся инциденты (27,9%) выявляются при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем и несут гораздо больший объем информации и критичность для информационной и экономической безопасности компании-клиента. Это позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критические таргетированные атаки.

Ключевые тенденции начала 2019 года

• Список самого распространенного вредоносного ПО не изменился по сравнению с 2018 годом. В начале 2019 года специалисты JSOC CERT все так же часто сталкивались с рассылками Loki Bot, Adwind RAT, FormBook, Scarab, Trickbot и AZORult.

• В течение первого квартала 2019 года фиксировались массовые фишинговые рассылки шифровальщика Troldesh по крупным российским компаниям. Это была первая в России фишинговая атака, осуществлявшаяся с роутеров, доступных из интернета по административным портам и имевших ненадежные логин и пароль.

• Киберпреступники продолжают атаки на банки с использованием трояна RTM. Анализ образцов начала 2019 года показывает, что троян был многократно модифицирован с целью предотвращения его обнаружения и повышения надежности работы. С начала года троян несколько раз менял оболочку, а также получил возможность общения с C&C-серверами в сети TOR.

• В марте были зафиксированы попытки заражения ряда банков вредоносным программным обеспечением семейства Emotet. Злоумышленники взламывали общедоступные ресурсы с уязвимой версией WordPress, загружали на них вредоносные файлы и затем рассылали ссылки на эти ресурсы по электронной почте.

• Злоумышленники перенимают друг у друга лучшие практики. В 2019 году для обхода средств защиты все чаще используется техника бесконечного цикла, когда загрузчик вредоносного ПО скачивает его на сервер или рабочую станцию не сразу, а через произвольное время. Таким образом, если загрузчик изначально попадает в песочницу, его вредоносная функциональность остается нераскрытой, а аналитики не могут получить основное тело ВПО для последующего анализа.

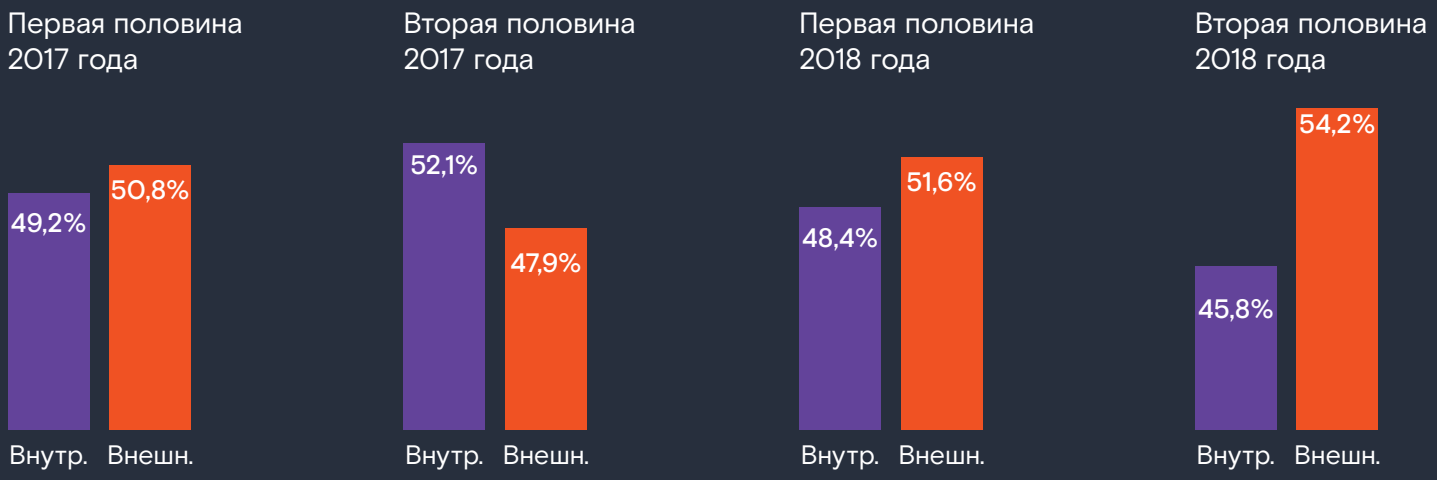
Ранее эта техника использовалась преимущественно группировкой Silence, но сейчас постепенно становится все более массовым инструментом.

• В 2019 году стало известно о том, что архив с исходными кодами вредоносного программного обеспечения группировки Carbanak/Fin7 выложен на общедоступном сервисе VirusTotal. Архив легко может быть использован как инструкция для тех, кто занимается или хотел бы заниматься разработкой вредоносного кода, поэтому можно быть уверенными, что хорошо документированный исходный код вредоносного ПО уже изучают не только специалисты по информационной безопасности, но и их противники.

• Группировка Fin7 продолжает свою деятельность. Злоумышленники обновили арсенал и сейчас используют модули вредоносного программного обеспечения, написанные на языке JavaScript, распространяя его с помощью тщательно подготовленных фишинговых писем. Группировка пока обходит стороной российские компании, но, учитывая историю, репутацию и уровень подготовки Fin7, организациям необходимо проявлять бдительность.

Общая статистика по инцидентам

Распределение инцидентов по внешним и внутренним



Распределение общего числа инцидентов по времени суток

Распределение критических инцидентов по времени суток

Распределение критических внешних инцидентов по времени суток

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:

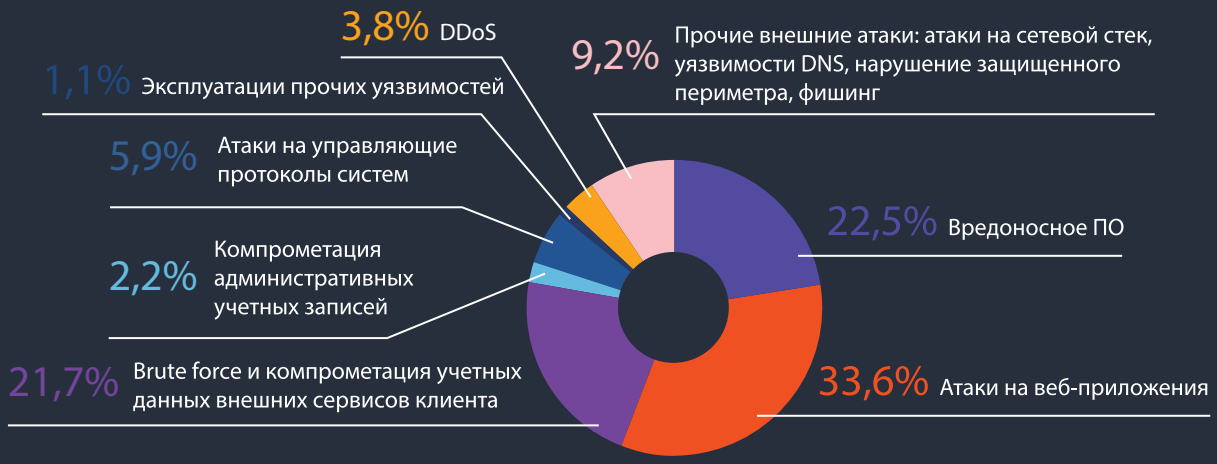
- Длительное прерывание (более получаса) или остановка функционирования систем и сервисов клиента, относящихся к категориям Business и Mission Critical;
- Повреждение, потеря или компрометация критически важной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам;
- Прямые финансовые потери на сумму более 1 млн рублей.

Внешние инциденты

В этой части отчета рассматриваются инциденты, причиной которых становились действия лиц, не являющихся внутренними пользователями организаций. 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.

Направления атак

1-е полугодие 2018



2-е полугодие 2018

Ключевые тенденции

• По сравнению с 2017 годом количество DDoS-атак выросло почти в два раза – на 95%. Во многом это связано с их дешевизной и эффективностью. Тенденция к увеличению числа и интенсивности DDoS прослеживается во всех отраслях, чувствительных к данному типу атаки, – игровом сегменте, e-commerce, банках, органах государственной власти.

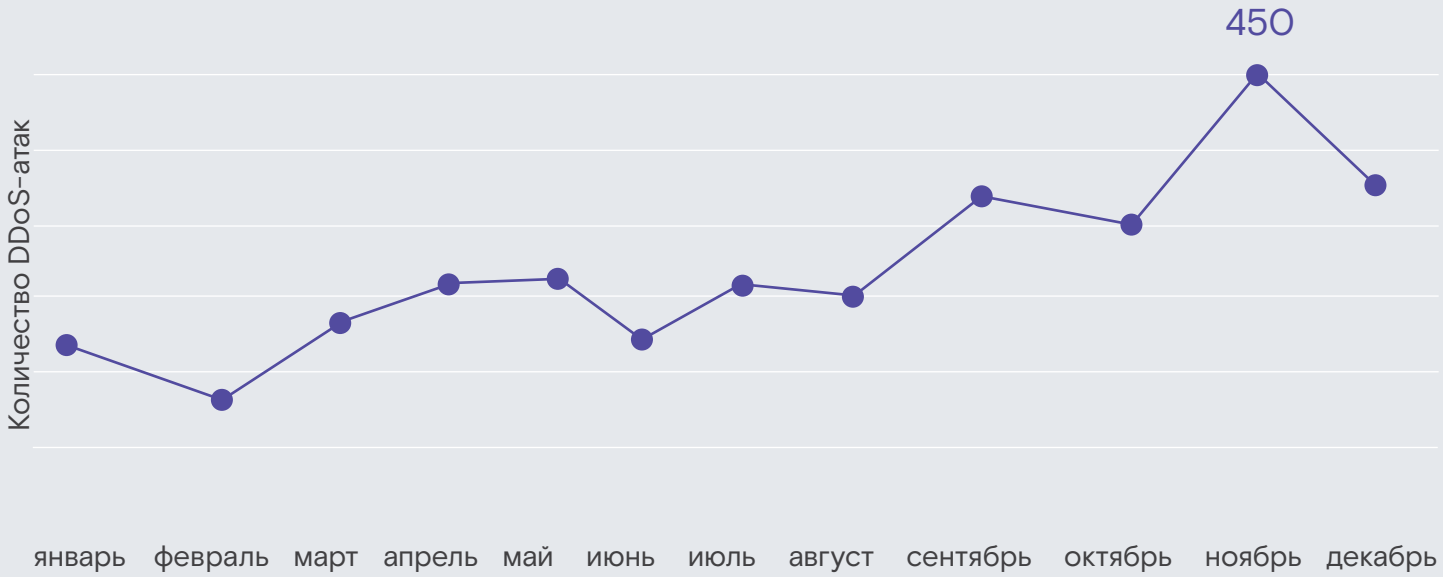
• Серьезно выросло число инцидентов, связанных с заражениями вредоносным ПО. Это свидетельствует не столько об увеличении типов вредоносных программ, сколько о ширине охвата и массовости вредоносных рассылок. Все чаще письма, ориентированные на банковский сектор, выявляют в энергетических компаниях, органах государственной власти и промышленных предприятиях. Нерелевантный таргетинг не делает рассылки менее опасными, поскольку часть сотрудников все равно открывает вредоносные письма, а злоумышленник, получив доступ к инфраструктуре, может развивать атаку, догружая дополнительные функциональные модули, уже ориентированные на организации данной конкретной отрасли.

• По-прежнему часто фиксируются новые шифровальщики и криптомайнеры, использующие уязвимость CVE-2017-0144 (EternalBlue), – несмотря на то, что с момента появления массовых вирусных эпидемий прошло уже два года. По всей видимости, ряд инфраструктур российских компаний все же уязвим к этой атаке.

DDoS-атаки

По сравнению с 2017 годом количество DDoS-атак выросло почти в два раза – на 95%. На наш взгляд, во многом это связано с их дешевизной и эффективностью, которая будет способствовать увеличению числа атак и в 2019 году. Пик DDoS-атак в 2018 году пришелся на ноябрь-декабрь. Эти месяцы считаются ключевыми с точки зрения продаж в сегменте электронной коммерции – покупательская активность растет в связи с предпраздничным периодом и стартом крупных распродаж. DDoS позволяет на время заблокировать ресурсы конкурента или может использоваться в качестве орудия шантажа тех компаний, которые в ноябре-декабре получают большую часть выручки.

Распределение количества DDoS-атак по месяцам, 2018 год



Самая продолжительная атака длилась **280 часов** (11 суток и 16 часов).
Обычно злоумышленники прекращают вредоносную активность через **1,5-2 часа**.

В ушедшем году произошел резкий скачок мощности DDoS-атак. Если в 2017 году этот показатель не превышал 54 Гбит/с, то в 2018 самая серьезная атака велась уже с интенсивностью 450 Гбит/с. Это не единичный случай: лишь дважды за год пиковая месячная мощность DDoS-атаки составляла менее 50 Гбит/с – в июне и августе.

Статистика 2018 года подтверждает, что угроза DDoS наиболее актуальна для отраслей, чьи критически важные бизнес-процессы зависят от доступности онлайн-сервисов и приложений – в первую очередь это игровой сегмент и электронная коммерция.

Распределение DDoS-атак по отраслям, 2018 год

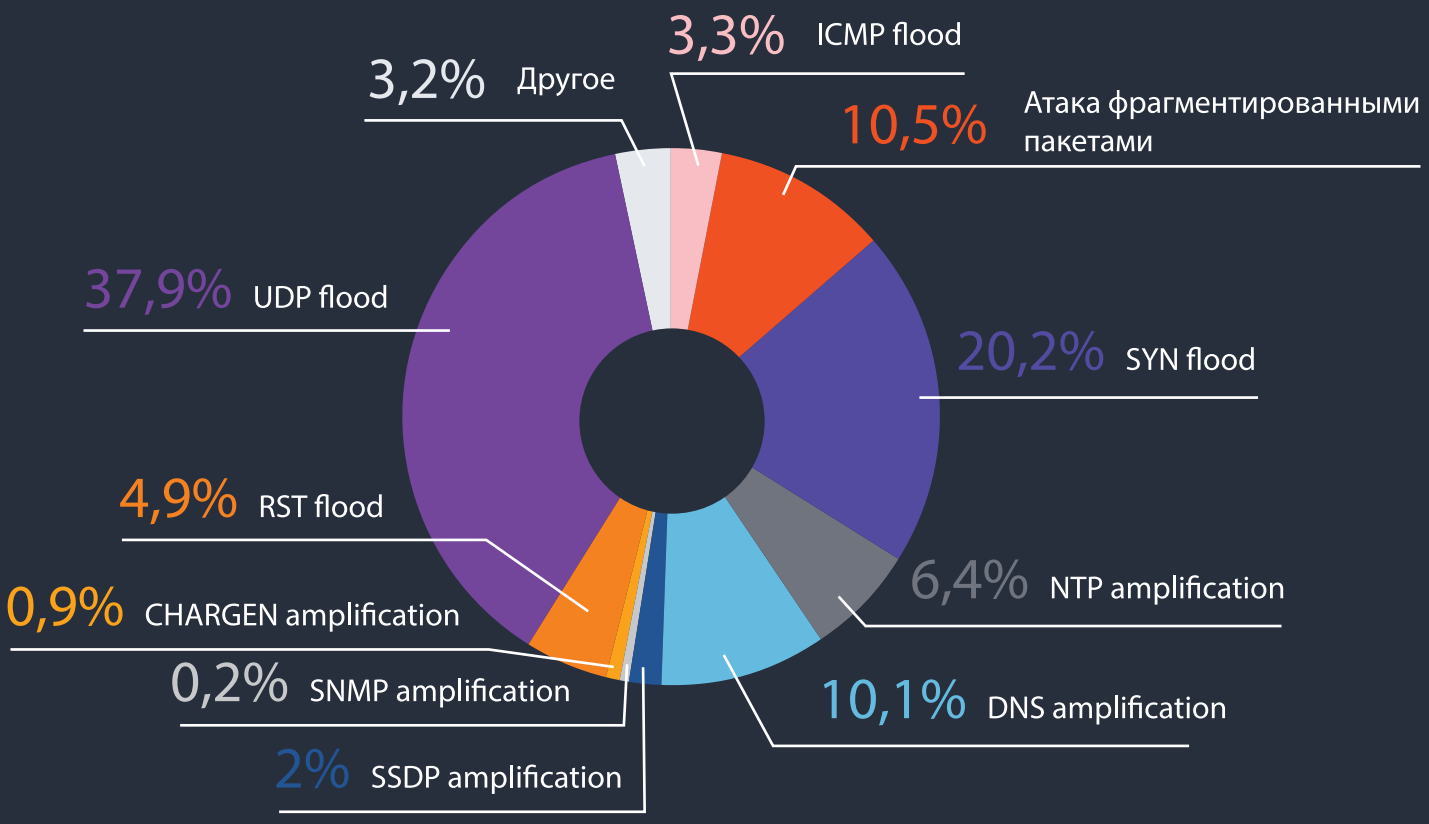
Игровая индустрия лидирует с большим отрывом: в 2018 году доля атак на эти компании составила 64%.

По нашим прогнозам, данная картина не изменится в ближайшие годы, а с развитием киберспорта и

появлением там еще больших денег можно ожидать дальнейшего роста числа атак на эту отрасль. Сфера электронной коммерции стабильно удерживает второе место (16%).

Наиболее популярным методом DDoS является UDP-флуд – почти 38% всех атак осуществляется именно этим способом. При этом отмечается резкий рост доли атак с амплификацией и атак типа SYN-флуд. Их объединяет то, что первые не требуют наличия ботнета (и затрат на его организацию или покупку), а вторые могут осуществляться как с использованием ботнета, так и без него.

Распределение DDoS-атак по типам, 2018 год



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: нарушение или халатность в соблюдении политик информационной безопасности, утечки информации, компрометация или передача учетных данных к внутренним системам, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование систем.

1-е полугодие 2018

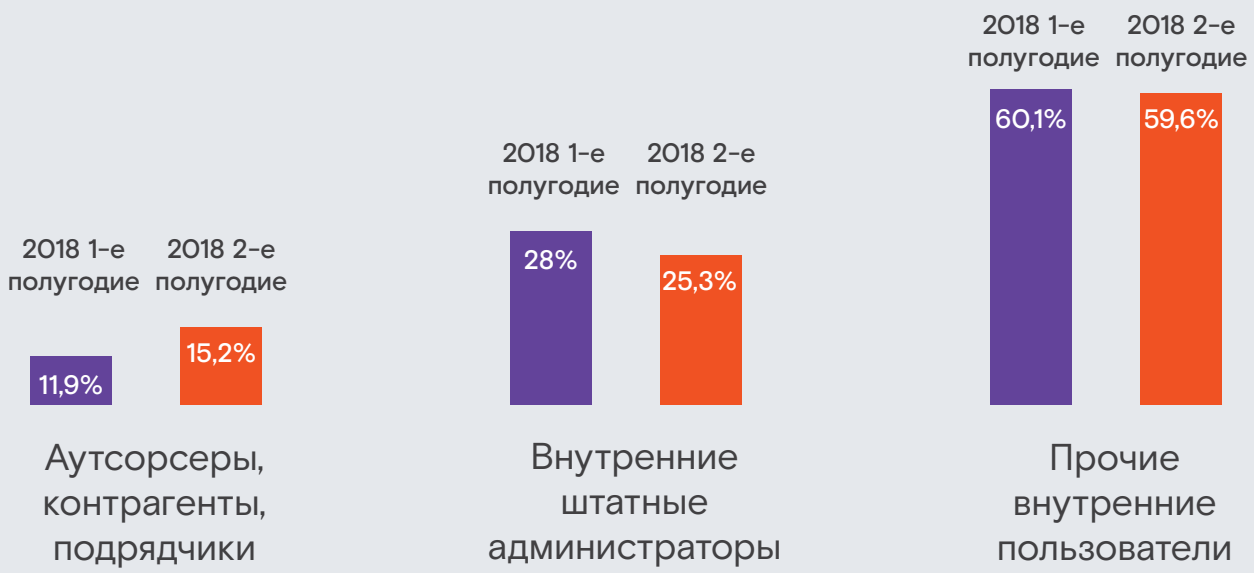
2-е полугодие 2018

Ключевые тенденции:

• Существенно снизилось количество инцидентов, связанных с компрометацией внутренних учетных записей. Во многом это объясняется повышением общего уровня осведомленности пользователей об угрозах информационной безопасности, которому способствует внимание к этой проблеме со стороны государства и средств массовой информации.

• Утечки конфиденциальной информации составляют почти половину всех внутренних инцидентов информационной безопасности. Количество утечек обычно растет к концу года, и собранная нами за годы наблюдений статистика позволяет достаточно уверенно связывать число инцидентов с кадровыми циклами набора и увольнения сотрудников.

Инициаторы внутренних инцидентов



Растет доля инцидентов, происходящих по вине аутсорсеров и подрядчиков. Преимущества сервисной модели способствуют развитию рынка аутсорсинга, однако не все компании понимают, что установленные у них политики информационной безопасности должны распространяться и на подрядчиков.

Обзор инструментов и методов киберпреступников

Цели атак. Ключевые тренды.

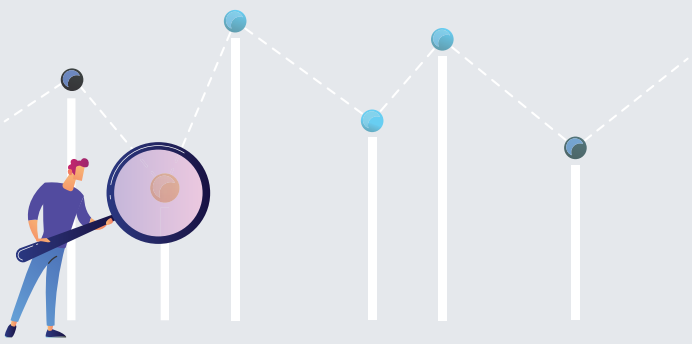
В этом году в отчет впервые включено распределение атак по целям злоумышленника. Определение итоговой цели зависит от действий киберпреступника в инфраструктуре, функциональных возможностей вредоносного ПО, внедренного в компанию, и т.д. В отчете учтены как внешние, так и внутренние атаки.

Ключевые тенденции

• На 20% по сравнению с первой половиной года выросло количество атак, направленных на получение контроля над инфраструктурой. Злоумышленники стремятся незаметно закрепиться в инфраструктуре, чтобы детально исследовать ее и получить как можно более глубокий доступ к информационным и технологическим системам. При этом на старте злоумышленники зачастую используют совершенно непрофильные инструменты: так, мы фиксировали случаи рассылки банковских троянов на органы государственной власти и энергетические организации. В дальнейшем управляемые сегменты бот-сети перепродаются другим группировкам и развитие атаки идет уже с помощью специализированного инструментария.

• На 37% относительно первой половины года выросло количество атак, направленных на кражу денежных средств. Однако развитие информационного обмена в рамках сообщества по-прежнему позволяет кредитно-финансовым организациям своевременно получать информацию о способе реализации атаки и препятствовать действиям злоумышленников. Тем не менее фиксируемый рост говорит о том, что атаки будут продолжаться, а инструментарий – постепенно усложняться.

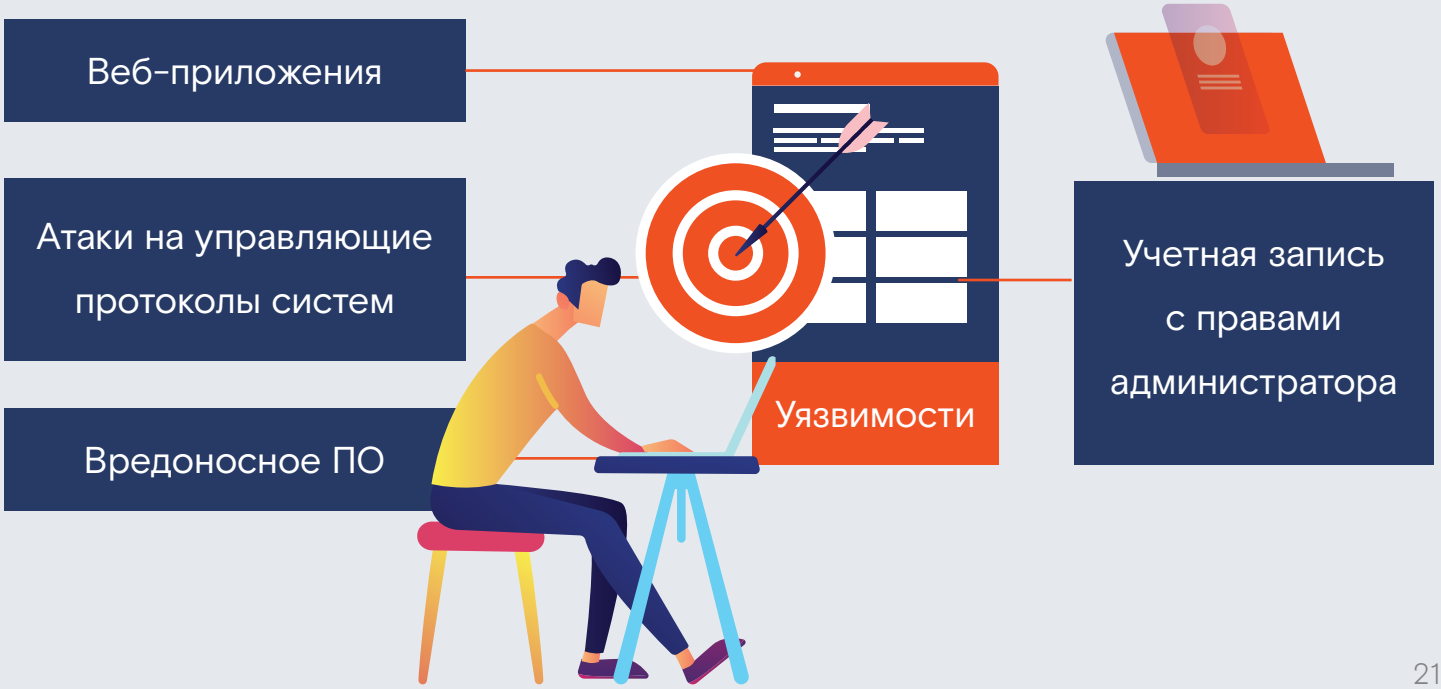
• Во второй половине года аналитики Solar JSOC регулярно сталкивались с вредоносным ПО, оптимизированным для обхода средств защиты, в том числе антивирусов и песочниц. Также в 2018 году отмечалась тщательная проработка и усиление социального вектора атак. Фишинговые письма становятся все больше похожи на привычные рассылки о промоакциях, предстоящих мероприятиях и т.д.



Инструментарий и векторы реализации атак

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.

В 2018 году аналитики Solar JSOC в 97% случаев сталкивались со следующей общей моделью атаки. После первого проникновения в сеть компании (статистика описана чуть ниже) злоумышленник сканирует ее, пытаясь найти уязвимый сервер. Если эксплуатация уязвимости прошла успешно, злоумышленник может в короткие сроки получить доступ к привилегированным учетным записям сети (технологическим учетным записям, записям ИТ-администраторов), из-под которых в свою очередь добраться до многих объектов инфраструктуры.



Инструменты киберпреступников для проникновения в инфраструктуру компаний

	2017		2018	
	1-е полугодие	2-е полугодие	1-е полугодие	2-е полугодие
1. Вредоносное ПО, доставляемое на машину пользователя через зараженные флеш-носители либо вследствие компрометации хоста за пределами корпоративной сети	13%	8%	3%	3%
2. Вредоносное ПО, доставляемое на машину пользователя через вредоносные вложения или фишинговые ссылки в электронных письмах	54%	65%	71%	70%
3. Атака на веб-приложение	11%	10%	20%	19%
4. Атака на управляющие протоколы систем	22%	17%	6%	8%

В 8% случаев атака злоумышленников начиналась с использования уязвимостей или ошибок конфигурации в управляющих протоколах систем. Несмотря на то, что ситуация с контролем и инвентаризацией периметра организаций существенно улучшилась, до сих пор можно отметить ряд системных проблем в обеспечении безопасности инфраструктур.

- В каждой десятой организации одно из устройств защиты или телекоммуникационного оборудования имеет опубликованный в интернет порт управления с дефолтными или легко подбираемыми учетными записями и паролями.

- В каждой организации в среднем раз в месяц появляется 2-3 неучтенных или неинвентаризированных сервиса, доступных из интернета. Обычно это происходит из-за того, что ИТ-специалисты при выполнении работ не консультируются со службой ИБ, в том числе в отношении использования наложенных средств сетевой безопасности для защиты публикуемых сервисов.

- Несмотря на активную борьбу с массовыми атаками в 2017-2018 годах, уровень контроля защищенности периметра организаций в среднем по стране оставляет желать лучшего. Так, на сегодняшний день число серверов, подверженных уязвимости CVE-2017-0144 (EternalBlue), составляет более 1 665 050 в мире и более 266 294 – в России. Количество единиц сетевого оборудования с незакрытым протоколом Cisco SMI составляет более 88 805 в мире и 953 - в России. Все это повышает вероятность стать жертвой таких, казалось бы, устаревших атак, как WannaCry или атаки на оборудование Cisco.

В 19% случаев на первом этапе злоумышленники атаковали веб-приложение компании. При общем тренде перевода бизнеса в онлайн стоит отметить и более специализированные проблемы. Зачастую для повышения эффективности работы сотрудников за пределы периметра выводят вторичные для деятельности компании системы – службы для восстановления пароля удаленного доступа, шлюзы проверки контрагентов, системы видео-конференц-связи. Недостаточная защита таких систем открывает новые возможности для злоумышленников, позволяя им реализовать достаточно специфические векторы атак.

Социальная инженерия. Фишинг.

Значимость этого вектора атак заметно выросла за два года (с 54% до 70%), в связи с чем мы решили обратить на него более пристальное внимание.

Ключевые тенденции

• В среднем каждый 7-й пользователь, который не проходит регулярное повышение осведомленности, поддается на социальную инженерию: открывает зараженный файл или отправляет свои данные злоумышленникам. Наиболее подверженные атаке подразделения:

- Юридическая служба – каждый 4-й сотрудник;
- Бухгалтерия и финансово-экономическая служба – каждый 5-й сотрудник;
- Логистика – каждый 5-й сотрудник;
- Секретариат и helpdesk – каждый 6-й сотрудник.

• Обучение сотрудников основам киберграмотности и регулярная тренировка их навыков существенно влияют на уровень защищенности организаций. Эффективность социальной инженерии снижается практически в 2 раза: на атаки поддается уже лишь каждый 12-ый пользователь. Разница в результатах до и после начала обучения и регулярных тренировок сильнее всего заметна у сотрудников финансового и юридического департамента.

• Эффективность фишинговых атак, в особенности тщательно подготовленных, серьезно повышается

накануне праздников. Правильное использование информационных поводов может дать мошенникам фантастическую конверсию рассылки и резко упростить взлом инфраструктуры.

Перед Новым годом мы наблюдали несколько достаточно курьезных ситуаций, когда сотрудники промышленных компаний получили очень качественные фишинговые письма со списком новогодних акций в популярных интернет-магазинах и с промокодами на скидки. Сотрудники не только сами пытались перейти по ссылке, но и пересылали письмо коллегам из смежных организаций. Поскольку ресурс, на который вела ссылка в фишинговом письме, был заблокирован, сотрудники начали массово оставлять ИТ-службе заявки на предоставление доступа к нему. Этот пример показывает, что минимально продуманная социальная инженерия может дать эффект, превосходящий изначальные ожидания киберпреступников.

Ключевые тренды развития вредоносного программного обеспечения

В этом разделе мы собрали наблюдения и интересные факты о вредоносном программном обеспечении, с которым JSOC CERT сталкивался в 2018 году.

- Во втором полугодии 2018 года сменился лидер среди ВПО для фишинговых атак на российский финансовый сектор: троян Dimnie, чаще всего встречавшийся нам в первой половине года, уступил место банковскому трояну RTM.

- Мы считали, что утечка исходного кода проекта Pegasus, произошедшая

6 июля 2018 года, станет сильным катализатором для вирусописателей, и ожидали вскоре увидеть ее последствия. К нашему удивлению, за прошедшие полгода мы так и не встретили модули этого проекта «in the wild».

• В то же время проект Buhtrap, утекший в сеть еще в 2016 году, до сих пор активно используется злоумышленниками. За последние полгода он несколько раз сменил загрузчик (от привычного js до необычного DotNet), легитимное приложение, за счет которого оказывался в памяти (Морской бой, Судоку, Punto Switcher и др.), и не всегда использовал привычный для себя NSIS Installer.

• В сентябре мы зафиксировали использование злоумышленниками нескольких вредоносных библиотек, написанных для легитимных программ удаленного доступа (RMS, Teamviewer). Библиотеки оказывались в памяти приложений благодаря классической технике DLL HiJacking. Предназначение библиотеки – перехват API-вызовов для сокрытия различных событий, фиксируемых программами (например, удаленного подключения).

• Отдельно отметим вредоносные образцы и внутренние изолированные инфраструктуры. Во второй половине 2018 года мы несколько раз столкнулись с крупным заражением инфраструктуры, изолированной от интернета. Как правило, средства антивирусной защиты в таких сетях необходимо обновлять вручную, так как доступа к внешним серверам обновления просто нет. Семейства вирусов, которые, казалось бы, побеждены – WannaCry, WannaMine, Palevo Tracker и т.п. – живут в таких инфраструктурах гораздо дольше.

• Нельзя не упомянуть и Cobalt. Информация о возможности использования уязвимости CVE-2018-15982 для проведения целенаправленных атак появилась 5 декабря 2018 года. Уже 6 декабря группировка Cobalt рассылала вредоносное ПО, эксплуатирующее эту уязвимость.

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.).

Ниже приведена статистика по использованию различных источников Threat Intelligence в детектировании инцидентов.

Источник Threat Intelligence	% от общего количества инцидентов, детектированных с помощью TI
1. Opensource	8,9%
2. Reputation feeds	20,8%
3. APT/IoC reporting	18,8%
4. Information Exchange	20,9%
5. Internal Solar JSOC database	20,8%
6. User Experience	9,8%

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

Для заметок

Для заметок

Для заметок

rt.ru
rt-solar.ru

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