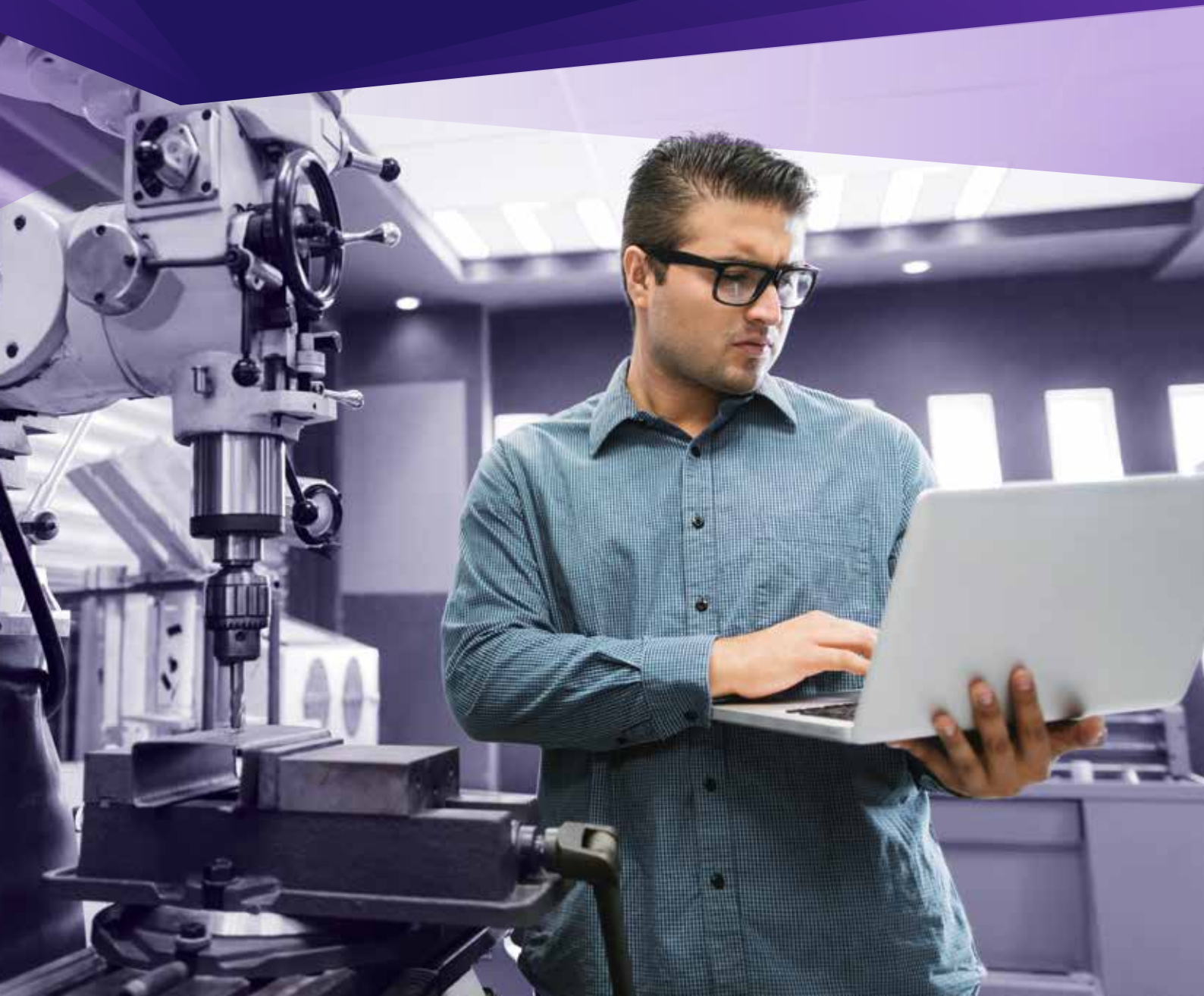
ОТЧЕТ

Отчет компании Fortinet о тенденциях в сфере безопасности операционных технологий за 2019 год

Дополнительные материалы о спектре угроз для систем ICS и SCADA



Содержание

Аннотация

Поскольку организации в ответ на вызовы быстро развивающегося рынка делают свои операции более динамичными, многие эксплуатационные системы (OT) впервые подключаются к внешнему миру. Эта тенденция обещает организациям существенные преимущества, но при этом OT-системы оказываются под прицелом современных непрерывных угроз. Физическое разделение, которое защищало OT-системы от хакеров и вредоносных программ, во многих организациях больше не используется, в результате чего злоумышленники все чаще выбирают своей целью OT-системы.

В отчете Fortinet за 2019 год о тенденциях в сфере безопасности OT-систем анализируются сводные данные, полученные в FortiGuard Labs с целью сформировать представление о состоянии безопасности для систем диспетчерского контроля и сбора данных (SCADA) и других промышленных систем управления (ICS). Анализ показывает, что OT-системы все чаще становятся объектами атак, использующих информационные технологии (IT), зачастую устаревших, которые больше не действуют на IT-системы, а также атак, направленных именно на OT-системы. Логично, что эти атаки, как правило, направлены на самые слабые компоненты OT-сетей и используют разнородность, которая связана с отсутствием стандартизации протоколов. При этом злоумышленники не проводят различий между отраслями или регионами, поскольку каждая отрасль и каждый регион подвергались значительным атакам.

Поскольку OT-системы становятся все более связанными с внешним миром, тенденция роста количества атак скорее всего продолжится. В условиях новых рисков организации должны придерживаться более жестких рекомендованных методов выполнения операций безопасности и управления жизненным циклом, чтобы обезопасить саму основу своего бизнеса от крупных угроз. В результате OT- и IT-отделам приходится налаживать совместную работу, чтобы противостоять угрозам с учетом всех аспектов.

Инфографика: основные выводы

Количество эксплойтов **и их распространенность увеличились** в 2018 году почти для всех поставщиков ICS/SCADA.

Злоумышленники регулярно **повторно запускали угрозы** на целевых OT-системах.

85%

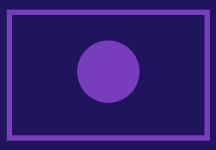
уникальных обнаруженных угроз было нацелено на машины, использующие:

OPC Classic

BACnet

Modbus

Атаки на BACnet, которые достигли пика в **январе–апреле 2018 г.,** были связаны с ботнетом Mirai.



Уязвимость **Moxa 313** имела максимальную концентрацию в Японии.

Введение

Традиционно изолированные путем физического разделения OT-системы теперь все чаще подключаются к внешнему миру — иногда в значительно большей степени, чем представляют себе операционные директора и специалисты по промышленному регулированию. Согласно одному из последних исследований, почти две трети OT-устройств подключены к ИТ-сетям — 32% напрямую к Интернету и еще 32% через шлюз на предприятии.[1] Иногда этот шлюз безопасен не более, чем персональный компьютер, который имеет отдельные подключения к OT-системе и Интернету.

Интеграция IT и OT-систем — хорошее бизнес-решение, предоставляющее для многих организаций следующие преимущества:

- **более эффективный и рациональный мониторинг процессов** с возможностью вносить важные изменения на лету;
- **возможность использовать данные, полученные от устройств Интернета вещей (IoT)**, для информированного принятия решений, добавления детализированного уровня информации о потребителях, продуктах и процессах;
- **доступ к рыночной информации в режиме реального времени,** для оптимального расчета сроков поставок продукции и более удобного взаимодействия с цепочкой поставок;
- **существенная экономия** на энергопотреблении, сокращении потерь сырья, а также за счет эффективности сотрудников.

Интеграция OT приводит к росту проблем безопасности.

Несмотря на эти очевидные преимущества, отказ от физического разделения подвергает OT-системы тем же рискам безопасности, которым подвержены IT-системы, и способствует более легкому распространению специализированных эксплойтов для OT-систем. Эта проблема усугубляется еще и тем, что системы ICS и SCADA всегда работали по более длинному циклу модернизации и замены, чем IT-системы, а это означает, что множество устаревших в технологическом отношении систем сейчас впервые подвергается современным непрерывным угрозам. Еще одна проблема связана с недостаточной видимостью: 82% респондентов в одном из исследований подтверждают тот факт, что они не способны идентифицировать все устройства, подключенные к их OT- и IT-сетям.[2]

Во многих организациях эти проблемы привели к недопустимо высокому количеству инцидентов безопасности. В последнем исследовании, проводившемся среди лидеров OT-отрасли, 77% респондентов заявили, что они столкнулись с вторжением вредоносных программ в последние годы, причем половина опрошенных называет цифры в диапазоне от 3 до 10.[3] Характер вторжений настораживает: респонденты сообщают о событиях, которые повлияли на производительность (43%), выручку (36%), репутацию бренда (30%), потерю данных (28%) и даже физическую безопасность (23%).

Безопасность OT-систем связана с существенным риском.

Действительно, у злоумышленников много побудительных мотивов для атак на системы ICS и SCADA. Преступники могут потребовать выкуп после приостановления работы на предприятии, отключить систему доступа по идентификационному жетону или перехватить управление компонентами критически важной инфраструктуры. Конкуренты — часто действующие от лица государственных предприятий хакеры — могут проникать в системы с целью промышленного шпионажа. А злоумышленники с политическими целями могут выбрать мишенью организации, которые, как они считают, стоят на их пути к цели, способствуя дестабилизации и хаосу.

Сотрудники, отвечающие за безопасность OT-систем, при подключении к сети сталкиваются с существенными проблемами:

- **увеличение количества векторов атак** вследствие отказа от физического разделения;
- **устаревшие системы** с функциями обеспечения безопасности, которые разрабатывались для неподключенной к сети инфраструктуры;
- **недостаточная видимость** в системах, часто с устройствами IoT, которые подключались по мере необходимости;
- **устаревшие устройства телеметрии,** работа которых может привести к катастрофическим последствиям;
- **плохая сегментация сети**: 45% пользователей ICS/SCADA не использовали функции управления привилегированными пользователями.[4]

В отчете компании Fortinet о тенденциях в сфере безопасности операционных технологий за 2019 год анализируются данные, собранные с миллиона устройств Fortinet с целью сформировать представление о состоянии информационной безопасности систем ICS и SCADA. Полученные результаты могут помочь сотрудникам, ответственным за безопасность этих систем, понять риски и расставить приоритеты для их устранения.

Тенденции спектра угроз для OT-систем

Тенденция: угрозы, связанные с информационными технологиями, оказывают все большее влияние на OT-системы

Как только OT-системы подключаются к IT-сетям, они часто становятся самым слабым звеном в цепочке безопасности. Данные FortiGuard Labs показывают, что злоумышленники используют IT-угрозы для атаки на OT-системы. В одном из распространенных сценариев злоумышленник одновременно атакует OT- и IT-системы при помощи одной и той же вредоносной программы. Поскольку OT-системы часто используют устаревшие технологии, а операции безопасности часто менее проработаны, у атакующих больше шансов на успех.

Злоумышленники используют старые вредоносные программы для OT

В следующем сценарии злоумышленники повторно используют пакеты устаревшей вредоносной программы, которая ранее использовалась для ИТ-атак, но теперь перехватывается любым решением ИТ-безопасности на основе сигнатур. На рис. 1 показано, сколько процентов известных угроз было обнаружено Fortinet в каждом месяце года, а также количество устройств с OT-протоколами, которые были атакованы любой из угроз каждый месяц. Обратите внимание, что шаблон очень цикличен: чем больше угроз используется, тем меньше устройств поражается, и наоборот.

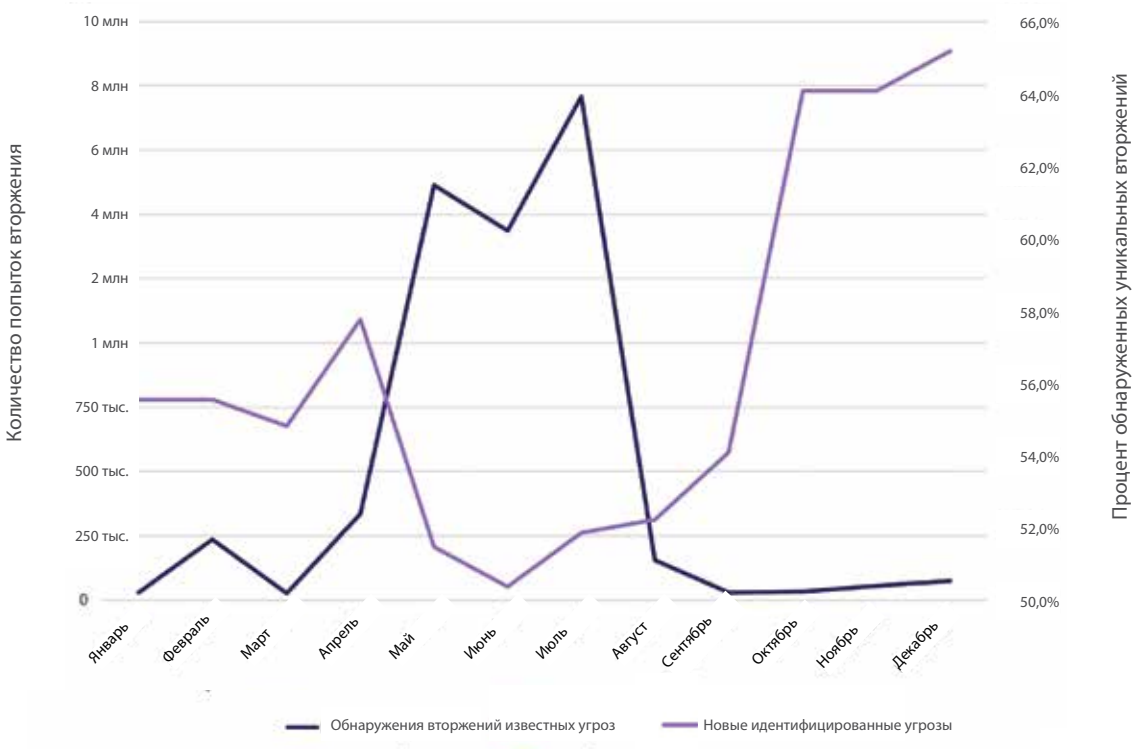


Рис. 1: общее количество обнаруженных вторжений по сравнению с количеством уникальных обнаруженных вторжений, 2018.

Этот цикл предполагает поиск злоумышленниками новых уязвимостей во вновь подключенных OT-системах. На этапе разведки они тестируют широкий спектр разнообразных устаревших вредоносных программ на относительно небольшом количестве компьютеров. Как только атакующие идентифицируют успешные угрозы, они переходят в фазу атаки, используя подмножество атак, оказавшихся успешными на большем количестве машин. Их цель — получить максимальную выгоду от существующих вредоносных программ, прежде чем вкладывать средства в создание новых, более целенаправленных атак.

На сезонную вариативность новых версий старых угроз может также влиять и другой фактор. В частности, складывается впечатление, что атаки на системы отопления, вентиляции и кондиционирования, а также на электрические сети с большей вероятностью происходят на пике их использования — в северном полушарии наиболее часто в летние месяцы. Еще одним фактором является возраст OT-системы, причем злоумышленники демонстрируют тенденцию выбирать устаревшие технологии чаще, чем новые, более безопасные.

Злоумышленники выбирают целью устройства, использующие различные OT-протоколы.

В то время как IT-системы уже много лет используют стандартный протокол TCP/IP, OT-системы работают на широком спектре протоколов, многие из которых являются специфическими для конкретных функций, отраслей и регионов. Консорциум OPC Foundation был создан в 90-х годах в попытке подтолкнуть промышленность к стандартизации протоколов. Новая унифицированная архитектура OPC (OPC UA) способна объединить протоколы для всех промышленных систем, но из-за распространенности устаревших протоколов и продолжительного цикла замены для систем OT консолидации придется ждать еще долгие годы.

Киберпреступники активно пытаются нажиться на отсутствии стандартизации, выбирая тонкие места в каждом из протоколов. Эти структурные проблемы усугубляются отсутствием стандартных средств защиты и плохой гигиеной безопасности во многих системах OT — наследие тех лет, когда они использовали физическое разделение.

По объему доминируют три протокола.

Нам представляется, что наиболее атакуемые протоколы (если смотреть по объему трафика) характеризуются двумя факторами: как часто они используются и насколько уязвимы. В совокупности на протоколы OPC Classic, BACnet и Modbus приходится 85% сигнатур контроля приложений, обнаруживаемых в элементах управления OT-систем.

Безусловно, если смотреть по трафику, чаще всего в качестве объекта атаки злоумышленники выбирают протокол **OPC Classic**, который был создан до протокола OPC UA, но в настоящее время используется гораздо чаще. Этот протокол использует более новые технологии, чем другие, большинство из которых разрабатывалось в конце 90-х и нулевых годов, но распространенность основанных на нем систем и то, что разработка их элементов не была стандартизованной, особенно привлекает киберпреступников.

Автоматизация в строительстве — одна из наиболее стандартизованных областей OT, ориентированная на использование единого протокола. Протокол **BACnet** используется практически в любой крупной организации независимо от отрасли — по большей части потому, что он используется такими крупными поставщиками систем отопления, вентиляции и кондиционирования, как Johnson Controls и Carrier. В результате BACnet является вторым из наиболее часто используемых протоколов. Еще один фактор: BACnet разрабатывался с использованием очень старой технологии, которая была разработана в 1987 году. Три из четырех самых распространенных по количеству устройств угроз в 2018 году работали на BACnet (рис. 2). Объем обнаруженных вторжений с использованием протоколов на машинах BACnet достиг пика в первой половине года (рис. 3), что соотносится с атаками ботнета Mirai на системы, использующие BACnet. Mirai вызывал распределенные атаки отказа в обслуживании (DDoS) по всему миру.[5] Тот факт, что Mirai появляется в статистике с октября по декабрь 2018 года, а BACnet в этот период отсутствует, свидетельствует о том, что Mirai, который представляет собой арендуемый ботнет, больше не используется для запуска атак против BACnet, зато используется для атак на другие OT-системы.

Рис. 2: четыре наиболее часто обнаруживаемых вторжения с использованием протоколов (по количеству устройств), 2018.

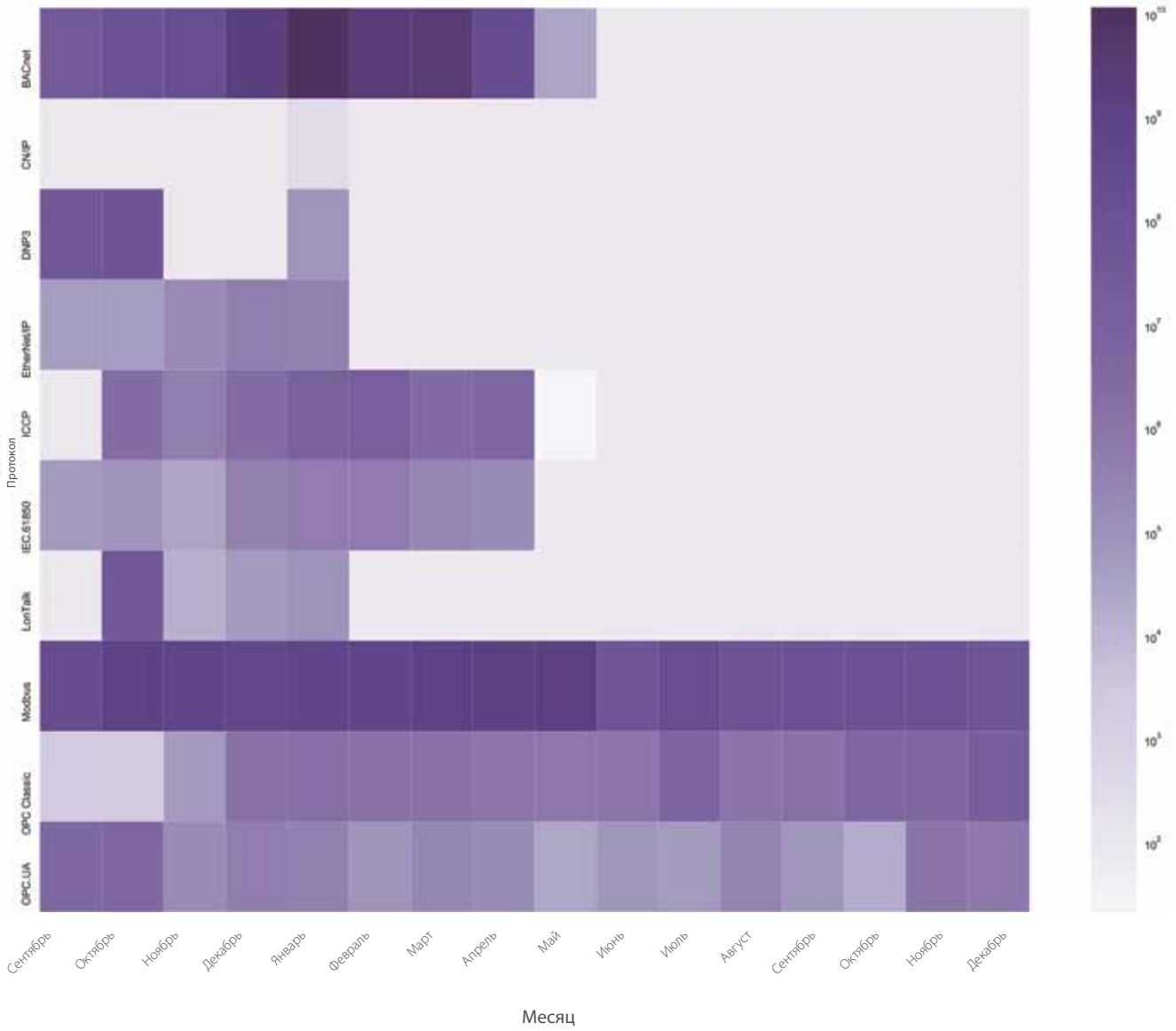


Рис. 3: объем обнаруженных вторжений с использованием протоколов, Сентябрь 2017 — Декабрь 2018.

Третий наиболее часто используемый протокол, **Modbus**, представляет собой протокол передачи данных, который обеспечивает эффективное взаимодействие между различными компонентами OT-систем. Эта технология была разработана в 1979 году и предназначалась для закрытых (то есть, использующих физическое разделение) систем. Modbus имеет десятки различных модификаций, созданных разными поставщиками, поэтому OT-специалистам сложно отслеживать его уязвимости.

Ни один поставщик ICS/SCADA не имеет иммунитета против угроз.

В 2018 году были зафиксированы атаки на каждого из 70 отслеживаемых нами поставщиков OT-систем, и, если не считать небольшого количества специфических атак (например, Schneider и Moxa), эти угрозы регулярно обнаруживались на протяжении всего года (рис. 4). При этом наиболее атакуемыми поставщиками по количеству уникальных угроз оказались самые крупные: Advantech, Schneider, Moxa и Siemens (рис. 5). Как правило, более старые, усложненные предложения поставщиков имели больше уязвимостей, чем новые, более совершенные продукты.

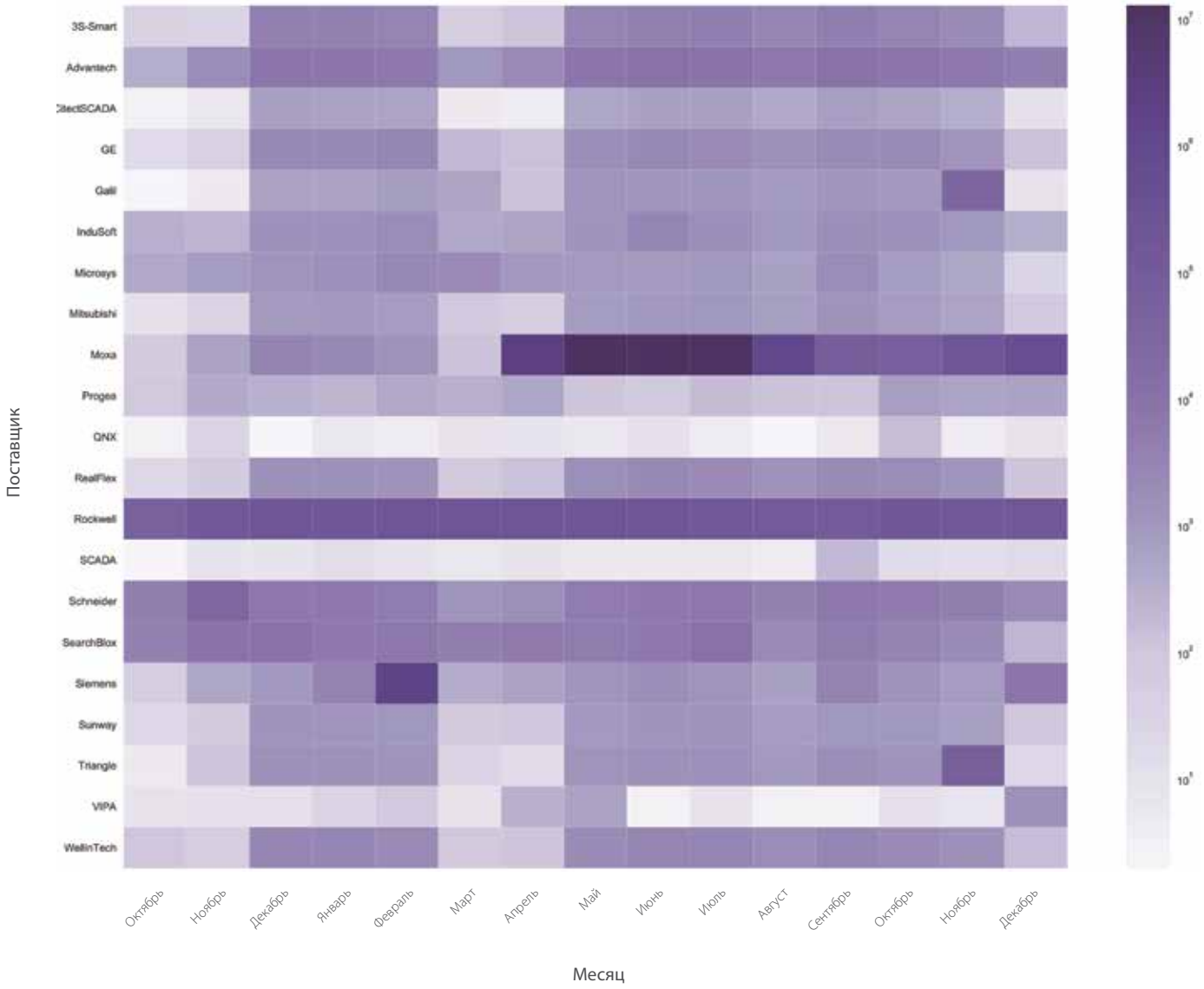


Рис. 4: объем обнаруженных вторжений угроз, нацеленных на поставщиков ICS/SCADA, Октябрь 2017–Декабрь 2018.

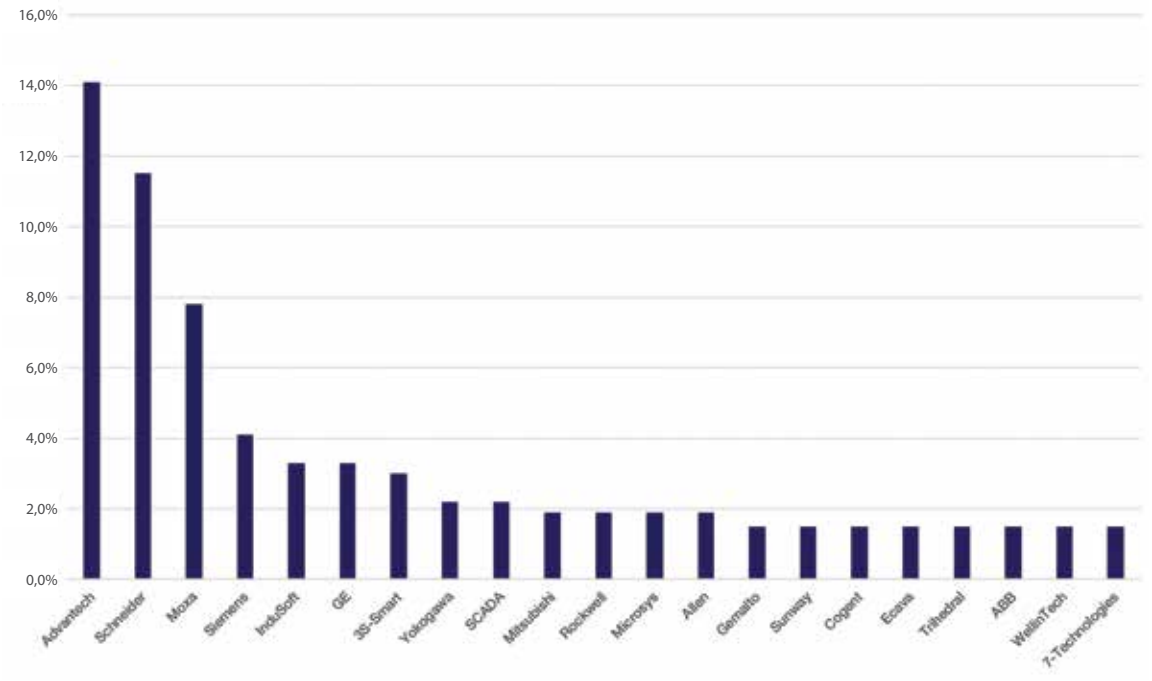


Рис. 5: рейтинг поставщиков ICS/SCADA по количеству обнаруженных вторжений уникальных угроз.

В целом, количество ИТ-угроз растет.

Несмотря на сезонные колебания и широкий спектр целей, данные однозначны: количество атак с применением IT на OT-системы растет. Например, на рисунке 1 показано, что всплеск новых обнаруженных угроз намного выше в конце года, чем в начале. На рисунке 6 показано, что в течение 2018 года увеличился объем и распространенность эксплойтов, нацеленных почти на каждого поставщика ICS. Нет никаких оснований ожидать, что эта тенденция изменится в 2019 году. Объем является показателем общей частоты угроз, который соответствует совокупному количеству наблюдений за угрозой в абсолютном или относительном выражении. Распространенность — это показатель распространения или распространенности по группам, который показывает количество организаций, сообщивших хотя бы об одном наблюдавшемся событии угрозы, в относительном выражении (процентах).

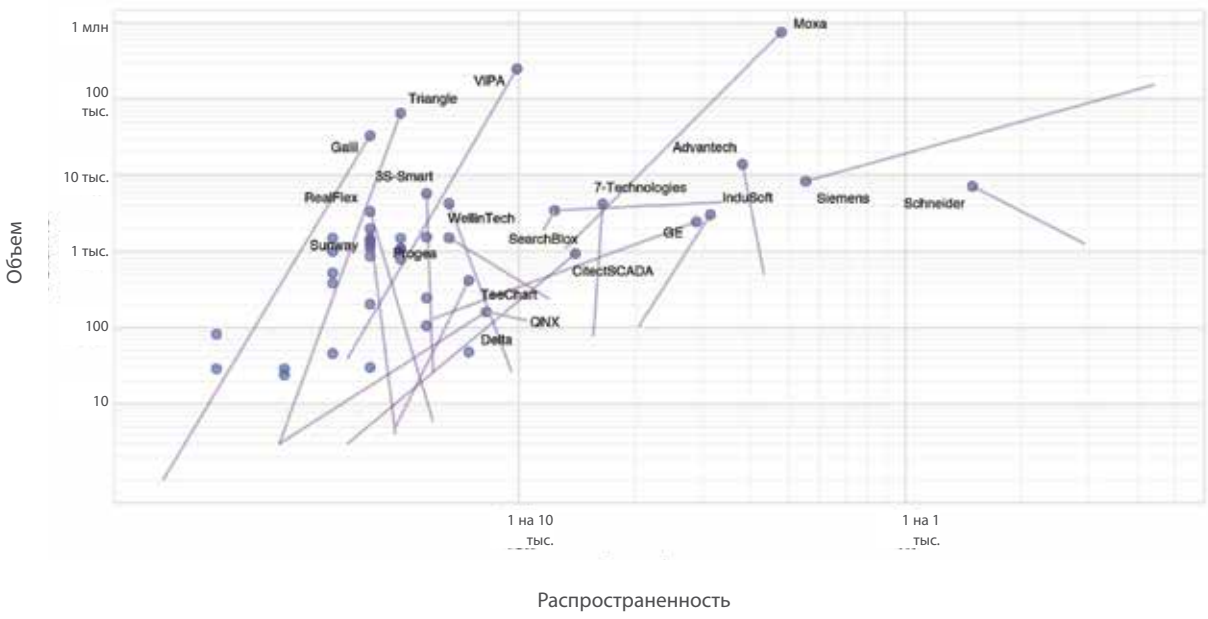


Рис. 6: изменение распространенности и объема эксплойтов, нацеленных на поставщиков системы ICS, I-IV квартал 2018 года.

Тенденция: продолжают появляться атаки, специально разрабатываемые для OT-систем, и теперь их целью являются системы обеспечения безопасности

Вредоносные программы, предназначенные для систем ICS и SCADA, разрабатываются около десяти лет или чуть больше, но примеров насчитывается довольно много. Среди эксплойтов для OT-систем — **Stuxnet, Havex, Industroyer** и новейший **Triton/Trisis.**

Считается, что эксплойты Industroyer и Havex впервые были применены российскими войсками в качестве кибероружия для поражения украинской энергосистемы во время вооруженного конфликта в 2016 году. Потом произошла утечка вредоносной программы, которая стала использоваться против других сетей, построенных на той же инфраструктуре Schneider Electric.[11]

Системы безопасности подвергаются новым опасным атакам.

Triton/Trisis поражает контроллеры приборных систем обеспечения безопасности (SIS) компании Triconex, которые также продаются Schneider Electric и очень распространены в энергетической отрасли. Первая жертва этого эксплойта, нефтегазовая установка в Саудовской Аравии, пострадала от полной остановки своих мощностей в 2017 г.[12] Учитывая тот факт, что вредоносные программы поражают системы безопасности, могут быть и более тяжкие последствия — вывод из строя оборудования и угроза жизни людей. [13] В апреле 2019 года стало известно о второй жертве эксплойта Triton/Trisis — не названной компании на Среднем Востоке.[14] Эксперты выражают опасения по поводу Triton/Trisis, который во многих отношениях является первой настоящей киберфизической атакой на OT-системы.

Программы-вымогатели продолжают атаковать OT-системы

В начале 2018 года исследования FortiGuard Labs продемонстрировали резкое увеличение количества программ-вымогателей и червей-вымогателей в IT-средах[6] Это произошло вслед за массированной и весьма успешной атакой NotPetya в 2017 году, в результате которой пострадали IT- и OT-системы по всему миру. Атаке подверглись следующие OT-системы:

- **Merck:** атака угрозы NotPetya вызвала прекращение работы OT-систем на большей части предприятий этого фармацевтического гиганта, в результате чего было остановлено производство. Это заставило компанию арендовать партию доз гардасила стоимостью 240 млн долларов у центра лечебно-профилактической помощи (CDC). [7] С учетом всех убытков, атака обошлась компании почти в 1 млрд долларов.

- **A.P. Møller – Maersk:** крупнейшая в мире компания по контейнерным перевозкам потеряла 20% объема в результате атаки NotPetya. Цифра могла бы быть гораздо больше, если бы самоотверженные сотрудники не провели масштабную глобальную операцию и не перестроили всю электронную инфраструктуру вручную всего за 10 дней. [8] Ущерб, понесенный компанией в результате атаки, оценивается как минимум в 200 млн долларов.

К концу 2018 года атаки с использованием программ-вымогателей пошли на убыль, и многие злоумышленники предположительно перешли на другие типы атак, например криптоджекинг. [9] Однако киберпреступники имеют тенденцию повторно использовать вредоносные программы для атак на OT-системы, многие из которых не так хорошо защищены, как IT-системы. Это может указывать на то, что в ближайшем будущем программы-вымогатели будут гораздо более опасной угрозой для OT-систем, чем для IT-систем. Поскольку SCADA Masters часто выполняются на оборудовании под управлением Microsoft Windows и Linux, программы-вымогатели могут воздействовать на эти машины, если они не защищены должным образом.

Продолжаются атаки с помощью старых OT-угроз.

Согласно данным от FortiGuard Labs, специализированные вредоносные программы для OT продолжают поражать устройства по всему миру. Например, на рис. 7 показаны измеряемые попытки вторжения с помощью Industroyer в 2018 году, особенно в первой половине года. Сложные вредоносные программы вроде Industroyer, как правило, живут долго даже после обнаружения и рассылки сигнатур.

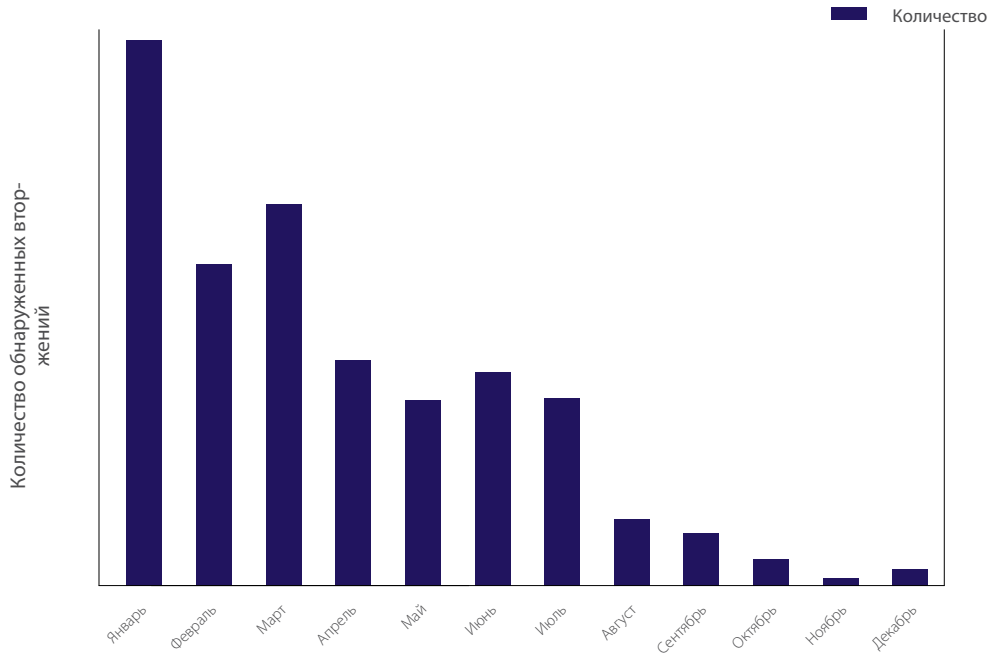


Рис. 7: частота обнаруженных вторжений вредоносной программы Industroyer, 2018 г.

Этот сценарий развития событий подтвердила атака на алюминиевый гигант **Norsk Hydro** в марте 2019 года, которая привела к останову нескольких заводов и в первую неделю стоила компании 40 млн долларов. Хотя сообщалось, что вредоносная программа **LockerGoga**, которая использовалась в этой атаке, дорабатывается и совершенствуется, ее первое появление было относительно стандартным и напоминало поведение более ранних вредоносных программ. [10]

EternalBlue: угроза устаревшим Windows-системам

Согласно заявлению бывшего сотрудника, угроза EternalBlue была разработана Агентством национальной безопасности США (NSA). 24 апреля 2017 года она была похищена хакерской группой Shadow Brokers и использовалась в атаках программ-вымогателей WannaCry и NotPetya позже в том же году. Предполагается также, что она является компонентом банковского червя Retefe. Угроза использует уязвимость в протоколе компании Microsoft Server Message Block (SMB).

Корпорация Microsoft обновила SMB до нового протокола, который получил название Common Internet File Sharing (CIFS), поэтому IT-системы с обновленной инфраструктурой Microsoft Windows просто должны настроить в CIFS запрет на прием запросов, использующих старый протокол SMB. К сожалению, многие системы ICS / SCADA построены на более старых версиях Windows, которые не поддерживают CIFS. Это требует размещения в межсетевом экране следующего поколения (NGFW) внешнего элемента управления, который пропускает определенные типы трафика SMB, и отклоняет весь остальной трафик.

Тенденция: глобальная география атак на OT-системы

В глобальной экономике, в которой во многих отраслях доминируют глобальные игроки и которая характеризуется чрезвычайной связностью, границы легко пересечь как легальным субъектам, так и преступникам. Рисунок 8 показывает, что, хотя атаки, нацеленные на большинство поставщиков, имели относительно низкий уровень в разных регионах, от эксплойтов для Rockwell и Schneider в большей степени пострадала Америка (Северная и Южная), где их доля на рынке наиболее высока. С другой стороны, системы Moxa распространены повсеместно и подвергаются атакам по всему миру, несмотря на то, что самая крупная атака на их пользователей — уязвимость Moxa 313 — была ориентирована на Японию (см. «Уязвимость Moxa 313: эксплойт с локализованной целью» на странице 13).

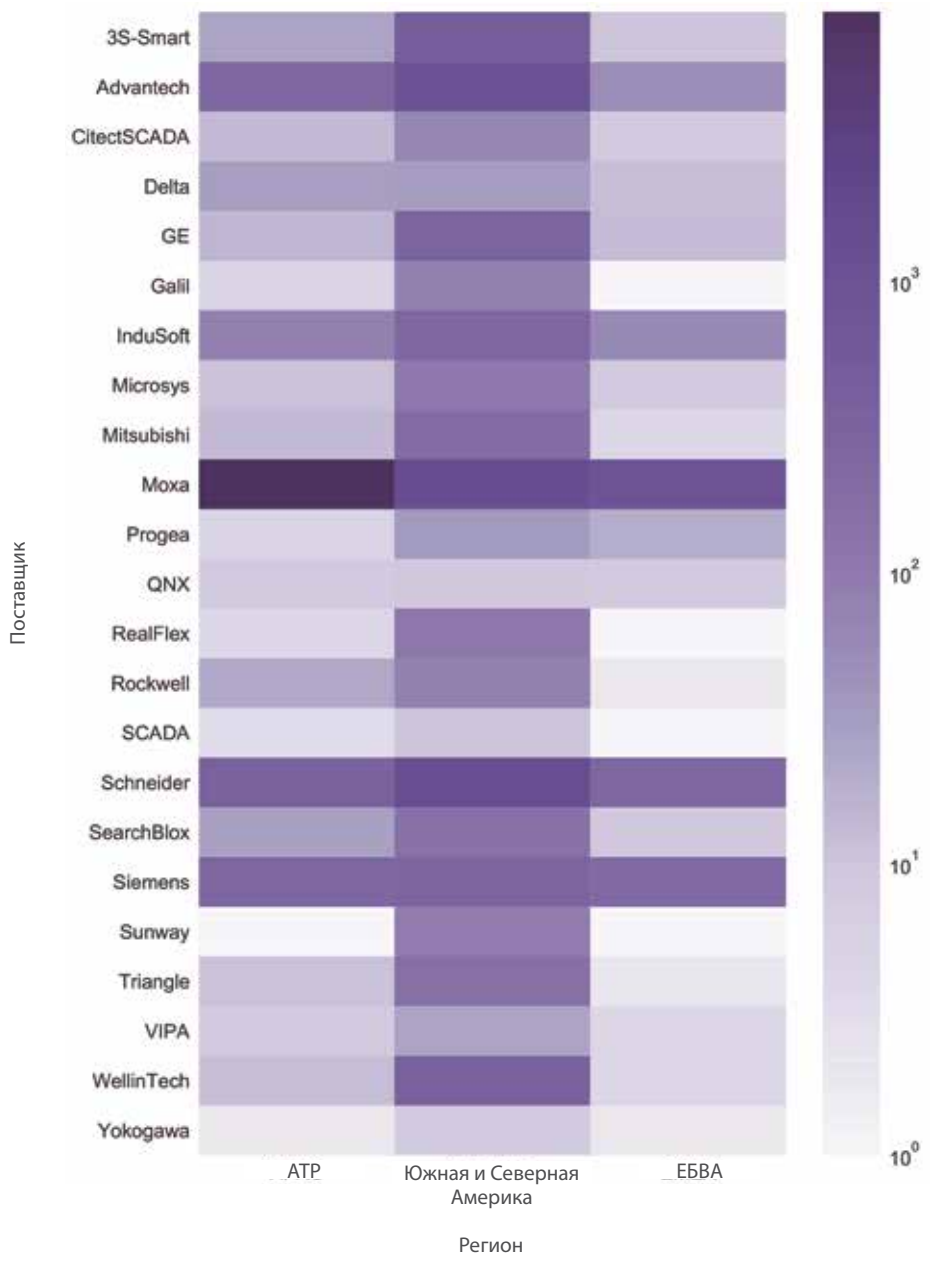


Рис. 8: распределение обнаруженных вторжений существующих угроз, нацеленных на ICS/SCADA-системы конкретных поставщиков, по регионам, 2018.

На рис. 9 показано, что хотя протоколы BACnet и Modbus широко использовались по всему миру, в странах ЕБВА их используют наиболее интенсивно. Объем обнаруженных протоколов был или равномерно распределен по разным регионам, или сконцентрирован в областях, где они используются больше всего. Например, протокол ICCP используется главным образом такими поставщиками, как Siemens и Honeywell, присутствие которых в Азии незначительно.

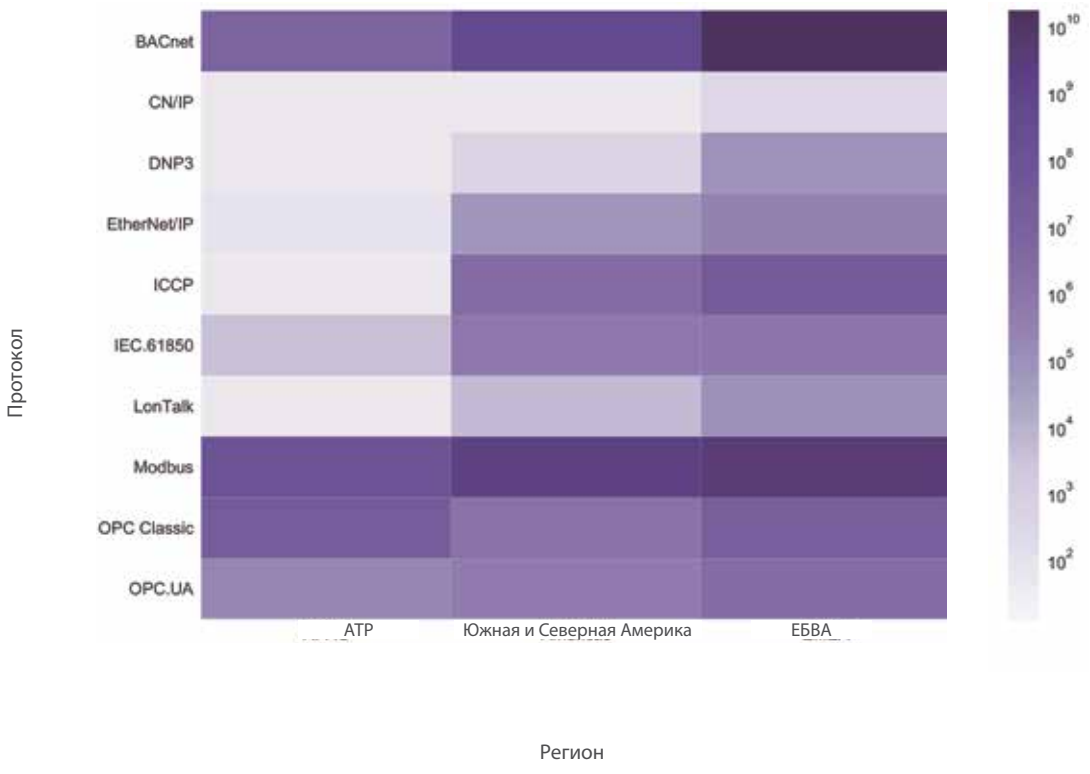


Рис. 9: распределение всех обнаруженных вторжений существующих угроз, 2018.

Уязвимость Moxa 313: эксплойт с локализованной целью

Эта атака, обнародованная в апреле 2018 года, нацелена на уязвимость при выполнении команд операционной системы на устройствах Moxa, из-за которой системе не удается проверить ввод при обработке вредоносного запроса Telnet. В апреле, мае и июне она с рекордной скоростью поразила тысячи межсетевых экранов следующего поколения (NGFW), а к сентябрю почти полностью исчезла (рис. 10) — вероятно, из-за установки в системы исправлений безопасности для защиты от этой угрозы.

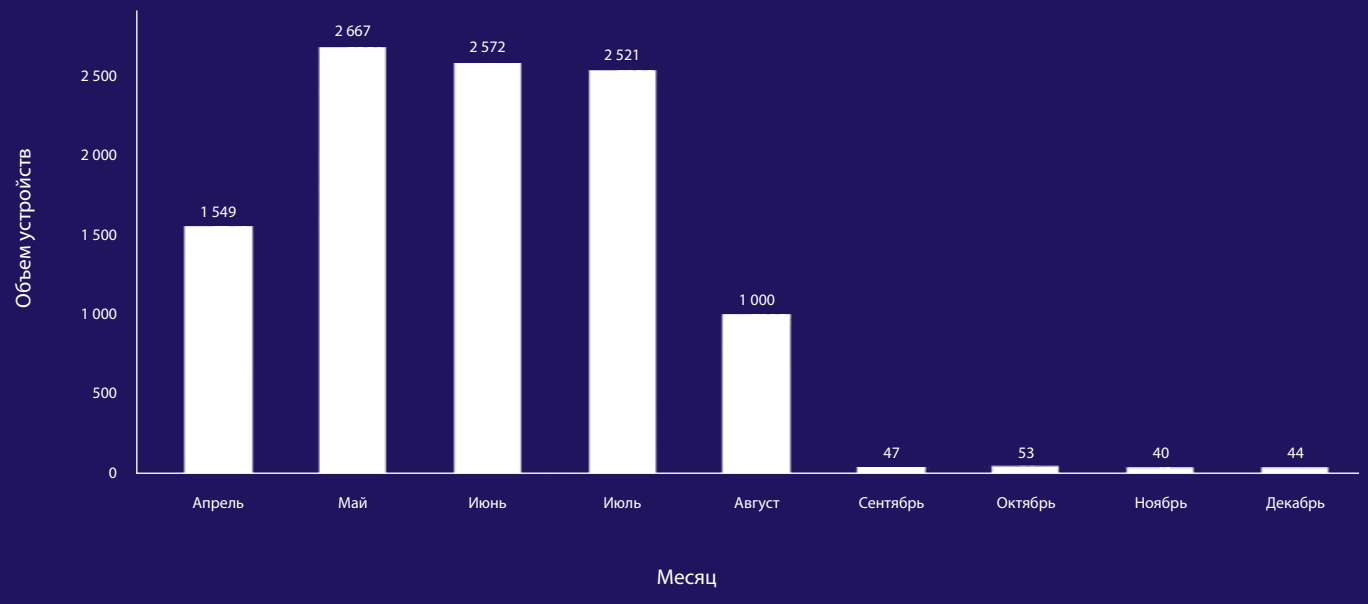


Рис. 10: частота обнаруженных вторжений Moxa 313 по месяцам, 2018 г.

Анализ географического распределения этого эксплойта показывает, что атака почти полностью ограничена Японией (рис. 11), где технология Moxa широко используется в продуктах автоматизации для дома и бизнеса. Однако Moxa часто используется в других странах мира. Тот факт, что эта атака развивалась очень быстро — даже в изолированном регионе — подчеркивает тот факт, что субъекты угрозы, как правило, нацелены на самые маленькие и самые простые части инфраструктуры OT: мосты и последовательные преобразователи.

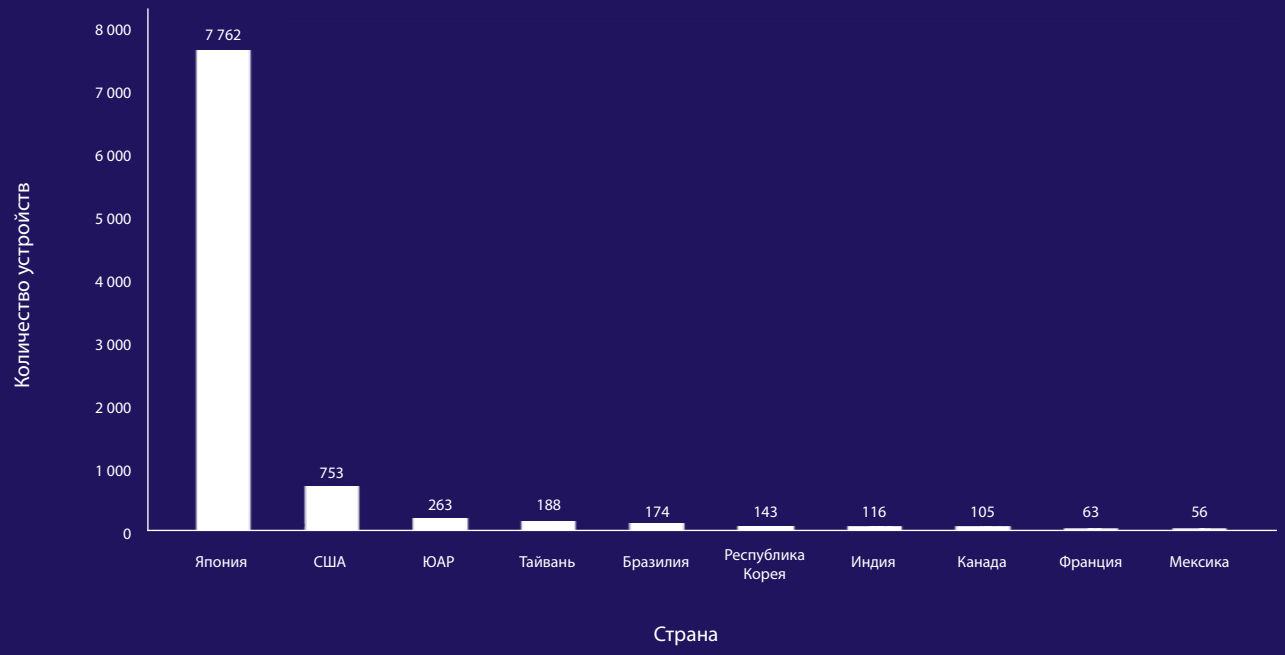


Рис. 11: частота обнаруженных вторжений Moxa 313 по странам, 2018 г.

Заключение

Отчет компании Fortinet о тенденциях в сфере безопасности эксплуатационных технологий за 2019 год описывает реальную картину, к которой все организации, подключающие системы ICS/SCADA, должны отнестись со всей серьезностью. Злоумышленники обладают стратегическим мышлением и извлекают максимальную выгоду из каждой новой угрозы, которую разрабатывают, используя эксплойты в незащищенных системах и уязвимости как в старых, так и в новых технологиях. Специфические проблемы, вызванные продолжительными циклами замены оборудования и вытекающим из этого преобладанием устаревших технологий, остаются актуальными уже много лет.

Правительства стран мира реагируют на эти новые угрозы, особенно в отношении критически важной инфраструктуры. Риски велики, вплоть до глобального экономического коллапса. В противовес рискам правительства разработали руководящие принципы, помогающие предприятиям защитить свои критически важные ресурсы. Например, стандарты Североамериканской корпорации по вопросам надежности электроснабжения (NERC) были введены в ответ на отключение электроэнергии в 2003 году на северо-востоке США. Тот факт, что стандарты NERC и Национального института стандартов и технологий (NIST), становятся все более строгими, является еще одним признаком реальности угрозы.

Системы ICS и SCADA с давних пор были и остаются рабочими лошадками технологических процессов во многих организациях и на протяжении десятилетий работают без значительных обновлений. Реальность продвинутых постоянных угроз требует более стратегического подхода — от установки обновлений безопасности до сегментации и управления доступом. Крайне важно, чтобы на эти системы распространялся тот же уровень защиты, те же стандарты безопасности и те же процессы отслеживания и отчетности, что и в IT-сети. В противном случае OT-сеть станет слабым звеном, через которое злоумышленники смогут осуществить вторжение и получить доступ к критическим системам и данным — как OT, так и IT.

Чтобы исправить положение, сотрудники IT- и OT отделов во всех организациях должны преодолеть культурные проблемы, вызванные их изолированным положением в прошлом. Группы должны прийти к пониманию ценностей друг друга, чтобы в будущем можно было установить взаимовыгодные отношения. Угрозы реальны, и они будут расти. Лучший способ противостоять им — это комплексный стратегический подход, распространяющийся на всю организацию.

Справочные материалы

[1] Барбара Филкинс (Barbara Filkins), The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns, SANS Analyst Program, июль 2018 г.

[2] Джеф Голдман (Jeff Goldman), IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices, eSecurity Planet, 8 ноября 2017 г.

[3] State of Operational Technology and Cybersecurity Report, Fortinet, март 2019 г.

[4] Серьезные риски кибербезопасности, которые угрожают системам SCADA/ICS, выявленные в ходе независимого исследования, Fortinet, 7 мая 2018 г.

[5] Оливер Гессер (Oliver Gasser) и др., Security Implications of Publicly Reachable Building Automation Systems, Technical University of Munich, по состоянию на 18 апреля 2019 г.

[6] Quarterly Threat Landscape Report, Q4 2018, Fortinet, по состоянию на 9 апреля 2019 г.

[7] Эрик Палмер (Eric Palmer), Merck has hardened its defenses against cyberattacks like the one last year that cost it nearly $1B, FiercePharma, 28 июня 2018 г.

[8] Ричард Чиргвин (Richard Chirgwin), IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz, The Register, 25 января 2018 г.

[9] Quarterly Threat Landscape Report, Q4 2018, Fortinet, по состоянию на 9 апреля 2019 г.

[10] Линдси О'Доннел (Lindsey O'Donnell), Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities, Threatpost, 27 марта 2019 г.

[11] Чарли Осборн (Charlie Osborne), Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout, ZDNet, 30 апреля 2018 г.

[12] Лили Хей Ньюман (Lily Hay Newman), Menacing Malware Shows the Dangers of Industrial System Sabotage, WIRED, 18 января 2018 г.

[13] FortiGuard Threat Intelligence Brief, Fortinet, 2 февраля 2018 г.

[14] Тара Силс (Tara Seals), SAS 2019: Triton ICS Malware Hits A Second Victim, Threatpost, 10 апреля 2019 г.

www.fortinet.com/ru

октября 18, 2019 2:47 ПП

D:\Projekty\Fortinet (United Kingdom)\P-344888\02_to dtp qa\General\Report-security trends-A4\Report-security trends-A4_RU

352048-0-1-RU