# Потребность в безопасности **OT, вызванная кибератакой** на трубопроводы


Colonial Pipeline Pipeline 8 мая стал жертвой программной атаки, и в результате все операции были остановлены. «Атака на колониальный трубопровод указывает на необходимость закрытия топливопровода и повышения безопасности OT», - сказал Эрай Атлас из OTD Bilisim.OT security.”

Colonial Pipeline, один из крупнейших топливопроводов в США, 8 мая стал жертвой атаки программ-вымогателей, и в результате все операции были остановлены. Атака на колониальный трубопроводы, где добывается почти половина нефти и газа Восточного побережья, является последним примером того, почему киберпреступники нацелены на нефтегазовую промышленность.

## АТАКА НА КОЛОНИАЛЬНЫЙ ТРУБОПРОВОД С ПОМОЩЬЮ СЛУЧАЙНОГО ПРОГРАММНОГО

Согласно отчету The Wall Street Journal, компания Colonial Pipeline, оператор крупнейшего газопровода в США, была вынуждена прекратить свою работу 7 мая из-за атаки программы-вымогателя. Киберпреступники не только угрожают нанести ущерб энергетическим рынкам, они также нарушают поставки газа и дизельного топлива на Восточное побережье.Колониальный трубопровод служит важными воротами в восточную половину Соединенных Штатов. Трубопровод пропускной способностью около 4 миллионов баррелей в сутки является одним из основных источников бензина, дизельного и реактивного топлива для Восточного побережья. В субботу было опубликовано заявление, в котором говорится, что они стали жертвами атаки вымогателей, которая также затронула корпоративные ИТ-сети.

Эта атака не проводилась через операционные сети, которые контролируют трубопроводы и распределяют топливо отдельно от корпоративной сети. Colonial Pipeline в качестве меры предосторожности для сдерживания распространения атаки объявили, что закрывают трубопроводы. Многие люди, работающие в сфере безопасности, впервые подумали, что это еще одна атака иностранного правительства. Однако в субботу (8 мая) агентство Bloomberg представило отчет о том, что инициатором атаки была группа программ-вымогателей DarkSide. Известная своими планами «двойного вымогательства», DarkSide в четверг за два часа получила почти 100 гигабайт данных из сети Colonial. Если злоумышленники не заплатят требуемый выкуп, Colonial Pipeline сможет передать все украденные данные в Интернет, зашифровать компьютеры злоумышленников и полностью заблокировать сеть Colonial.Непонятно, сколько денег хотят киберпреступники и как они используют сеть. Однако ясно то, что эта атака является конкретным примером того, как киберпреступники сосредотачиваются на промышленных предприятиях, независимо от масштаба или отрасли.

## ПРИВЛЕКАТЕЛЬНАЯ ЦЕЛЬ: НЕФТЕГАЗОВАЯ ПРОМЫШЛЕННОСТЬ

За прошедшие годы нефтегазовая промышленность стала одной из самых мощных и экономически глобальных отраслей, поскольку она имеет решающее значение для мировой и национальной экономики. Это стало основной целью, поскольку конкуренты рассматривают эти отрасли как ценные цели для использования уязвимостей промышленных систем управления (ICS). В прошлом операционные технологии (OT), необходимые для нефтегазовых операций, были изолированными и «закрытыми», но сегодня операционные технологические сети обеспечивают более частые подключения к различным ИТ-инфраструктурам и Интернету, что открывает новые возможности для атак. Конвергенция и конвергенция OT и ИТ-сред в нефтегазовых операциях привели к бесконечному количеству уязвимостей безопасности как в ИТ, так и в средах OT.



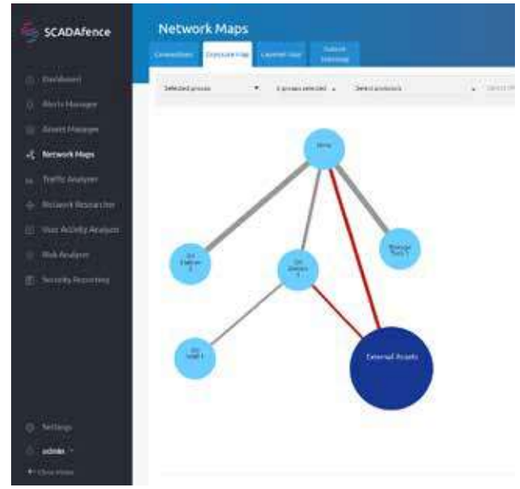


Также существуют постоянные и растущие приоритеты, направленные на соблюдение требований и риски, связанные с устройствами Интернета вещей (IoT). Их различное поведение очевидно из недавних атак на газовые и нефтяные компании, такие как Pemex и Colonial Pipeline. от понимания того, как использовать организации имеет много преимуществ. По этой причине никакие атаки не затрагивают мировую экономику и гражданскую безопасность. Защита стала необходимой для всех видов кибератак нефтегазовых организаций.

## ЗАЩИТА НЕФТЕГАЗОВЫХ ОПЕРАЦИЙ

Корпоративные сети конкурентов успешно атаковали Colonial Pipeline Подробности того, как это используется, не разглашаются. Однако он показал, что для нефтегазовых компаний настало время реализовать сильную стратегию безопасности OT. В прошлом месяце АНБ выпустило отчет, в котором объясняется важность защиты систем управления производством (ICS) и операционных технологий (OT) от кибератак. В отчете АНБ говорится, что «владельцы и операторы систем OT будут оставаться на недопустимом уровне риска, если не будут предприняты прямые действия по обеспечению устойчивости сетей OT и систем управления к уязвимостям в результате вторжений в ИТ и бизнес-сети». Кроме того, в отчете АНБ говорится, что организации и операторы должны защищать критически важные операции. «Системы OT редко нуждаются во внешнем подключении для правильного функционирования. Однако для удобства они часто предоставляют ссылки без учета фактического риска и потенциальных неблагоприятных результатов работы и задач. Незамедлительное принятие мер может помочь улучшить кибербезопасность и оставаться в курсе ». До того, как АНБ опубликовало этот отчет, содержащий его рекомендации, многие нефтегазовые компании приняли меры для защиты своих систем и сетей OT. В течение последних семи лет SCADAfence работала со многими организациями критически важной инфраструктуры, включая нефтегазовых операторов, для защиты своих сетей OT и обеспечения наличия соответствующей инфраструктуры кибербезопасности. Полная видимость сети также позволяет точно определять любое аномальное и вредоносное поведение, в том числе аномалии от атак программ-вымогателей.

SCADAfence работает со многими организациями критически важной инфраструктуры, в том числе с операторами нефтегазовой отрасли, для защиты сетей OT и обеспечения наличия соответствующей инфраструктуры кибербезопасности.




## ТАБЛИЦА ОБРАЗЦОВ МАСЛА В ПРИМЕНЕНИИ

На приведенной выше диаграмме показано, как SCADAfence помогает организациям в нефтегазовой и трубопроводной отраслях иметь полную видимость в своих ИТ-сетях и сетях OT. Таким образом определяется местоположение векторов атак и все соединения между сетями могут быть идентифицированы с абсолютной точностью. Благодаря такому подходу удалось успешно снизить количество аномальных действий в операционных сетях сотен организаций, которые впоследствии могут перерасти в кибератаки.

## В МИРЕ ОПЕРАЦИОННЫХ ТЕХНОЛОГИЙ НЕСПОСОБНОСТЬ ПЛАНИРОВАТЬ РАВНЯЕТСЯ ПЛАНИРОВАНИЮ К СБОЮ СИСТЕМЫ

Базовые методы кибербезопасности могут помочь предотвратить развитие этих атак. Это включает в себя обеспечение видимости всей сети, поскольку также сложно защитить то, что мы не видим. Дополнительные методы обеспечения безопасности включают сегментацию сети и даже микросегментацию, если это возможно, а постоянный мониторинг сети имеет решающее значение для предотвращения развития подобных атак. Многие нефтегазовые операторы уже используют технологии непрерывного мониторинга сети и обнаружения угроз для обеспечения видимости своих сетей OT и обеспечения безопасности критически важных инфраструктурных сетей. Благодаря этому целостному подходу к мониторингу сети, обнаружению аномалий, прозрачности удаленного доступа и соблюдению требований многие нефтегазовые организации снизили уровень риска будущих атак на 95%. Самое приятное то, что эти решения не требуют инструментов, ненавязчивы и способны выполнять эти задачи за небольшую часть затрат на сотрудника. Если вам тоже нужно защитить промышленные сети вашей организации, загрузите наше тематическое исследование с участием 100 лидеров нефтегазовой отрасли, чтобы узнать, как SCADAfence обеспечивает полную видимость сетей OT и обнаруживает угрозы злонамеренной активности в реальном времени. Если вы хотите попробовать платформу SCADAfence и найти какие-либо уязвимости в своей сети OT, мы будем рады вам помочь. Для получения более подробной информации о продуктах и вашего запроса PoC посетите страницу «https://onlineteknikdestek.com/Pocrequest?culture=tr». Если вам нужна более подробная информация об этой истории и подробная информация о продукте, вы можете связаться с отделом продаж OTD BİLİŞİM.