Объекты критической инфраструктуры: опасная иллюзия защищенности

В апреле 2020 года Национальный кибердиректорат Израиля (Israeli National Cyber-Directorate, INCD) выпустил предупреждение для компаний, работающих в сфере энергетики и водоснабжения, где просил как можно скорее сменить пароли для всех подключенных к интернету систем. В предупреждении сказано, что INCD получает сообщения о попытках атак на водоочистные сооружения, водонасосные станции и канализационные сети, которые подтвердили власти Израиля. Подробности атак не раскрываются, но глава INCD Игаль Унна заявил, что они могли привести к серьезной нехватке воды и потерям среди гражданского населения. Как сообщили власти, преступники атаковали автоматизированные системы управления технологическим процессом (АСУ ТП), но атаку удалось отразить.

Этот пример уязвимости казалось бы наиболее защищенных объектов, относящихся к критической инфраструктуре, был приведен на международный конференции CyberCrimeCon 2020 для иллюстрации иллюзии неуязвимости изолированных сетей госпредприятий. Результат —нередко формальный подход к обеспечению их кибербезопасности. Спустя почти десятилетие после успешного «нападения» на завод по обогащению урана в иранском городе Натанз с помощью червя Stuxnet и череду громких инцидентов на предприятиях энергетики — BlackEnergy в Украине и атаки на ГЭС в Венесуэле

— этот подход жив. Череда подобных громких событий заставляет промышленные предприятия обращать все более пристальное внимание вопросам защиты от киберпреступников. Следуя тренду, Group-IB вывела на рынок– Sensor Industrial, программно-аппаратный комплекс для раннего обнаружения сложных угроз и реагирования на атаки в промышленном секторе. Впервые он был представлен на CyberCrimeCon2020 как часть комплексной системы Threat Hunting Framework (THF).

Group-IB Threat Hunting Framework – сложная инженерная разработка, использующая собственные запатентованные технологии, не имеющие аналогов в мире. Она опровергает тезис о том, что детектирования и блокировки атаки сегодня достаточно. В THF заложена интеллектуальная система выявления угроз, которая учитывает тактические и стратегические знания об атакующих, их мотивацию, инструменты и инфраструктуру. Концепция хантинга за угрозами (от англ Threat Hunting), заложенная в разработку его создателями нашла отражение в Sensor Industrial, решающий вопросы дисбаланса в обеспечении безопасности технологического и корпоративного сегментов.

Давайте разберемся в этом детально: корпоративные сети — первый рубеж для киберпреступников — обороняются высококвалифицированными ИБ специалистами с использованием современных средств защиты. Для них существует актуальная карта угроз и прогнозируемые риски.

Технологические сети зачастую существуют в условиях недостатка материальных и людских ресурсов для обеспечения их кибербезопасности. Это усугубляет и без того сложную естественную проблематику – долгий жизненный цикл оборудования, быстро устаревающее программное обеспечение, сложность его обновления без остановки производства, длинная цепочка координации между ИТ, ИБ и АСУ подразделениями.

Автоматизация бизнес-процессов и связанное с ней сращивание корпоративного и технологических сегментов в разы увеличили уязвимость последнего. Даже опосредованное подключение промышленных систем, в том числе АСУ ТП, к другим сетям позволяет злоумышленники применять самые различные методы — от поиска уязвимостей в протоколах сетевого взаимодействия систем АСУ ТП до социальной инженерии — для компрометации компьютеров сотрудников.

Исходный вектор

Насколько серьезны проблемы промышленного сектора? Практика сокрытия киберинцидентов на промышленных объектах и производственных предприятиях, которые зачастую являются объектами критической инфраструктуры, затрудняет ответ. Условия, в которых жертвам тяжело хранить молчание, — перебои в производстве или даже его остановка. Критичность известных инцидентов говорит сама за себя.

Примеры атак на критическую инфраструктуру:

тревожных сирен, установленных на улицах города.

***2017 г.** - С 12 по 15 мая WannaCry проник в промышленные сети производственных компаний, нефтеперерабатывающих заводов, объектов городской инфраструктуры и распределительной энергосети.*

***2018 г.** - В августе нефтехимическая компания с заводом в Саудовской Аравии была поражена новым видом кибератаки, которая должна была саботировать деятельности компании и вызвать взрыв на производстве.*

***2019 г.** - В 2019 году Lazarus атаковал энергетическую ядерную корпорацию в Индии. В результате 19 октября 2019 года второй энергоблок АЭС был отключен. Выбор жертвы нетипичен для этой прогосударственной группы и может свидетельствовать о растущем интересе к таким атакам со стороны военных ведомств.*

***2020 г.** - Японский автоконцерн Honda подвергся атаке шифровальщика Snake, в результате чего компания была вынуждена приостановить производство на ряде предприятий.*

Киберпреступники используют три основных сценария атак на технологический сегмент. Первый – атаки на пользовательские устройства корпоративной сети с использованием социальной инженерии. Открывая фишинговое письмо с файлом или ссылкой, ведущими на загрузку вредоносного ПО, пользователь впускает злоумышленника на рабочую станцию. Даже если в этот момент атаку заметят службы ИБ и постараются остановить, этих действий может быть уже недостатоточно. Дальше это ВПО распространяется на другие хосты в корпоративной сети, чаще всего берет под контроль управление доменом Active Directory и ищет «мостики» в технологическую сеть. Если они есть – перемещается в нее и развивается уже в сети АСУ ТП. Совершенно не обязательно активные действия последуют незамедлительно: целевые атаки на технологические сети развиваются годами.

Второй путь, тоже традиционный, это заход с внешнего периметра — проникновение в корпоративную сеть через веб-сервисы, «торчащие наружу», например корпоративный портал или почтовый сервис.

Аналитика реагирований на киберинциденты экспертов Лаборатории компьютерной криминалистики Group-IB, говорит, что в 90% случаев атаки на технологический сегмент идут именно через корпоративные сети, то есть через первые два сценария.

Третий сценарий таргетирован на предприятия, использующие подход air-gap, т.е. поиск «воздушного зазора» для проникновения в физически изолированные критические сегменты сети. В этом случае ВПО может попасть в технологическую сеть через, например, флеш-носители.

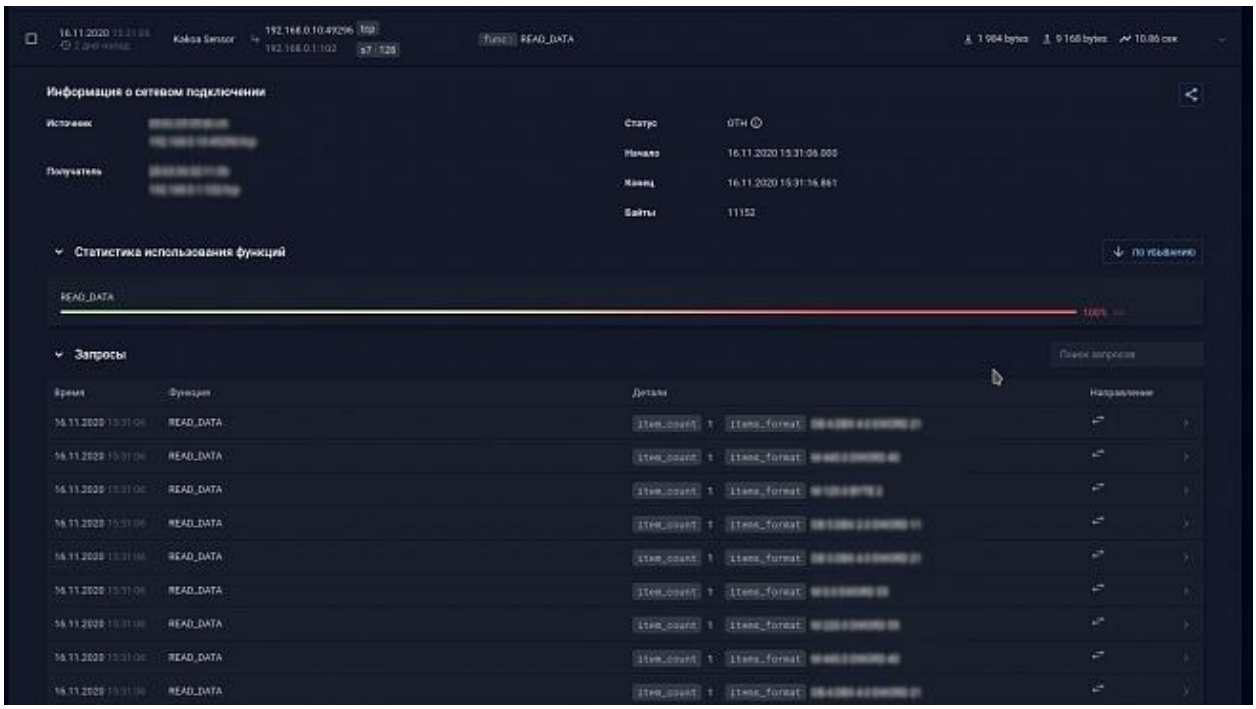
Мотивы киберпреступников, атакующих АСУ ТП, могут быть разными: это вывод из строя оборудования, остановка производства, шпионаж. Согласно отчету Hi-Tech Crime Trends 2020-2021: Компрометация АСУ ТП позволяет фиксировать технологии производства и конечные параметры изделий. Можно вести учет объемов: например, для производства определенных видов военной продукции необходимы сплавы с четко заданными параметрами. Если известен объем производства этих сплавов, то вычислить, сколько из них сделано конечных изделий, вычислить нетрудно. Промышленный шпионаж и военная разведка — области, где слежка за АСУ ТП крайне эффективна.

Экспертам Group-IB известны кейсы, когда злоумышленники попадали внутрь инфраструктуры промышленных предприятий непреднамеренно. Они не преследовали цель вывести из строя оборудование конкретного объекта: его остановка происходила в результате случайного заражения, например вирусом-шифровальщиком. Опасность таких атак заключается в их непредсказуемости.

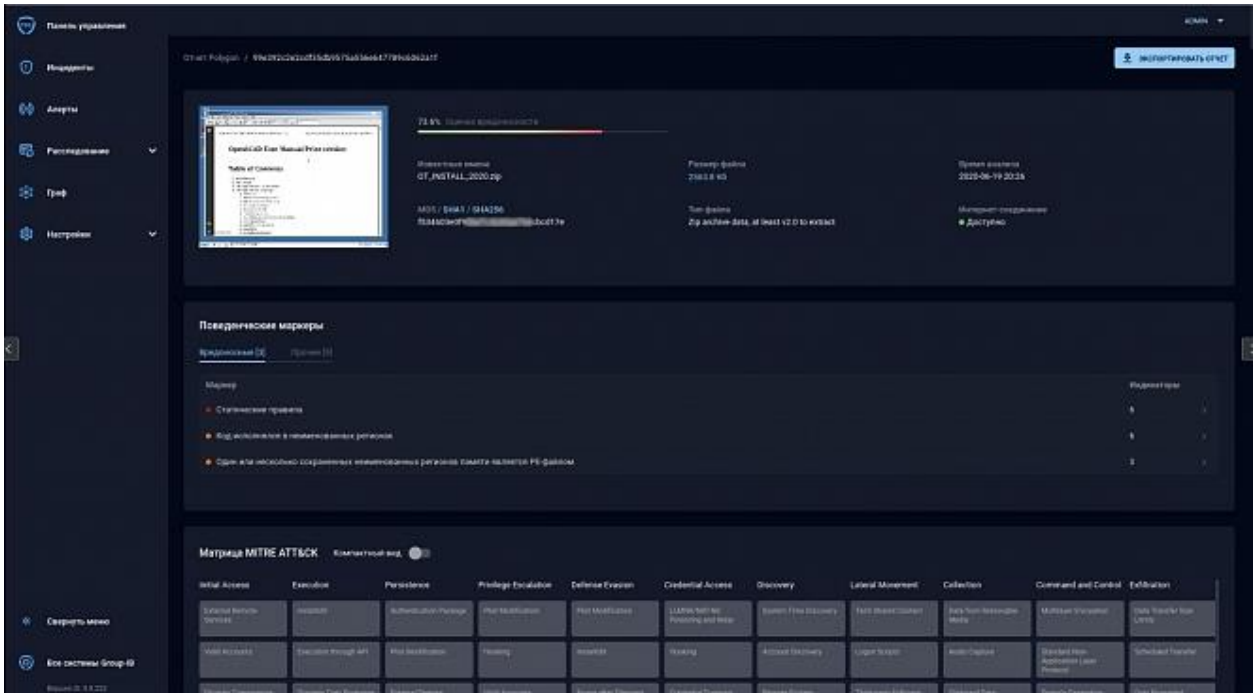
Защита от высокотехнологичных атак

Решения, обеспечивающие безопасность инфраструктуры объектов промышленности и производства, должны быть комплексными и способными выявлять кибератаки на любом этапе их осуществления. Их задача — полностью контролировать сеть, мониторить аномалии и нестандартную сетевую активность АСУ ТП, фиксировать недокументированные возможности промышленных протоколов, отслеживать все действия в сети. Новый игрок на рынке таких решений — Group-IB Threat Hunting Framework.

Его модули соединяют в себе защиту корпоративного и технологического сегментов сети, что позволяет детектировать весь спектр угроз для ИТ-инфраструктур промышленных предприятий — эксплойты, бэкдоры и вредоносные скрипты; скрытые каналы передачи данных; бестелесные угрозы; атаки с использованием легитимных инструментов; а также угрозы нулевого дня.



Threat Hunting Framework выявляет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Аппаратно-программный комплекс THF работает с копией трафика АСУ ТП, ведет пассивный мониторинг. Продукт обеспечивает защиту рабочих мест операторов, каналов взаимодействия между узлами связи и между сегментами сети.



Функциональные особенности

Архитектура Threat Hunting Framework представлена шестью модулями:

Sensor предназначен для анализа входящих и исходящих пакетов данных. Он позволяет выявить взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Для работы сенсор использует собственные сигнатуры, детект аномалий для выявления скрытых туннелей в верхнеуровневых протоколах и выявления Lateral Movement (распространения угроз во внутренней инфраструктуре и между сегментами), а также поведенческие правила.

Polygon проводит поведенческий анализ подозрительных объектов в безопасной среде. Полученные по электронной почте или скачанные из интернета файлы проверяются до попадания на компьютеры пользователей. Применение технологий машинного обучения позволяет выявить ранее неизвестные вредоносные программы без использования сигнатур, а также блокировать их доставку пользователям.

Huntpoint позволяет проводить фиксацию хронологии поведения пользователя, отслеживать процессы, происходящие на системе для выявления вредоносной активности, а также проводить сбор дополнительной контекстной информации для выявления вредоносного поведения на хосте.

Huntbox – центр управления, мониторинга, хранения событий и обновлений, устанавливаемый внутри инфраструктуры заказчика.

Sensor Industrial предупреждает атаки на ранних стадиях в технологическом сегменте предприятия.

Decryptor – дополнительный опциональный модуль, представляющий собой программно-аппаратный комплекс, предназначенный для вскрытия и анализа содержимого шифрованных сессий, позволяющий повышать видимость и уровень контроля трафика защищаемой инфраструктуры, а также качество обнаружения целевых атак.

Модуль Sensor Industrial имеет конструктор правил, характерный для технологического оборудования. Можно задать необходимые диапазоны наиболее критичных параметров, которые необходимо отслеживать.

Базовая версия Sensor Industrial отслеживает факты подключения к технологическому оборудованию, попытки модификации, скачивания, загрузки программ управления, остановки технологических процессов и другие нарушения. Sensor Industrial не просто мониторит подозрительные действия, но позволяет восстановить весь ход вторжения, определить его цель и источник угрозы.

Доступны несколько вариантов развертывания комплекса: от полностью автономного программно-аппаратного до облачного. Инсталляция на виртуальной машине в частном облаке заказчика – наиболее распространенный вариант проведения пилота. Он сразу позволяет увидеть, какое вредоносное ПО находится в сети — как в корпоративном, так и в технологическом сегменте.

Для Threat Hunting Framework реализована интеграция с SIEM-системами: наилучшие результаты достигаются при совместном применении THF и SIEM, одно другого не заменяет. Выполняется сигнатурный анализ сетевого трафика, выявление сетевых аномалий, таких как DGA (Domain Generation Algorithm) или туннели в прикладных протоколах, с помощью алгоритмов машинного обучения.

Комплекс THF является частью экосистемы раннего предупреждения и поиска киберугроз Group-IB, построенной на общей технологической платформе Threat Intelligence & Attribution. В нем используются эксклюзивные данные киберразведки о действиях злоумышленников, в том числе информация о появлении новых вредоносных программ и адресов командных центров, изменениях известных вирусов, смене тактики атак, что позволяет быстро адаптировать защитные механизмы к постоянно меняющемуся ландшафту угроз.

кибербезопасность, Корпоративная информационная безопасность

Горячие темы: Аксиомы кибербезопасности

Журнал: Журнал IT-Manager [№ 11/2020], Подписка на журналы

Group-IB

https://www.it-world.ru/cionews/security/168026.html