Киберугрозы для промышленных предприятий в 2021 году

Евгений Гончаров

Представляем наше видение того, какие вызовы уже стоят или вскоре будут стоять перед промышленными предприятиями и чего ожидать от киберпреступников в 2021 году.

Случайные заражения

1. Заражения будут становиться менее случайными или иметь неслучайные продолжения. У злоумышленников было несколько лет, чтобы провести профилирование случайно зараженных компьютеров, имеющих либо прямое отношение к технологическим сетям промышленных предприятий, либо периодический доступ к ним. Доступ к компьютерам будут перепродавать (возможно, уже продают) продвинутым группировкам, у которых есть специфические схемы монетизации атак на технологические системы промышленных объектов.
2. Некоторые группировки уже несколько лет специализируются на атаках промышленных предприятий для прямой кражи денег — по схемам BEC или проводя сложные хакерские атаки, чтобы получить доступ к финансовым и бухгалтерским системам организации-жертвы.
3. За эти годы они хорошо изучили особенности бизнес-процессов промышленных предприятий, а также получили доступ к большому объему технической информации об объектах технологической сети и технологическом процессе. Мы ожидаем появления новых интересных сценариев атак на АСУ ТП и полевые устройства, а также неожиданных схем их монетизации. Времени и возможностей для их разработки у злоумышленников было предостаточно.
4. Снятие с поддержки Windows 7 и Server 2008, популярных в ICS по всему миру, и, особенно, утечка исходных кодов Windows XP, которая до сих пор очень часто встречается в промышленных сетях, представляют существенную угрозу безопасности промышленных предприятий. Есть высокая вероятность повторения сценария наподобие WannaCry в самом ближайшем будущем. И промышленные предприятия могут оказаться в числе наиболее пострадавших.

Атаки вымогателей

1. Вымогатели становятся все более технологически оснащенными и изощренными. Злоумышленники продолжат использовать приемы хакерских атак и APT: будут кропотливо изучать сеть атакованной организации и осторожно продвигаться внутри нее, чтобы закрепиться и найти наиболее ценные или уязвимые системы для атаки, получить аккаунты администраторов, молниеносно и одновременно запускать атаку стандартными средствами администрирования.
2. Злоумышленники почувствовали вкус к нападениям на промышленные компании, ведь те платят выкуп. Атаки продолжатся.

3. Мы ожидаем гибридные атаки с кражей документов и последующей угрозой их публикации в случае отказа платить выкуп или продажей украденной информации в даркнете.
4. Получат развитие идеи, реализованные в Snake: выраженная направленность шифровальщиков на АСУ ТП.
5. Велика вероятность, что мы увидим атаки, замаскированные под атаки вымогателей, но с совсем иными целями, как это уже было с ExPetr.

Кибершпионаж

1. Злоумышленники поймут (а некоторые уже поняли), что внутри периметра OT секреты охраняются хуже, чем в офисных сетях, а пробиться в технологическую сеть может быть даже проще ввиду наличия собственного периметра и поверхности атаки.
2. «Плоская сеть» и прочие проблемы с разграничением доступа в OT-сетях могут сделать их привлекательной точкой входа в труднодоступные уголки корпоративной сети или дорожкой к инфраструктуре других организаций, а также прочим объектам холдингов и корпораций.
3. Санкционная политика и стремление многих стран к технологической независимости приведут к тому, что среди мишеней атаки будут не только геополитические противники, но и тактические и стратегические партнеры — никому нельзя будет доверять. Примеры таких атак мы видим уже сейчас.

APT

1. Количество APT-группировок продолжит расти — мы будем видеть все больше новых акторов, в том числе атакующих организации, относящиеся к различным промышленным секторам.
2. Активность группировок будет коррелировать с локальными конфликтами, в том числе в «горячей фазе»: кибератаки, включая атаки на промышленные предприятия, будут использоваться как инструмент военных действий наряду с беспилотниками и информационными атаками через СМИ.
3. Помимо задач «закрепиться на черный день» и кражи информации, кто-то рано или поздно обязательно перейдет к более активным действиям. Не исключено, что в 2021 году мы увидим продолжение серии Stuxnet — Black Energy — Industroyer — Triton.

Последствия COVID-19

1. На фоне общего ухудшения экономической обстановки, локдаунов, снижения темпов роста, разорения и банкротства мелкого бизнеса повысится конкурентная привлекательность предложений киберкриминала на соответствующем рынке труда – пополнятся ряды киберзлоумышленников и усилятся группировки, ассоциированные с правительствами многих стран.

2. Переход в онлайн и цифровизация муниципальных и государственных сервисов сделают их более уязвимыми для злоумышленников, создадут больше возможностей для кросс-ведомственных атак и атак на смежные структуры. Злоумышленники могут добраться до финальной цели, такой как, например, транспортные системы, через каналы связи и цепочки поставок, объединяющие различные государственные, муниципальные и даже частные структуры, начав свою атаку, скажем, с веб-сервиса муниципальных или правительственных органов. Например, атака через сайт «Госуслуги» или через терминал оператора в районном центре «Мои Документы» на системы МВД и далее на камеры контроля скорости и элементы транспортной инфраструктуры.

3. Ограничение возможности проведения работ «на месте» замедлило темпы усиления защиты периметра — помешав, например, установке и настройке нового оборудования во многих промышленных организациях. Вкупе с увеличением количества и разнообразия сессий удаленных подключений это может привести даже к снижению уровня защиты периметров технологических сетей промышленных предприятий. Безопасность промышленных объектов в таких условиях будет в значительной степени зависеть от эффективности работы endpoint-решений и программ повышения осведомленности персонала. В то же время кибератаки, нацеленные на промышленные компании, становятся более зрелыми. Как следствие, даже несмотря на то, что количество атакованных компьютеров сокращается, число серьёзных инцидентов уменьшаться не будет.

4. Количество персонала на местах, способного своевременно перейти на ручное управление атакованными системами и установками в случае успешной кибератаки на компьютеры в технологической сети промышленных предприятий, сократилось. Это может способствовать увеличению масштаба распространения вредоносного ПО и усугубить последствия киберинцидентов.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com