Kaspersky ICS CERT

kaspersky

Киберугрозы для промышленных предприятий и OT-инфраструктур в 2024 году

Евгений Гончаров

31.01.2024 Version 1.0

Вымогатели 1
Хактивисты 4
Из «серой зоны» — в «тень» 5
Угрозы, связанные с логистикой и транспортом 6

Мы не ожидаем стремительных изменений в ландшафте киберугроз для промышленных предприятий в 2024 году. Большинство из описанных ниже тенденций уже наблюдаются, многие не первый год. Однако по некоторым направлениям накопилась критическая масса невидимых на первый взгляд изменений, способная привести к качественному сдвигу ландшафта угроз, который вполне может произойти и в следующем году.

Вымогатели

1. **Вымогатели останутся бичом № 1 промышленных предприятий в 2024 году**.

   В 2023 году атаки вымогателей прочно закрепились на первой позиции в рейтинге угроз ИБ для промышленных предприятий. Как видно из анализа официальных заявлений организаций, пострадавших от киберинцидентов в первом полугодии 2023 года, как минимум в каждом шестом случае атака вымогателей приводила к остановке производства или поставки продукции. В некоторых случаях ущерб от атаки оценивался в сотни миллионов долларов. На текущий момент не просматривается причин, по которым в ближайшее время ситуация могла бы измениться.

2. **Атаки вымогателей на крупные организации** или на поставщиков уникальных продуктов (оборудования, материалов), крупные логистические и транспортные компании **могут приводить к тяжёлым экономическим и социальным последствиям**.

   Уже сейчас минимум 18% атак вымогателей на промышленные предприятия по официальным подтверждениям атакованных компаний приводят к остановкам производства и/или поставок продукции. При этом атакующие явно уходят в «верхний сегмент» при выборе целей, предпочитая выбирать жертв именно среди крупных организаций, способных заплатить серьёзные суммы выкупа.

Складывается ситуация, когда атакующие, сознательно или по неосторожности, могут снова переступить черту, за которой последствия атаки имеют инфраструктурный характер, как это было при атаке на Colonial Pipeline. Недавняя атака на DP World, логистическую компанию и оператора контейнерных перевозок из Дубая, привела к частичной остановке портов Сиднея, Мельбурна и Брисбена, в которых было заблокировано около 30000 контейнеров.

3. Рынок вымогателей стремится к своему пику, за которым может последовать его падение или стагнация. Вряд ли потенциальные жертвы станут в ближайшее время недосягаемы для атак. Но они могут научиться более эффективно смягчать их последствия (например, вложившись в безопасность наиболее конфиденциальных данных и организовав правильные процессы резервного копирования и реагирования на инциденты).

   Если в результате жертвы станут реже и меньше платить, злоумышленникам придется искать **новые типы целей и новые схемы монетизации атак**. Примеры возможных путей развития:

   a. **Атаки на логистические и транспортные компании могут быть нацелены** не на поддерживающую операции IT-инфраструктуру, а **на сами транспортные средства** (автомобили, суда).

      На первый взгляд, реализацию такой атаки затрудняет большое разнообразие транспортных средств в парках и флотах, что многократно увеличивает расходы злоумышленников на разработку и, соответственно, приводит к удорожанию атаки. Однако атака может быть нацелена не на одного конкретного владельца или оператора, а на множество транспортных средств определенного типа, одинаковых или сходных с точки зрения внутренних систем управления.

      Другой фактор, упрощающий атаку, заключается в том, что владельцы и операторы флотов дополнительно оснащают транспортные средства своими кастомными системами сбора телеметрии, часто неявно обладающими и возможностями удалённого управления (например, для удалённой прошивки самого блока или для изменения набора собираемых данных). То же самое иногда делают и производители транспортных средств, и провайдеры различных сервисов. Таким образом этот вектор становится вполне реалистичным.

      В случае такой атаки самостоятельно восстановить операционную деятельность жертва не сможет, не понеся расходов, несовместимых с продолжением бизнеса. Восстановить (например, из бэкапов) работу зашифрованных IT-систем гораздо проще, чем решить даже технически

простую проблему (например, удалить вредоносное ПО, не дающее запустить двигатель грузовика или отключающее электропитание систем судна) на разбросанных по большой территории транспортных средствах. Компании, вероятно, окажутся не в состоянии самостоятельно решить проблему за разумное время и с приемлемыми для бизнеса финансовыми потерями.

b. **Этот же вектор актуален и для владельцев и операторов различной спецтехники**, работающей на труднодоступных удалённых площадках, например в горнодобывающей промышленности или в сельском хозяйстве.

c. Проблема обеспечения кибербезопасности множества труднодоступных объектов актуальна и для нефтегазовых компаний, организаций, предоставляющих коммунальные услуги, и вообще любых организаций, имеющих сильно распределённую OT-инфраструктуру. **Атака на далёкие и труднодоступные объекты, исключающая возможность удалённого восстановления** (например потому, что штатный канал удалённого доступа заблокирован вредоносным кодом), **гарантирует выплату выкупа**.

d. **Нестандартные способы монетизации** (например, посредством игры на бирже) **атак на экономически значимые предприятия** — крупные транспортные и логистические организации, крупные добывающие компании, производителей и поставщиков материалов (например металлов, сплавов и композитов), сельскохозяйственной продукции и продуктов питания, поставщиков уникальных / востребованных продуктов, недопоставки которых сложно быстро компенсировать (микрочипы, удобрения и прочее).

   Перебои с поставкой продуктов таких предприятий могут заметно сказаться на рыночной цене товаров. При этом, помимо прямых последствий, могут возникать и цепные реакции, и совсем уже опосредованные побочные эффекты. Вспомним, как атака Shamoon на Saudi Aramco внезапно повлияла на стоимость жёстких дисков на мировых рынках — после того как компания приняла неожиданное решение поменять жёсткие диски всех своих поражённых атакой компьютеров на новые.

Хактивисты

4. **Действия политически мотивированных хактивистов** вдоль линий геополитической напряжённости **будут иметь более разрушительные последствия**.

   Мы все помним нашумевшие атаки хактивистов на железнодорожный транспорт и на заправочные станции в Иране в 2022 году. В прошедшем 2023 году — атаку на системы поставки воды для ирригации в Израиле, серию атак на израильские ПЛК Unitronics Vision, жертвами которых стали объекты водоснабжения в США и Ирландии, и последнюю атаку, вновь направленную на заправочные станции Ирана. Если оставить за скобками PR-эффект, во всех этих случаях реальный масштаб негативных последствий действий злоумышленников был достаточно скромным.

   Однако в последних атаках хактивисты продемонстрировали способность добираться до OT-систем. В нескольких случаях, расследованных за прошедшее время специалистами Kaspersky ICS CERT, для нанесения физического ущерба злоумышленникам лишь немного не хватило подготовки и упорства. Эскалация напряжённости вполне может привести к тому, что атаки политически мотивированных хактивистов перейдут на качественно новый уровень и станут более опасными.

5. **В дополнение к протестным движениям внутри стран** на фоне роста социальной напряжённости (ввиду религиозных и этнических конфликтов и нарастающей экономической нестабильности во многих регионах планеты), **мы станем свидетелями развития космополитических протестных движений**, поддерживаемых хактивистами, — как следствия внедрения новой социокультурной и макроэкономической повестки. В частности, тема экологии и зелёных технологий (возобновляемая энергетика, электромобили и прочее) будет вызывать как поддержку, так и протест «экохактивистов». Пример — атака на горнодобывающую компанию в Гватемале, ответственность за которую взяла на себя группа «Guacamaya Roja».

6. Повсеместный всплеск по-разному мотивированных хактивистских движений приведёт к **развитию хактивизма анархического типа** — многие атаки будут совершаться без явных обоснований, просто для развлечения, как, например, в случае с Idaho National Laboratory, атакованной хактивистами SiegedSec.

Из «серой зоны» — в «тень»

7. Широкое использование методов «наступательной кибербезопасности» (offensive cybersecurity) для задач сбора данных кибербразведки (cyberthreat intelligence) будет иметь как позитивные, так и негативные последствия.

   С одной стороны, мы увидим некоторый рост защищённости организаций, так как наступательная кибербразведка (offensive cyberthreat intelligence) позволит добывать признаки компрометации не только из данных телеметрии защитных решений, результатов исследования инцидентов, косвенных источников и дарквеба, — как это делают поставщики «традиционного» CTI, — но и напрямую из инфраструктуры, контролируемой злоумышленниками. Это даст жертвам возможность эффективнее и быстрее восстанавливать безопасность своих систем.

   С другой стороны, став новой нормой, пусть и не легализованной официально, но применяемой с молчаливого согласия государств, использование наступательной кибербразведки будет иметь и негативные последствия — ведь грань между «серой зоной» и «тёмной стороной» порой исчезающе тонка, а искушение её переступить может оказаться непреодолимым. Прикрываясь потребностями в защите от агрессора, корпорации, следуя примеру государств, увеличат спрос на подобные услуги, в том числе и в целях, не связанных с кибербезопасностью. И некоторые промышленные компании могут также оказаться «в игре». Это особенно вероятно для высококонкурентных экосистем, к которым можно отнести строительство, добычу полезных ископаемых, энергетику и некоторые другие промышленные секторы.

   Такие кибер-активности будут ещё более точечными, чем мы привыкли видеть в операциях APT. В арсенал будет входить в основном коммерческий и open-source-инструментарий, что позволит эффективно маскировать активность на общем высоком фоне киберкриминальных атак. В результате подобные операции будут обнаруживаться и исследоваться ещё реже, чем операции APT.

Угрозы, связанные с логистикой и транспортом

8. Продолжающиеся высокими темпами **автоматизация и цифровизация логистики и транспорта приведут**:

   a. **К б*о*льшему сращиванию киберкриминала с традиционным**, в частности, в таких традиционно криминальных областях, как:

      - Кража автомобилей и прочего транспорта с использованием киберсредств (последнее особенно актуально в отношении автомобилей азиатских брендов, а также новых автопроизводителей, использующих агрессивную политику выхода на мировые рынки, — ввиду ожидаемых проблем со зрелостью их кибербезопасности).
      - Пиратство и нарушение логистических цепочек с использованием киберсредств — как логическое продолжение атак с использованием современных технологий, таких как недавние атаки на систему AIS (Automated Tracking System) в Красном море и Индийском океане или атака на иранский порт Шахид Райе в 2020 году.
      - Кража товаров с использованием киберсредств.
      - Нелегальная перевозка и импорт / экспорт товаров (контрабанда) — как логическое продолжение истории «Тринадцати друзей Оушена» в порту Антверпена.
      - Прочие махинации в логистических и транспортных операциях (например, для получения денег по страховкам и неустойкам) или другие трудно предсказуемые сценарии, как в недавнем случае с нечестной конкуренцией на железных дорогах в Польше.

   b. **К увеличению вероятности физических последствий случайных заражений**. Уже сейчас известны случаи заражения транспортных средств различных типов вредоносным ПО. В ближайшем будущем количество таких случаев будет расти — из-за всё более частого использования в транспорте «традиционных» ОС типа Android и Linux, широкой интеграции стандартных IT-компонентов и протоколов связи, увеличения количества сценариев, задействующих подключения к облачным сервисам. Есть немалая вероятность, что некоторые из них могут приводить к сбоям работы важных систем мониторинга и управления с трудно предсказуемыми последствиями. В первую очередь риск касается речного, морского, грузового автомобильного и спецтранспорта — состояние информационной безопасности этих объектов часто оказывается более плачевным, чем у легковых автомобилей.

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