kaspersky

Киберугрозы для АСУ и промышленных предприятий в 2022 году

Какими мы их видим в ноябре 2021 года

Евгений Гончаров

23.11.2021 Version 1.0

Продолжение тенденций последних лет

Мы наблюдаем различные тенденции изменения ландшафта угроз для промышленных предприятий, большинство из которых развиваются уже довольно долго. С большой степенью уверенности мы можем утверждать, что многие из тенденций не только сохранятся, но и получат новое развитие в будущем году.

Дальнейшая эволюция киберугроз как ответная реакция на внедрение средств и мер ИБ

Улучшение состояния защищенности организаций, внедрение все новых инструментов и мер защиты заставляют эволюционировать и киберугрозы. Вот некоторые из направлений такой эволюции, на которые хочется обратить внимание.

- **Уменьшение количества целей каждой отдельной атаки**

  Отдельные атаки в рамках криминальных кампаний уже сейчас становятся нацеленными на все меньшее количество жертв. Так, мы видим, что в криминальной экосистеме кражи данных аутентификации с использованием шпионского ПО выделилось новое направление: каждая отдельная атака направлена на очень небольшое количество целей (от нескольких единиц до нескольких десятков). Тенденция развивается настолько быстро, что в некоторых регионах мира до 20% ото всех компьютеров АСУ, на которых мы блокируем шпионское ПО, атаковано с использованием этой тактики. Вероятно, в следующем году такие атаки составят еще большую часть ландшафта угроз. Скорее всего, эта тактика распространится и на другие типы угроз.

- **Сокращение жизненного цикла вредоносного ПО**

  Для обхода детектирования все больше злоумышленников следуют стратегии частого обновления вредоносного ПО выбранного семейства: используют зловред на пике его эффективности после очередной пересборки для «сбивания детекта» защитных решений и переходят к новой сборке, как только предыдущая начинает уверенно детектироваться. Для некоторых типов угроз (например, для тех же шпионских программ) время жизни каждой сборки сокращается и во многих случаях не превышает уже трех-четырех недель (а часто оказывается еще меньше). Развитие современных MaaS-платформ существенно упрощает применение этой стратегии для операторов вредоносного ПО по всему миру. В следующем году мы, безусловно, столкнемся с еще более частым ее использованием для различного типа

угроз. В совокупности с тенденцией к уменьшению количества жертв каждой отдельной атаки широкое применение этой стратегии приведет к еще большему разнообразию вредоносного ПО и поставит тем самым непростую задачу для разработчиков защитных решений.

- **Современные APT: часто более упорные, чем продвинутые**

  Похожая в каком-то смысле тенденция прослеживается и в тактиках многих APT. Величина P (Persistent) в аббревиатуре APT все реже стала зависеть от качества A (Advanced). Мы давно наблюдаем, как постоянство присутствия в инфраструктуре жертвы обеспечивается скорее настойчивостью и аккуратностью действий операторов, а увеличение разнообразия инструментария и регулярное его обновление становятся альтернативой поиску оригинальных технических решений и затратной разработке сложных фреймворков, рассчитанных на то, что они долгое время не будут никем обнаружены. По всей видимости, эта стратегия будет еще чаще прослеживаться в APT-кампаниях.

- **Минимизация использования вредоносной инфраструктуры**

  В борьбе со средствами защиты злоумышленники, естественно, часто стремятся к тому, чтобы их операции оставили как можно меньше следов. В частности, это отражается в попытках сократить до минимума использование вредоносной инфраструктуры. Так, например, мы наблюдали, как в ряде случаев C&C некоторых APT жили очень короткое время, не более пары часов, в течение проведения той фазы операции, для которой они предназначались.

  А иногда злоумышленникам удается и вовсе отказаться от использования в своих атаках не только какой-либо вредоносной, но и любой подозрительной и недоверенной инфраструктуры. Например, популярной тактикой шпионских атак стала рассылка фишинговых писем со скомпрометированных корпоративных почтовых аккаунтов организации — партнера следующей жертвы. Хорошо составленные письма в таком случае никакими особыми признаками уже не отличаются от легитимных, и их практически невозможно обнаружить автоматическими средствами.

  При расследовании инцидентов, связанных с атаками APT на промышленные предприятия, мы натыкались на следы того, как злоумышленники, помимо работы по плану основной атаки, параллельно пытались из инфраструктуры скомпрометированного промышленного объекта получить доступ к другим организациям (ресурсам материнского холдинга, правительственных учреждений и так далее) —

отчасти, вероятно, в надежде, что такие попытки имеют больше шансов остаться незамеченными.

Без сомнения, в следующем году мы будем наблюдать более частое использование подобных тактик в операциях различных категорий злоумышленников.

Действия различных категорий злоумышленников

Рассуждения о том, каких угроз следует в первую очередь опасаться промышленным организациям, часто основываются на сравнениях APT и киберкриминала. И планы по улучшению информационной безопасности, внедрению новых средств и мер защиты так или иначе отталкиваются от выбранной модели нарушителя. При этом следует учитывать, что представления об интересах, возможностях и modus operandi некоторых категорий злоумышленников могут устаревать и поэтому требуют постоянного обновления. Расскажем о некоторых важных в этом смысле тенденциях, которые наверняка сохранятся или усилятся в следующем году.

- **Техники, тактики и даже стратегии, применяемые киберкриминалом и APT, все чаще становятся одинаковыми и могут требовать сходных мер защиты**

  В самом деле, во многих случаях действия APT и киберкриминала выглядят похоже и порой трудноразличимы даже для специалистов. Например:

  - Технически несовершенные APT и «продвинутые» криминальные атаки уже перестали кого-либо удивлять. В частности, нам не раз приходилось видеть совсем неуклюже составленные, изобилующие видимыми невооруженным глазом ляпами фишинговые письма в кампаниях, ассоциированных с действиями известных APT. И не раз мы наблюдали практически безупречно сделанные письма в целевых кампаниях киберкриминала.
  - Точно так же перестали удивлять APT, маскирующиеся под действия киберкриминала, и атаки киберкриминала, пытающегося прикинуться APT.
  - Без сомнения, мы не раз еще увидим в арсенале APT не только применение коммерческого инструментария, но и использование инфраструктуры и средств доставки MaaS как способа первоначального проникновения.

- **В списке целей и потенциальных жертв атак киберкриминала и APT легко могут оказаться одни и те же организации**

  Вероятно, из множества промышленных компаний в фокусе APT окажутся организации:

  - ВПК и аэрокосмической промышленности — скорее всего, в целях военного и технологического шпионажа;
  - энергетики, транспорта и ЖКХ — в попытке закрепиться «на всякий случай» и «на чёрный день» в критической инфраструктуре «вероятного противника» и для использования этой инфраструктуры с целью развития прочих атак (см. примеры выше);
  - наукоёмких отраслей производства — прежде всего, в целях промышленного шпионажа.

  Киберкриминал будет продолжать атаковать всех, до кого сможет дотянуться, и монетизировать атаки будет в подавляющем большинстве случаев все теми же хорошо отработанными способами, такими как:

  - прямая кража денег методом подмены банковских реквизитов — с использованием тактики BEC или доступа к финансовым системам организации;
  - шантаж и вымогательство у тех, кто способен и готов заплатить выкуп;
  - перепродажа украденной информации другим злоумышленникам, конкурентам жертвы и прочим заинтересованным лицам и организациям.

- **Прямой финансовый ущерб от атак киберкриминала больше, но ущерб от деятельности APT труднее прогнозировать, и он может оказаться более значительным в долгосрочной перспективе**

  Если по событиям прошедшего года судить о величине прямого финансового ущерба, причиненного промышленным организациям в результате различных кибератак, то криминальные атаки могут показаться намного опаснее для промышленных организаций, чем APT. Так, в 2021 году мы стали свидетелями остановки множества производств и выплаты десятков миллионов долларов вымогателям. При этом за весь год известен всего один случай безусловно существенного финансового ущерба от APT — и это случилось, когда атакующие решили маскироваться под вымогателей.

  Однако APT-атаки могут иметь отложенный во времени негативный эффект, который очень трудно заранее оценить (например, какая-нибудь иностранная организация может через несколько лет воспользоваться результатами атаки при создании нового продукта).

- **Не стоит забывать о киберхулиганах и хактивистах**

  В 2021 году хулиганам и хактивистам удалось как минимум трижды заявить о себе на весь мир, продемонстрировав, что важная для нашей жизни промышленная инфраструктура зачастую, может до сих пор быть легко доступна извне и недостаточно защищена. Вопрос о том, все ли возможное было сделано для того, чтобы в следующем году предотвратить случаи, подобные упомянутым выше, мы предлагаем читателю задать самому себе.

- **Вымогатели**

  Относительно, пожалуй, главного тренда уходящего года стоит сказать, что, несмотря на громкие заявления политиков и активные действия государственных структур, набравший обороты маховик вымогательства невозможно будет сразу остановить. Атаки продолжатся, в том числе и на промышленные предприятия. Злоумышленники станут лучше защищаться и «страховать» свои риски. Дополнительные расходы они покрывать будут, очевидно, за счет своих жертв — суммы выкупа будут расти.

Актуальные векторы атак

Следующие тактики и техники злоумышленников будут, без сомнения, активно применяться в грядущем году.

- **Фишинг** — как средство №1 первоначального проникновения в рамках целевой (и не очень) атаки. Как показывает практика минувшего года:
  - Даже очень плохой фишинг, как ни грустно это признавать, неплохо работает. Обучайте своих сотрудников элементарной внимательности и критическому отношению ко входящей корреспонденции. Ошибки в орфографии и грамматике, неверное употребление слов и неуместные выражения, неправильные названия организаций и должностных лиц, странный выбор темы и неожиданный поворот в тексте — все это может быть признаками неумело составленного фишингового письма. Распознать их способен каждый сотрудник, даже не имеющий специальных знаний и навыков.
  - Качественный целевой фишинг работает, к сожалению, «с гарантией». В каждой организации обязательно найдется человек, который откроет вложение, перейдет по ссылке или нажмет кнопку, а то и пообщается со злоумышленником, поможет решить проблемы совместимости и запустить вредоносную нагрузку в своей системе.

- Киберкриминал разного профиля освоил целевой фишинг без использования вредоносной инфраструктуры и фишинг, использующий только доверенную инфраструктуру (о нем много написано выше). Причем последний — это наиболее трудно обнаруживаемая и опасная тактика. К сожалению, она, вне всяких сомнений, найдет много жертв в грядущем году.

- **Известные уязвимости в оборудовании, доступном из интернета,** также, очевидно, останутся популярным вектором проникновения. Обновляйте вовремя свои фаерволы и VPN-SSL-шлюзы.

- **Уязвимости нулевого дня в компонентах ОС и популярных IT-продуктах** останутся относительно редким инструментом продвинутых APT, в то время как **неизвестные дыры безопасности в менее распространенных (и поэтому, вероятно, хуже оттестированных) продуктах** будут активно применяться и киберкриминалом.

- **Компрометация доменных регистраторов и certification authorities, атаки на поставщиков**

  Что касается этих «продвинутых» тактик — в минувшем году мы вновь увидели сценарии атак с компрометацией и доменных регистраторов (как минимум доступа к веб-панели управления доменной зоной жертвы), и certification authorities, а также новые сценарии атак на поставщиков. Подобные угрозы способны долгое время оставаться необнаруженными, гарантируя стабильность выполнения операций злоумышленникам. Несомненно, те из них, которым эти векторы по карману, не станут от них отказываться.

  Так что при планировании мер и средств защиты на будущий год не забывайте следить за безопасностью не только вашей собственной инфраструктуры, но и внешних сервисов, которыми пользуетесь. Выбирая поставщиков продуктов для ваших IT- и OT-систем, транслируйте на их продукты и на них самих ваши требования к киберзащите. А заводя деловых партнеров, помните об угрозах, которые могут представлять для вас недостатки их информационной безопасности.

Развитие успешных операций 2021 года

В 2021 году злоумышленники добились, безусловно, существенных успехов — один только список громких инцидентов, связанных с атаками вымогателей на промышленные предприятия, в этом году оказался, наверное, длиннее кумулятивного списка за все предыдущие годы. Кампаний APT, нацеленных в том числе на промышленные организации, также было исследовано немало.

Следует помнить, что многие достижения злоумышленников в этом году станут для них хорошим заделом на следующий год.

- **Украденные данные и скомпрометированные IT-системы**

  По данным нашей телеметрии и согласно результатам анализа найденной в darkweb информации, злоумышленникам в 2021 году удалось скомпрометировать по меньшей мере тысячи промышленных организаций по всему миру. Мы считаем, что общее их число многократно превышает количество организаций, которые в результате подверглись вымогательству или оказались в фокусе APT. Кому-то из числа скомпрометированных, возможно, повезет, и о них просто забудут. Но наверняка повезет не всем. Последствия компрометации в 2021 году, вероятно, настигнут некоторые промышленные компании уже в следующем, 2022 году.

- **Угрозы в технологической сети**

  Еще одно тревожное наблюдение: признаки компрометации многих организаций, к сожалению, были обнаружены нами и на компьютерах, имеющих прямое отношение к АСУ. Так что шифрованием IT-систем и кражей данных в офисной сети ущерб для кого-то может и не ограничиться.

- **«P» значит Persistent (упорство)**

  Как уже замечено выше, букву P в аббревиатуре APT стоит понимать не только как «длительное присутствие», но и как «настойчивость» или «упорство». Так что тем организациям, которые уже когда-то атаковали, следует быть настороже: очень вероятно (в случае некоторых APT можно даже сказать — наверняка), их атакуют еще — и, возможно, не раз.

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