KASPERSKY lab

Угрозы безопасности промышленных предприятий и IoT: прогноз на 2018 год

Kaspersky Lab ICS CERT

Ландшафт угроз в 2017 году

2017 год был одним из самых насыщенных в плане инцидентов, связанных с информационной безопасностью промышленных систем. Эксперты по безопасности обнаружили сотни новых уязвимостей, исследовали новые векторы атаки на АСУ ТП и технологические процессы, собрали и проанализировали статистику случайных заражений промышленных систем и обнаружили целевые атаки на промышленные предприятия (в частности, Shamoon 2.0/StoneDrill). Кроме того, впервые после Stuxnet был обнаружен и исследован вредоносный инструментарий, предназначенный для проведения атак на физические системы – CrashOverride/Industroyer. Некоторые специалисты стали относить его к категории кибероружия.

Однако наиболее значительной угрозой для промышленных систем в 2017 году стали атаки шифровальщиков-вымогателей. По данным Kaspersky Lab ICS CERT, в первой половине года промышленные информационные системы в 63-х странах мира подверглись множественным атакам с использованием программ-шифровальщиков, относящихся к 33 различным семействам. Судя по всему, разрушительные атаки программ-вымогателей WannaCry и ExPetr навсегда изменили отношение промышленных предприятий к проблеме защиты ключевых производственных систем.

Чего ожидать в 2018 году?

1. **Рост числа случайных заражений вредоносным ПО**

   За редкими исключениями киберпреступнники пока не нашли простых и надежных схем монетизации атак на промышленные информационные системы. В 2018 году продолжатся случайные заражения и инциденты в промышленных сетях, вызванные «обычным» вредоносным ПО, предназначенным для атак на традиционные мишени, такие как корпоративные «офисные» сети и компьютеры частных лиц. Вероятно, в будущем последствия таких заражений для индустриальных сред будут все более серьезными. Проблема регулярного обновления ПО в промышленных системах по образцу корпоративных сетей остается нерешенной, несмотря на многократные предупреждения экспертов по информационной безопасности.

2. **Увеличение риска целевых атак с применением программ-вымогателей**

   Атаки WannaCry и ExPetr показали как экспертам по безопасности, так и киберпреступникам, что технологические сети могут быть даже более уязвимыми для подобных атак, чем корпоративные, и также могут быть доступны из интернета. Более того, ущерб от активности вредоносного ПО в технологической сети может превышать вред, наносимый этим же ПО в корпоративной сети, а «тушить пожар» в промышленной сети гораздо труднее. Хуже всего, наверное, то, что, по опыту инцидентов стало понятно, насколько на промышленных предприятиях плохо организованы и неэффективны действия персонала в случае кибератаки на

технологическую инфраструктуру. Все эти факторы делают промышленные системы привлекательными мишенями для атак с применением программ-вымогателей.

3. Рост количества атак кибермошенников на промышленные предприятия

В 2016 - 2017 годах мы наблюдали проявление невиданного ранее интереса кибермошенников к промышленным компаниям и организациям. Об одной такой расследованной нами кампании (атаки типа «Business Email Compromise»), осуществляемой по всему миру преступниками из Нигерии, мы писали в наших отчётах ранее.
Удивительно, но факт: особенности бизнес-процессов промышленных предприятий и, соответственно, коммуникации продавцов и покупателей промышленных товаров и услуг, а также продавцов и поставщиков средств промышленного производства оказались очень уязвимыми к отработанным схемам атак кибермошенников. Судя по всему, промышленные компании стали интересной целью для преступников.

Этот неутешительный вывод подтверждают и наши новые находки: методы «нигерийцев» взяли на вооружение преступники и из других стран. Мы исследуем активность нескольких таких группировок, специализирующихся в атаках на промышленные организации.

Очевидно, что проблема не исчезнет сама собой – в ближайшее время нас ожидает рост количества подобных атак.

4. Увеличение числа инцидентов, связанных с промышленным кибершпионажем

Интерес киберпреступников к целевым атакам на промышленные компании с применением программ-вымогателей может стать локомотивом развития еще одного направления киберпреступной деятельности – кражи данных из промышленных информационных систем для подготовки и реализации целевых атак (в том числе с применением программ-вымогателей).

5. Появление вредоносного ПО, эксплуатирующего уязвимости в компонентах систем автоматизации

В уходящем 2017 году на черном рынке существенно вырос спрос на эксплойты нулевого дня для систем АСУ ТП. Это говорит о том, что преступники уже сейчас готовят целевые атаки на промышленные предприятия. Что, в целом, не удивительно – в течение последних пяти лет мы наблюдали множество предвестников такого развития событий:

- Рост количества целевых атак на ICS, в которых обычное вредоносное ПО используется для получения удалённого доступа к системам промышленной автоматизации, а сами вредоносные действия осуществляются вручную, при помощи скомпрометированных легитимных средств управления – HMI, инженерной среды и т.д.;

- Появление ICS-ориентированных модулей в составе платформ/фреймворков вредоносного ПО (таких как BlackEnegry);
- Появление специализированного ПО, автоматизирующего вредоносные воздействия на промышленные системы (пример CrashOverride);
- Рост интереса киберпреступников (даже средней и низкой квалификации) к промышленным компаниям;
- Непрерывное увеличение уровня автоматизации промышленных предприятий и, как следствие, рост количества ICS, так или иначе (необязательно напрямую) доступных из интернета.

При этом с бо́льшей вероятностью в первую очередь будут эксплуатироваться уязвимости в «общих» компонентах промышленных систем, разрабатываемых сторонними производителями.

В этом году мы уже видели примеры уязвимостей в продуктах сторонних производителей (hasplms), которые открывают возможности атак сразу на множество различных систем промышленной автоматизации. Вероятно, для реализации атак злоумышленники будут в первую очередь использовать как раз такие уязвимости.

6. Появление новых видов вредоносного ПО и вредоносных инструментов

Вероятно, появится новое вредоносное ПО, предназначенное для промышленных сетей и систем. Это ПО будет действовать скрытно, оставаясь в неактивном состоянии в корпоративных сетях, чтобы избежать обнаружения. Оно будет переходить в активный режим в технологической инфраструктуре, уровень защищенности которой значительно ниже. Возможно также появление программ-вымогателей, нацеленных на устройства полевого уровня АСУ ТП и физических систем (насосов, переключателей и т.п.).

7. Использование преступниками результатов анализа угроз, обнародованных исследователями безопасности

В 2017 году исследователи хорошо поработали: мы узнали о множестве новых векторов атак на промышленные системы и инфраструктуру, был проделан глубокий анализ обнаруженного вредоносного инструментария. Всё это, безусловно, полезно для защиты промышленных объектов. Но, возможно, в своем стремлении доказать необходимость защищать системы промышленной автоматизации исследователи ИБ несколько перестарались, детально расписывая обнаруженные векторы атак. Этой информацией вполне могут воспользоваться и преступники.

Например, хактивисты могут использовать опубликованные сведения об инструментах CrashOverride/Industroyer для организации DoS-атак на энергосистемы; преступники могут создать программы-вымогатели, предназначенные для проведения целевых атак или даже придумать новые схемы монетизации сбоев в электроснабжении. Концепт червя для ПЛК может вдохновить преступников на создание полнофункциональных вредоносных червей, распространяющихся с одного ПЛК на другой, а кто-то, возможно,

попытается создать вредоносное ПО с помощью одного из стандартных языков программирования для ПЛК. Возможно даже, что кто-то из злоумышленников разработает вредоносное ПО для ПЛК, работающее на низком уровне, используя подход, продемонстрированный исследователями ИБ. Оба последних подхода, вероятно, могут создать серьёзную проблему для разработчиков существующих защитных решений.

8. Новые сегменты подпольного рынка, обслуживающие атаки на промышленные системы

Внимание злоумышленников к промышленным системам управления неизбежно приведёт к появлению новых сегментов киберкриминального рынка, ориентированных на кражу сведений о конфигурации систем АСУ ТП и данных для доступа к этим системам. Кроме того, возможно, на рынке появятся предложения ботнетов с «промышленными» узлами.

Подготовка и реализация сложных кибератак на физические объекты и системы требует экспертных знаний об АСУ ТП и о специфике отраслей, в которых они применяются. Спрос на такие дефицитные знания, вероятно, приведет к развитию таких услуг как «вредоносное ПО как сервис», «разработка векторов атаки как сервис», «организация атак на заказ» и т.д., ориентированных именно на атаки на промышленные предприятия.

На примере упомянутых ранее мошеннических атак типа «Business Email Compromise» мы уже сейчас видим, что появилась специализация преступников по различным отраслям промышленности – металлургия, нефтехимия и так далее. Даже для реализации таких относительно несложных схем атак на промышленные организации преступникам требуются специфические знания из соответствующей отрасли – как минимум, чтобы «общаться» с их потенциальными жертвами на одном языке.

9. Изменения в нормативной базе

В 2018 году вступают в силу многие новые инициативы регуляторов, касающиеся промышленных систем автоматизации – как в России, так и в некоторых других странах. Помимо всего прочего это заставит компании, владеющие критически важными объектами инфраструктуры и промышленными объектами, уделять больше внимания оценке их киберзащищенности. Можно ожидать, что результатом станет обнаружение новых уязвимостей промышленных систем. Возможно, мы также узнаем об инцидентах на промышленных предприятиях и ранее неизвестных атаках.

Однако некоторые из действий регуляторов, направленные на ограничение доступа иностранных компаний и специалистов к промышленным предприятиям и объектам критической инфраструктуры страны, будут иметь негативные последствия с точки зрения информационной безопасности. Как минимум в кратковременной (порядка нескольких лет) перспективе, пока в стране не появится необходимое количество своих собственных экспертов достаточной квалификации и отработанные технологии. На этот период времени преступники получат значительное преимущество.

Да и в дальнесрочной перспективе, вероятно, подобные решения не дадут хороших результатов. Многолетний опыт «Лаборатории Касперского» показывает, что бороться с глобальной преступностью локально – крайне малоэффективно.

10. Формирование рынка страхования промышленных предприятий от кибер-рисков и рост инвестиций в этот вид страхования

Страхование от рисков, связанных с киберугрозами, становится неотъемлемой частью системы управления рисками на промышленных предприятиях. До недавнего времени риски, связанные с инцидентами кибербезопасности, исключались из контрактов страхования – фактически, страховые компании ставили киберинциденты в один ряд с террористическими атаками. Однако ситуация меняется, и появляются новые инициативы – как со стороны компаний, специализирующихся на кибербезопасности, так и со стороны основных игроков страхового бизнеса. Как следствие, в 2018 году вырастет число проводимых аудитов/оценок защищенности промышленных систем автоматизации и число зарегистрированных и исследованных инцидентов кибербезопасности.

11. Использование методов кибератак для совершения традиционных преступлений на промышленных предприятиях

Как уже отмечалось выше, схемы монетизации атак на системы управления технологическим процессом промышленных предприятий сложны и малодоступны для атак киберпреступников «извне» предприятия или отрасли. Очевидно, что заработать деньги на украденной цистерне нефтепродуктов, сидя за компьютером и не используя методов преступников обычных (не «кибер-»), почти невозможно. Однако, это не значит, что «обычные» преступники не используют «кибер-» методов для совершения преступлений. Наш опыт показывает, что значительное количество таких преступлений на промышленных предприятиях совершается с участием людей «изнутри» отрасли – они-то уж знают, что и как делать с неучтённой цистерной горючего. Увеличение степени автоматизации промышленных предприятий делает не только возможным, но и неизбежным применение методов кибератак для осуществления такого рода преступлений. Несомненно, количество таких случаев будет неуклонно расти в ближайшие годы.

Internet of Things (IoT)

Когда дело касается информационной безопасности, и для организаций, и для частных пользователей IoT-устройства находятся на периферии их внимания. Они как-то всегда «не основные», «вспомогательные», пусть и «удобные», и «полезные», но «не обязательные» и потому «менее важные». Уже сейчас IoT-устройств очень много, и большинство из них – слишком специфичны, чтобы защищать их традиционными мерами: своевременно накатывать патчи, устанавливать и настраивать антивирусы, следить за актуальным состоянием антивирусных баз и т.д.

Производители спешат вывести на рынок всё новые и новые продукты и, в погоне за новыми клиентами и в стремлении опередить конкурентов, заботятся лишь об их функциональности.

Сложившейся ситуацией с информационной безопасностью IoT уже воспользовались кибепреступники, набившие руку на атаках традиционных IT-систем. Несомненно, количество атак на IoT будет расти.

1. **Появление новых ботнетов из IoT устройств для DDoS атак на традиционные IT-системы**

   Самым очевидным применением зараженных IoT-устройств стала возможность организации масштабных DDoS-атак на интернет-сервисы и телеком.

   Впервые масштаб этой угрозы мир осознал в 2016 году, когда создатели ботнета Mirai продемонстрировали, что безобидные на первый взгляд устройства могут представлять столь существенную угрозу. Более полумиллиона «умных» видеокамер были использованы для проведения серии масштабных DDoS-атак.

   В этом году мы также могли наблюдать появление нескольких крупных зомби-сетей, состоящих из IoT гаджетов.

   Несомненно, тема ботнетов из IoT-устройств интересна как сообществу специалистов, так и широкой публике. Большое количество исследований, статей, докладов на конференциях и публикаций в СМИ привлекает внимание злоумышленников. Например, в апреле 2017 года была опубликована статья, согласно которой более 1000 моделей IP-камер 354 разных производителей содержат опасную уязвимость во встроенном веб-сервере. Результат не заставил себя долго ждать: уже в мае был обнаружен новый IoT-ботнет из уязвимых камер, названный исследователями Persirai.

   Совсем недавно, в октябре 2017 года, была обнаружена ещё одна крупная сеть заражённых IP-видеокамер. Новый ботнет получил имя Reaper. Как сообщается, вредоносная программа использует для заражения устройств сразу несколько уязвимостей камер различных фирм. По оценкам экспертов число уязвимых устройств может доходить до двух миллионов. Если Reaper удастся добраться хотя-бы до части из них, он станет очень серьёзным оружием в руках киберпреступников.

С большой вероятностью в 2018 году мы увидим заметное увеличение числа IoT- зомби-сетей. Также можно ожидать, что злоумышленники перестанут фокусироваться лишь на IP-камерах и обратят свой взор и на другие типы «умных» устройств.

2. **Использование скомпрометированных IoT-устройств в качестве точки входа внутрь периметра IT- и OT-сетей**

Плачевное состояние дел с информационной безопасностью IoT открыло киберпреступникам ещё одну возможность: IoT-устройства можно использовать, чтобы попасть внутрь «хорошо защищённой» сети организации или частного лица. В процессе проведения исследований ИБ и тестов на проникновение мы нередко обнаруживаем подобного рода уязвимости и указываем нашим клиентам на соответствующие риски. По некоторым данным, системы видеонаблюдения и другие IoT-системы уже были использованы в целевых атаках на промышленные и инфраструктурные объекты.

С высокой вероятностью этот вектор будет в будущем использован злоумышленниками для организации целевых атак, и, возможно, даже для осуществления массовых случайных заражений IT- и OT-систем.

3. **IOT ransomware**

Развитие атак на IoT сейчас во многом напоминает историю ранних атак на IT – «детские» уязвимости, относительно несложные векторы атак. Очевидно, в ближайшее время можно ожидать появления такого неприятного явления, как вымогательское ПО, нацеленное на IoT-системы – компоненты умных домов, элементы инфраструктуры умного города, публичного транспорта и так далее. Учитывая опыт «классических» IT-систем, атаки с использованием вредоносных программ-вымогателей могут быть весьма прибыльными для киберпреступников. Первые примеры таких атак нам уже пришлось, к сожалению, наблюдать.

4. **Атаки через общие технологии**

Все многообразие IoT решений зачастую построено на множестве общих технологий: используется процессорная архитектура ARM и OS семейства Linux, различное прикладное ПО - IoT-брокеры (например, MQTT), OPC UA для IIoT решений и так далее. Уязвимости в подобных «общих» компонентах представляют огромную угрозу – они позволяют организовывать масштабные кибератаки и наверняка будут эксплуатироваться злоумышленниками в ближайшее время.

5. **Проникновение технологий Интернета вещей в сферу традиционной преступности**

Не секрет, что такие системы как Shodan или Censys, которые помогают искать доступные через интернет сервисы, включая компоненты IoT, могут быть целенаправленно использованы для поиска уязвимых IoT-устройств, доступных из интернета. Этим, к примеру, воспользовались создатели сервиса Insecam для вывода в общий доступ изображений с незащищенных камер видеонаблюдения по всему

миру. Целью сервиса является повышение осведомленности, поэтому его создатели не публикуют информации, которая может способствовать точной идентификации расположения камеры, однако дают понять, что это возможно.

Данные с видеокамер, устройств «умного дома» и «умного города» могут быть использованы злоумышленниками для планирования и координации традиционных (не кибер-) преступлений (о таких возможностях эксперт «Лаборатории Касперского» писал еще два года назад).

Вероятно, следующим шагом киберпреступников после создания ботнетов для осуществления DDoS-атак станет создание «платформ» сбора информации и управления IoT-устройствами – как дополнительного инструмента для преступников «традиционных».

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab 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 Lab ICS CERT **Ics-cert@kaspersky.com**