ICS CERT

Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2016

Kaspersky Lab ICS CERT

Содержание

В течение многих лет специалисты «Лаборатории Касперского» обнаруживают и исследуют киберугрозы, направленные на различные информационные системы – коммерческих и государственных организаций, банков, телеком-операторов, промышленных предприятий и частных лиц. Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) начинает серию регулярных публикаций наших исследований ландшафта угроз промышленных предприятий.

Основная цель публикаций – информационная поддержка глобальных и локальных команд реагирования на инциденты, специалистов по информационной безопасности предприятий и исследователей в области защищённости промышленных объектов.

Проблемы информационной безопасности АСУ ТП

Проблемы информационной безопасности сетей промышленных предприятий обусловлены спецификой их развития. На протяжении нескольких десятилетий эволюция систем автоматизации промышленных предприятий шла параллельным курсом с эволюцией IT-систем. Необходимость обеспечения непрерывности поддерживаемых процессов привела к тому, что технологии, применяемые на нижних уровнях, были направленны на решение задач, не свойственных для IT. Они не могли меняться так же быстро, как в IT. С течением времени для эффективного управления этими процессами предприятия внедряли построенные на современных IT-технологиях информационные системы верхнего уровня. Для интеграции этих систем стали появляться не предусмотренные на ранних этапах каналы информационного воздействия на нижние уровни вычислительной сети АСУ ТП, которые несут значительные риски сбоя процессов и нарушения функционирования оборудования на этих уровнях. В течение последних лет мы наблюдаем, как практически во всех индустриях весьма развитые цифровые технологии стали повсеместно внедряться и на нижнем (полевом) уровне как закономерный этап решения тех же самых задач повышения эффективности управления производственными процессами.

На сегодняшний день, несмотря на трудность частого обновления и замены оборудования и ПО, на очень многих предприятиях и средний, и нижний уровень иерархии систем промышленной автоматизации задействуют вполне современные технологии информационного обмена и управления процессами. Так, оборудование включает:

- стационарные и мобильные компьютеры операторов и инженеров АСУ ТП,
- серверы, в том числе серверы виртуализации, на которых установлено ПО мониторинга и управления технологическим процессом,
- промышленные сетевые маршрутизаторы,
- шлюзы данных,
- контроллеры,
- полевые промышленные устройства различной степени «интеллектуальности» с цифровым (характерно для более современных устройств) либо аналоговым интерфейсом коммуникации.

Как следствие, существенно усугубляются проблемы информационной безопасности в отношении сетей промышленных предприятий:

1. Растущая сложность оборудования и ПО ведет к высокой вероятности ошибок и уязвимостей, которые могут быть использованы злоумышленниками.
2. Вопросы технологической совместимости, высокой доступности и непрерывности производства требуют пересмотра мер безопасности, применяемых в отношении аналогичных решений в чистом информационном окружении. Часто это ведет к значительному снижению уровня защищенности.
3. Меры обеспечения функциональной безопасности, реализованные для систем управления технологическими процессами, как правило, не рассчитаны на намеренное нарушение удаленным нарушителем или злоупотребление внутренним пользователем

возможностями доступа. Это может привести к пагубным последствиям для процесса, оборудования или даже жизни и здоровья людей и безопасности окружающей среды.

4. Изоляция технологической сети от любых внешних систем, считавшаяся незыблемым требованием ещё 10-15 лет назад, больше не может рассматриваться как адекватная защитная мера. Она стала невыгодной экономически и крайне трудно реализуемой на практике.

Особенности современных технологических сетей

Организация сопряжения сегментов сети

В настоящее время **сопряжение технологической сети с корпоративной сетью необходимо как для управления производством, так и для администрирования промышленных сетей и систем.**

Хотя соединение между корпоративной и технологической сетями становится необходимостью, реализовано оно иногда без учета многих рисков ИБ.

Организация безопасного доступа между корпоративной и технологической сетями обычно сводится к одному из следующих решений:

- ограничение доступа по IP на межсетевом экране между технологической и корпоративной сетью («нечестный» DMZ);
- использование VPN-туннелей между компьютерами в технологической и корпоративной сетях;
- использование терминальных (jump) серверов с локальной или доменной авторизацией;
- использование авторизации в корпоративном домене (на сервере ActiveDirectory) для определения уровня доступа пользователя к объектам в технологической сети.

Как показывает практика, на сегодняшний день ни одно из этих решений по отдельности не может обеспечить необходимый уровень защиты. Оптимальный уровень защиты технологической сети должен позволить не только защитить сеть от внешних угроз, но и безопасно выполнять удаленное управление промышленных систем. Такой уровень может быть обеспечен лишь комбинацией из нескольких решений.

Доступ к внешним системам и сетям

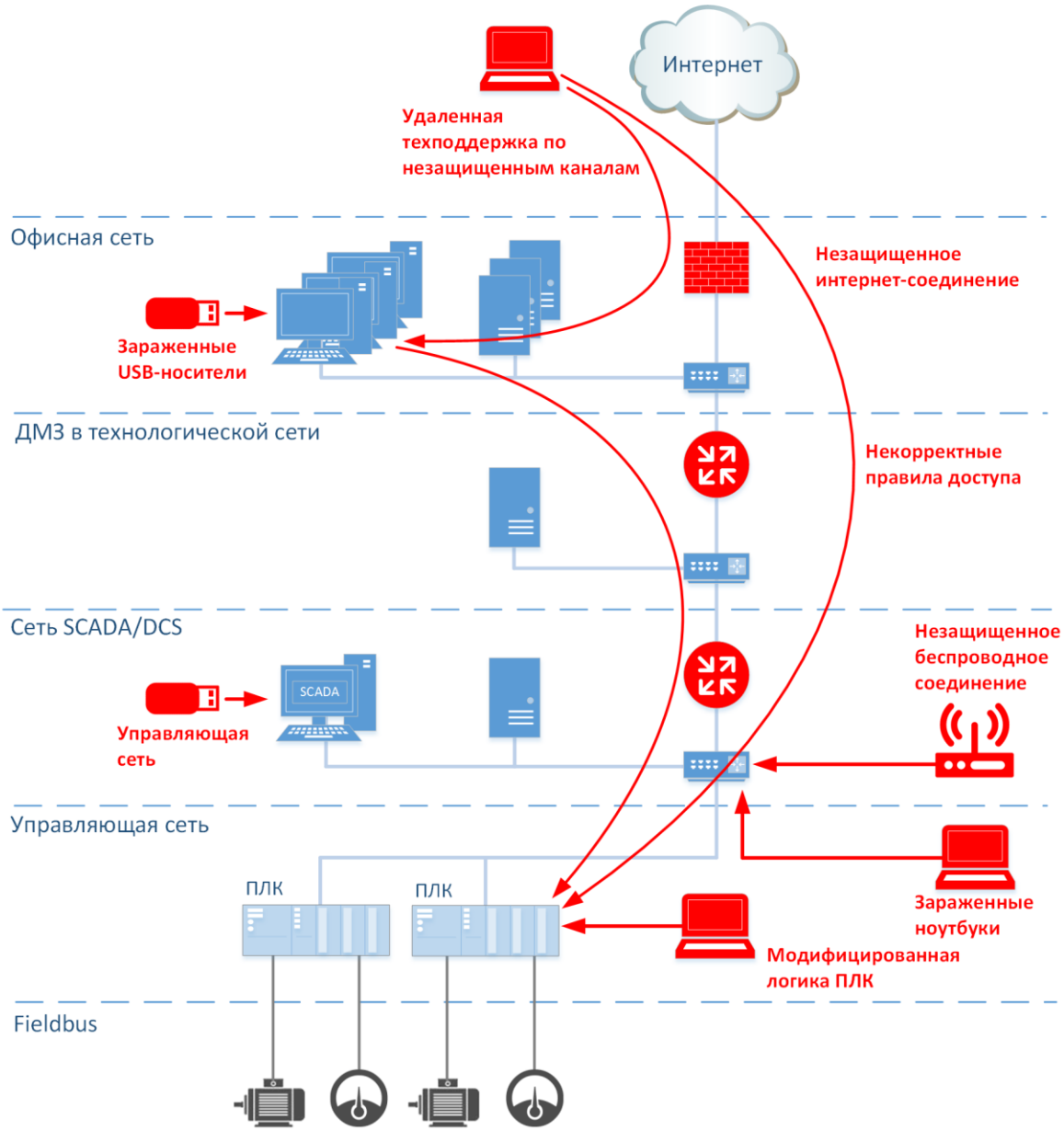
Доступ к интернету из технологической сети может быть не только результатом слабых ограничений, но и вынужденной необходимостью. Физически отдельные части АСУ ТП могут располагаться на территориях, не обжитых людьми. Их обслуживание производится удаленно через мобильные интернет-каналы. Ремонтная бригада выезжает туда только во время плановых осмотров и в случае возникновения аварийной ситуации.

Сопровождение и техническая поддержка систем промышленной автоматизации часто выполняются сотрудниками организаций-подрядчиков. Работы обычно проводятся с использованием удаленного доступа из сети подрядчика в промышленную сеть заказчика. В зависимости от конкретных обстоятельств сотрудник организации-подрядчика, находясь вне офиса, может подключаться к технологической сети заказчика (напрямую или через свою корпоративную сеть), используя любое доступное подключение.

Подключающийся извне технологической сети пользователь (подрядчик, разработчик, администратор) часто имеет высокие права доступа на уровне локальной системы или на уровне всей сети. Если разделение на уровни организовано в виде плоской сети или нескольких виртуальных подсетей (VLAN) с общим ядром сети и без достаточных разграничений доступа, то такой пользователь может случайно или намеренно заразить компьютеры в технологической сети.

На практике иерархическая структура технологической сети организована в виде нескольких VLAN, доступ между которыми не всегда ограничен производственной необходимостью.

Изменение ландшафта угроз



Векторы кибератак

В современных промышленных компаниях используются новые технологии, которые повышают прозрачность и эффективность процессов на уровне управления предприятием, а также обеспечивают гибкость и отказоустойчивость выполняемых функций на средних и нижних уровнях промышленной автоматизации. Это требует сопряженности систем и большей свободы коммуникаций. Вместе с тем, администрирование систем, в том числе технологических компонентов, возлагается на IT-департамент компании. В результате технологическая сеть все больше становится похожей на корпоративную – и по сценариям использования, и по применяемым технологиям.

Закономерно, что и ландшафт угроз промышленных информационных систем становится похожим на ландшафт угроз корпоративных систем. Свидетельства этому мы наблюдаем в наших исследованиях. Далее приведём результаты некоторых наших исследований, полученные в течение второго полугодия 2016 года – с момента создания Kaspersky Lab ICS CERT.

Уязвимости в программном обеспечении АСУ ТП

Относительно независимое (от «традиционного» IT) развитие систем промышленной автоматизации привело к тому, что производители индустриальных решений годами разрабатывали программное и аппаратное обеспечение АСУ ТП практически без учета требований информационной безопасности. При этом переход к разработке более безопасных решений — часто долгий и болезненный процесс, осложнённый требованиями сертификации и контроля производства.

Эксплуатация уязвимостей в программном обеспечении в технологических сетях предприятий, особенно объектов критических инфраструктур, может привести к катастрофическим последствиям. Поиск и устранение этих уязвимостей, помимо разработки более совершенных промышленных решений и специализированных средств защиты, является первоочередной задачей специалистов по безопасности.

К наиболее опасным относятся уязвимости, допускающие:

- удаленное выполнение произвольного кода,
- удаленный вывод из строя ПО или оборудования, отказ технологического процесса,
- атаки на криптографию,
- атаки на промышленные сетевые протоколы,
- удаленный несанкционированный доступ к информации,
- манипуляции с учетными данными удаленных пользователей.

Кроме этого, следует выделить распространенный класс уязвимостей, связанных с наличием статически заданных в коде учетных данных пользователей.

Количество обнаруживаемых с каждым годом уязвимостей растет в сравнении с количеством закрытых проблем. К примеру, по данным US ICS-CERT, в 2016 году этой организацией было зарегистрировано 187 уведомлений об уязвимостях. За этот же период ими было опубликовано 139 сообщений о закрытых уязвимостях.

Уязвимости, обнаруженные «Лабораторией Касперского»

В 2016 году «Лаборатория Касперского» провела оценку актуального состояния ИБ компонентов АСУ ТП различных производителей. По результатам исследований было выявлено 75 уязвимостей в компонентах АСУ ТП.

На рисунке ниже представлено распределение найденных уязвимостей по группам в соответствии с теми возможностями, которые дает использование уязвимости злоумышленникам.

Распределение уязвимостей, найденных «Лабораторией Касперского» в 2016 году, по возможностям использования

Краткое описание для каждой группы уязвимостей:

- RCE – (сокращение от английского remote code execution) — уязвимости, позволяющие удаленно выполнить произвольный код в целевой системе.
- DOS – (сокращение от английского denial of service) – уязвимости, позволяющие удаленно вызвать отказ в обслуживании. В случае успешной атаки программное или аппаратное обеспечение перестает отвечать на легитимные запросы. Требуется перезапуск программы, операционной системы или устройства.
- Инъекции – группа, в которой объединены уязвимости, позволяющие осуществлять SQL-инъекции и XML-инъекции. Такие уязвимости позволяют не санкционированно исполнять запросы и считывать данные на целевых системах. При определенных условиях данные уязвимости дают также возможность провести атаку типа RCE.
- Манипуляции с файлами – группа уязвимостей, позволяющих осуществлять удаленные действия с файлами (создание, удаление, перемещение). При определенных условиях эти уязвимости также дают возможность провести атаку типа RCE.
- Манипуляции с аккаунтами – группа уязвимостей, позволяющих провести атаку на легитимные данные пользователей (создать нового пользователя, удалить или заблокировать существующего пользователя).

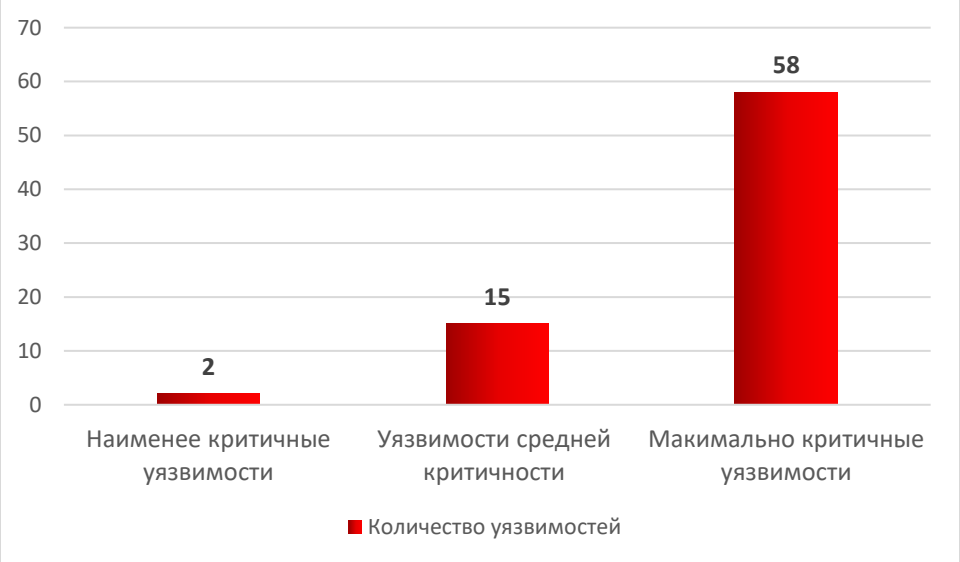
Уровень опасности обнаруженных уязвимостей

Мы рассмотрели найденные уязвимости и по уровню опасности для уязвимых систем. За основу мы взяли метрику CVSS v3.0.

CVSS (Common Vulnerability Scoring System) – это открытый стандарт, разработанный для оценки уровня опасности уязвимостей в ПО. CVSS присваивает уязвимости вес, который может составлять от 0 (наименее опасные) до 10 (наиболее опасные). Вес уязвимости рассчитывается на основании формулы, которая зависит от нескольких показателей, – в том числе учитывается легкость эксплуатации уязвимости и возможности, которые эксплуатация уязвимости дает злоумышленникам. Третья версия стандарта CVSS позволяет лучше оценивать уязвимости киберфизических систем, к которым относятся сети промышленных предприятий и их компоненты.

Следует отметить, что, хотя классификация уязвимостей, принятая для IT, действительна и для промышленных компонентов, риски, связанные с одними и теми же уязвимостями, могут отличаться для систем в корпоративной и технологической сети. CVSS 3.0 предлагает качественную градацию уровней критичности (всего 5), применимую в основном к уязвимостям в традиционном IT-окружении. Мы отказываемся от этой градации в применении к промышленным системам и рассматриваем все уязвимости в компонентах АСУ ТП как критичные, в соответствии со следующими уровнями:

- наименее критичные: вес уязвимости не более 5.0 по CVSS v3.0;
- средней критичности: вес уязвимости от 5.1 до 6.9 включительно по CVSS v3.0;
- наиболее критичные: вес уязвимости 7.0 и более по CVSS v3.0.



Распределение уязвимостей, найденных «Лабораторией Касперского» в 2016 году, по весовым коэффициентам

Существует множество легальных компаний, предлагающих любому желающему купить набор готовых Proof-of-Concept образцов кода для эксплуатации уязвимостей (без вредоносного функционала) в различном промышленном ПО. Кроме этого, можно провести исследование конкретного промышленного ПО на заказ.

Мы рассматриваем такую практику как недопустимую – велика опасность, что код попадет не в те руки. «Лаборатория Касперского» придерживается принципа ответственного раскрытия (responsible disclosure) информации о найденных уязвимостях, несмотря на не вполне ответственное отношение некоторых производителей ПО к закрытию этих уязвимостей.

Проблемы закрытия уязвимостей

Из 75 обнаруженных в 2016 году Kaspersky Lab уязвимостей к середине марта 2017 года производителями промышленного ПО было закрыто 30. Одну уязвимость (манипуляции с аккаунтами) производитель отказался закрывать, мотивируя это тем, что данный функционал, по мнению представителей компании, не является уязвимостью.

Наше взаимодействие с некоторыми производителями промышленных программ и оборудования показывает, что для устранения критических уязвимостей иногда требуется более полутора лет. Систематическая работа с уязвимостями в цикле разработки ПО пока не отлажена, в частности:

- приоритеты исправления выявленных уязвимостей в соответствии с их критичностью отсутствуют;
- обновления безопасности для уже используемого ПО не выпускаются, вместо этого производитель предпочитает учесть информацию о них в следующем релизе этого ПО;
- уведомления об уязвимостях не осуществляются, например, под предлогом того, что уязвимые решения используются «ограниченным числом» предприятий.

Мы прикладываем все усилия для того, чтобы производители промышленного ПО и аппаратного обеспечения устраняли уязвимости в кратчайшие сроки.

Другая проблема, не связанная напрямую с производителями промышленных компонентов, – обновление и установка исправлений безопасности ПО на предприятиях. Потери от простоя оборудования на время обновления ПО могут быть существенными, даже в сравнении с рисками, которые несут уязвимости. До установки обновлений они должны быть протестированы на совместимость с уже существующей инфраструктурой. Иногда тестирование и обновление происходит во время планового останова системы, но это, скорее, исключение, нежели правило.

Это, вкупе с общей неосведомленностью об уязвимостях, приводит к тому, что даже существующие обновления крайне редко устанавливаются вовремя. Так, команда Kaspersky Lab ICS CERT в 2016 году провела анализ существующих и публично известных уязвимостей, найденных в решениях компании Rockwell Automation в 2014 – 2016 годах. Согласно результатам исследования, у пользователей «Лаборатории Касперского» доля ПО данного производителя с незакрытыми уязвимостями может составлять от 17 до 93%. (Данные по распространённым продуктам других наиболее крупных вендоров будут опубликованы в течение 2017 года.)

На основании наших исследований и проводимых аудитов ИБ АСУ ТП мы полагаем, что процесс установки критических обновлений для владельцев АСУ ТП промышленных объектов либо слишком трудоемкий, либо не является приоритетной задачей в общем цикле жизнедеятельности системы. В результате на многих предприятиях критические обновления на различные компоненты промышленных систем не устанавливаются годами, что делает эти предприятия уязвимыми в случае кибератак злоумышленников.

Однако не все так печально. Производители с каждым годом всё более ответственно относятся к закрытию уязвимостей, появляются новые средства защиты АСУ ТП промышленных объектов,

которые включают в себя в том числе и функционал детектирования эксплуатации различных уязвимостей. Многие владельцы АСУ ТП уже начали процесс перехода своих систем на более защищённые архитектуры и решения. Теперь уже при разработке или модернизации АСУ ТП закладываются требования по информационной безопасности всей системы, что говорит о более зрелом и ответственном подходе к их проектированию и развитию.

Статистика угроз

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их анонимную передачу.

Процент атакованных компьютеров

В среднем в течение второго полугодия 2016 года продуктами «Лаборатории Касперского» во всем мире были предотвращены попытки атак на **39,2%** защищаемых нами компьютеров, которые Kaspersky Lab ICS CERT относит к технологической инфраструктуре промышленных предприятий. В России этот показатель составил **42,4**%.

В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

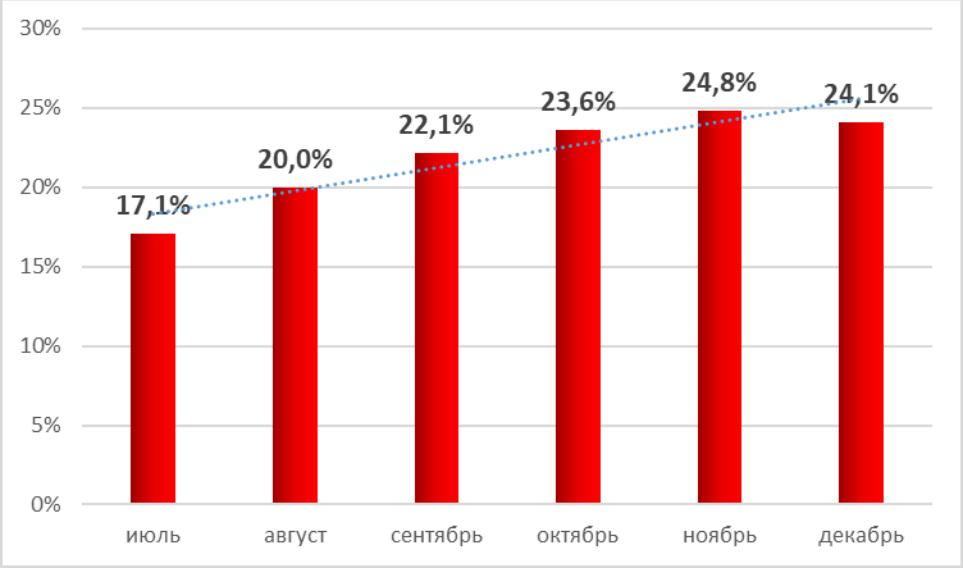
- серверы управления и сбора данных (SCADA),
- серверы хранения данных (Historian),
- шлюзы данных (OPC),
- стационарные рабочие станции инженеров и операторов,
- мобильные рабочие станции инженеров и операторов,
- Human Machine Interface (HMI).

А также компьютеры сотрудников подрядных организаций, компьютеры администраторов технологических сетей и разработчиков ПО для систем промышленной автоматизации.

Отметим, что процент атакованных промышленных компьютеров меньше, чем аналогичный показатель по корпоративным компьютерам в целом.

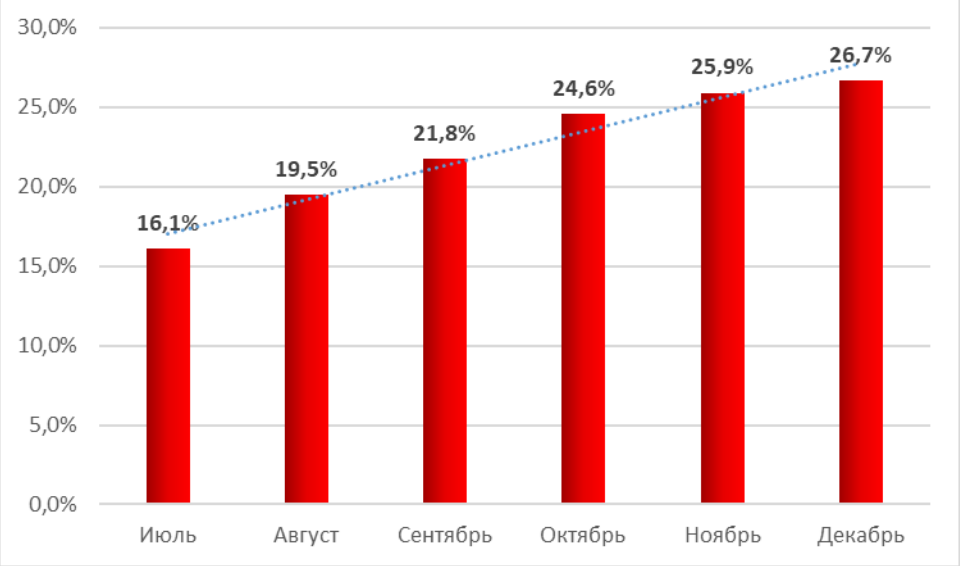
Процент атакованных промышленных компьютеров и атакованных корпоративных компьютеров (второе полугодие 2016)

Ежемесячно в среднем каждый пятый (20,1%) промышленный компьютер подвергается атакам вредоносного ПО.



Процент атакованных промышленных компьютеров по месяцам в мире (второе полугодие 2016)

Из месяца в месяц процент атакованных промышленных компьютеров растет. В России мы наблюдали схожую динамику:



Процент атакованных промышленных компьютеров по месяцам в России

Источники заражения промышленных систем

Источники угроз, заблокированных на промышленных компьютерах (второе полугодие 2016)

По нашим данным, во втором полугодии 2016 года загрузка вредоносного ПО из интернета и доступ к известным вредоносным и фишинговым веб-ресурсам были заблокированы на 22% промышленных компьютеров. То есть в этот период времени каждый пятый промышленный компьютер хотя бы раз столкнулся с риском заражения через интернет. В России этот показатель еще выше и достигает 27,9%.

В отличие от офисных корпоративных сетей, имеющих стабильное подключение к интернету, периодичность выхода в интернет промышленных компьютеров может варьироваться. Некоторые

компьютеры в нашей выборке (около 50%) регулярно или постоянно подключаются к интернету. Остальные выходят в интернет не чаще раза в месяц. Соответственно, риск заражения у таких машин меньше – из них с угрозами в интернете в течение второго полугодия 2016 года столкнулись только 6%. Отметим, что этот показатель меньше, чем у корпоративных пользователей в целом (18,2%).

Следует отметить, что ограничения доступа в интернет у компьютеров в технологической сети и компьютеров, составляющих инфраструктуру технологической сети, могут значительно отличаться. В большинстве случаев серверы АСУ ТП и стационарные компьютеры инженеров и операторов не имеют постоянного прямого выхода в интернет, по всей видимости, из-за ограничений технологической сети. Доступ в интернет может быть открыт на время технологического обслуживания.

С другой стороны, компьютеры системных/сетевых администраторов, разработчиков и интеграторов систем промышленной автоматизации, а также компьютеры подрядчиков, подключающиеся к технологической сети напрямую или удаленно (например, с целью мониторинга состояния и оказания технической поддержки), не привязаны только к одной промышленной сети с присущими ей ограничениями и могут свободно подключаться к интернету. На наш взгляд, эти компьютеры входят в группу наибольшего риска, о чём свидетельствует множество инцидентов, связанных с атаками (целевыми или случайными) на промышленные предприятия при посредничестве третьей стороны, которые произошли за последние годы (см., например, здесь и здесь).

На практике ограничения и специфика сети не всегда могут оградить промышленные компьютеры и их пользователей от внешних сетей и систем. Нередко компьютеры из сети с ограниченным доступом подключаются к интернету через сети мобильных операторов с помощью мобильных телефонов, USB модемов и/или Wi-Fi роутеров с поддержкой 3G/LTE.

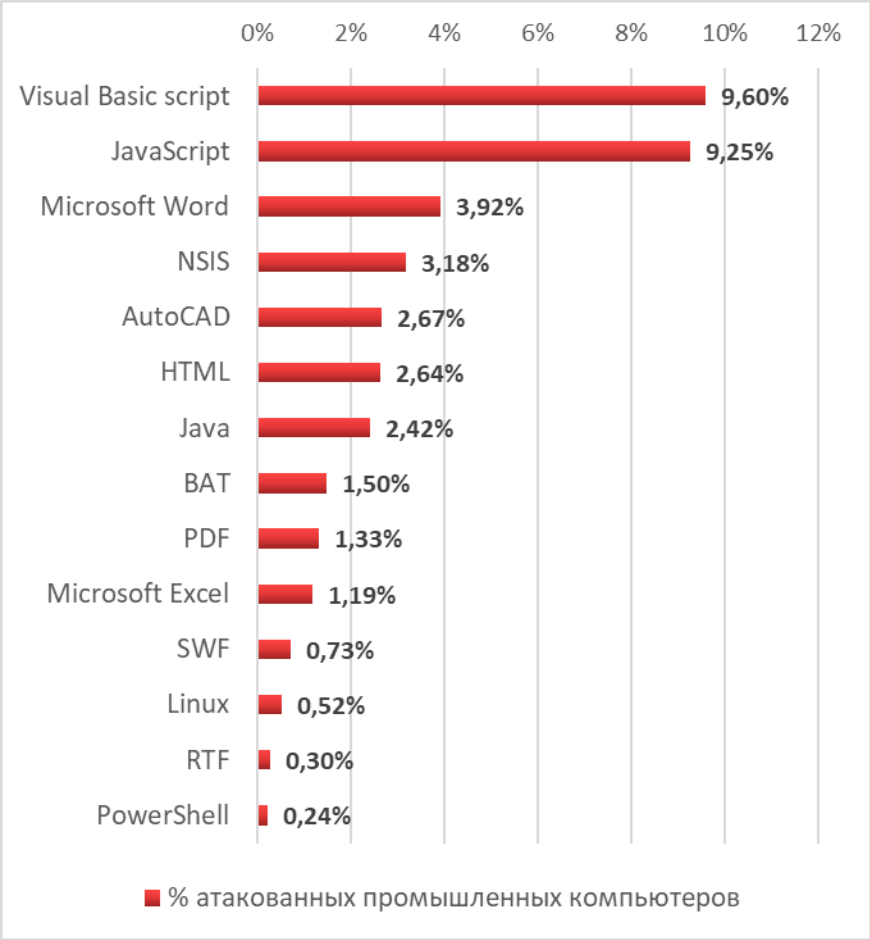
Примечательно, что на 0,1% промышленных компьютеров вредоносное ПО было обнаружено в локальных папках облачных файловых хранилищ. Такие папки автоматически синхронизируются с облачным хранилищем при подключении компьютера к интернету. И при заражении хранилища с какого-либо компьютера, имеющего к нему доступ (например, домашнего компьютера пользователя), зараженные файлы будут автоматически доставлены на все подключенные к хранилищу устройства.

Второе место в качестве источника заражения промышленных сетей занимают съемные носители информации. Во втором полугодии 2016 года на 10,9% промышленных компьютеров при подключении съемных носителей информации было обнаружено вредоносное ПО. В России этот показатель составил 6%.

Важно отметить, что в рейтинге вредоносных программ, детектируемых на промышленных компьютерах, значительный процент атакованных промышленных компьютеров связан с попытками заражений программами классов Virus, Worm и Net-Worm (см. ниже). Вредоносные программы, относящиеся к этим классам, использует съемные носители и сетевые папки в качестве основных путей распространения. Поскольку зловреды часто маскируются под файловое окружение на съемном носителе, заражая существующие файлы или используя схожие имена, пользователь может долгое время не знать, что файлы заражены. (Такой же подход используется и

при распространении вредоносного ПО через сетевые папки.) Пользователь может создавать защищенные архивы данных, в которые попадают эти файлы. Кроме того, зараженные файлы могут попадать в резервные копии файловой системы в процессе их создания операционной системой.

Вредоносные почтовые вложения и вредоносные скрипты, встраиваемые в тело электронных писем, были заблокированы на 8,1% промышленных компьютеров. В большинстве случаев злоумышленники используют обычный фишинг (письма, как правило, подделанные под сообщения от банков, служб доставки и т.п.) для привлечения внимания пользователя и маскировки вредоносных файлов. Чаще всего в таких вредоносных письмах зловреды распространяются в формате офисных документов, – таких как MS Office и PDF, – начиненных вредоносными скриптам и/или эксплойтами для уязвимостей в соответствующих приложениях.



Платформы, используемые вредоносным ПО для маскировки и обхода детектирования (второе полугодие 2016)

Отметим, что для обхода детектирования, маскировки вредоносного ПО и сокрытия следов заражения злоумышленники также прибегают к использованию небольших загрузчиков, написанных на JavaScript, Visual Basic Script и Powershell, и запускаемых в виде параметров командной строки для соответствующих интерпретаторов.

География атак на промышленные системы

Top 15 стран по проценту атакованных промышленных компьютеров:

	Страна*	% атакованных систем
1	Вьетнам	66,1
2	Алжир	65,6
3	Марокко	60,4
4	Тунис	60,2
5	Индонезия	55,7
6	Бангладеш	54,2
7	Казахстан	54,1
8	Иран	53,9
9	Китай	53,3
10	Перу	53,1
11	Чили	52,8
12	Индия	52,5
13	Египет	51,6
14	Мексика	49,6
15	Турция	46,2

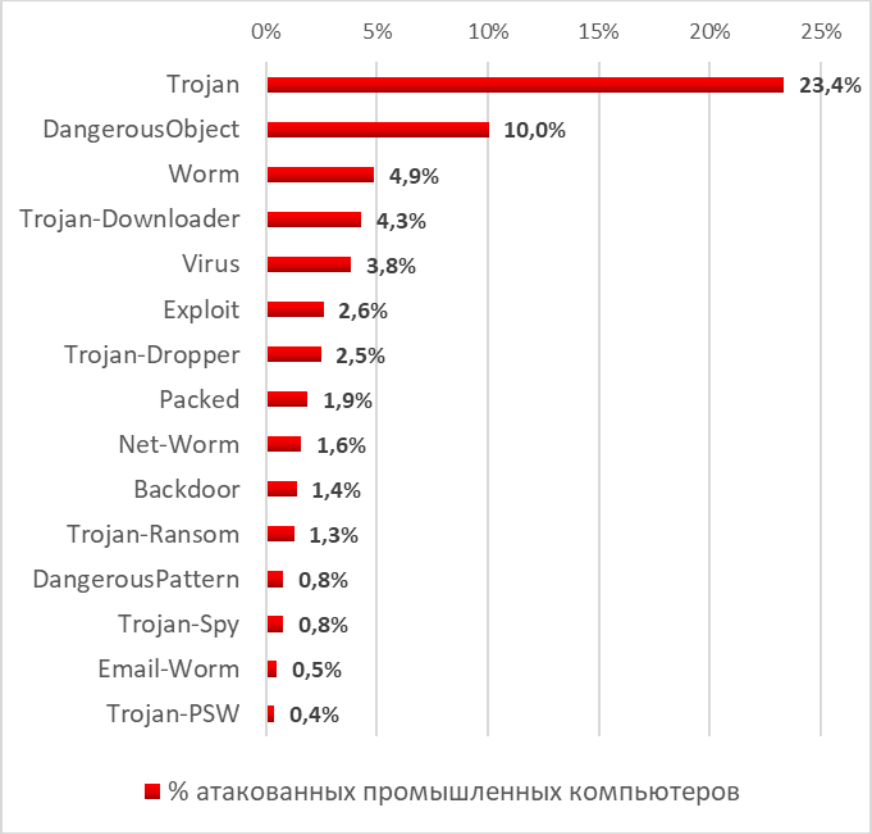
* При расчетах мы исключили страны, число промышленных пользователей в которых недостаточно для получения репрезентативных данных.
Россия в этом рейтинге занимает 22-е место.

Вредоносное ПО на системах промышленной автоматизации

В совокупности во втором полугодии 2016 года на системах промышленной автоматизации было обнаружено порядка двадцати тысяч различных модификаций вредоносного ПО, относящихся более чем к двум тысячам различных семейств.

В большинстве случаев попытки заражения промышленных компьютеров носят случайный характер, а функции, заложенные во вредоносное ПО, не являются специфичными для атак на системы промышленной автоматизации. Таким образом, все те угрозы и категории программ, которые представляют опасность для компаний по всему миру, актуальны и для промышленных компаний. Среди них – троянцы-шпионы, финансовые зловреды, программы-вымогатели (включая шифровальщики), бэкдоры и программы типа Wiper (KillDisk), выводящие из строя компьютер и затирающие данные на диске.

Примечательно, что рейтинги вредоносных программ, обнаруженных на промышленных компьютерах, и вредоносных программ, обнаруженных на корпоративных компьютерах, практически не отличаются. По нашему мнению, это свидетельствует об отсутствии существенных различий между компьютерами в корпоративной и технологической сетях, когда речь идет о риске случайного заражения. Но, очевидно, что в технологической сети даже случайное заражение компьютеров может привести к опасным последствиям.



Распределение атакованных промышленных компьютеров по классам атакующего их вредоносного ПО (второе полугодие 2016)

Вредоносное ПО, относящееся к классам Backdoor, Trojan-Ransom, Trojan-Spy и Trojan-PSW, представляет особую опасность для компьютеров в промышленной сети.

Trojan-Ransom. Одна из разновидностей программ-вымогателей (Trojan-Ransom) блокирует зараженный компьютер и требует перечисления на счет злоумышленника денежных средств за разблокирование. Практически любая такая программа может полностью парализовать контроль инженеров и операторов АСУ ТП над системой автоматизации. При этом сама программа-вымогатель может не располагать какой-либо информацией об автоматизированной системе, которую она заблокировала. Другая разновидность Trojan-Ransom шифрует рабочие документы и файлы, что, в случае заражения систем промышленной автоматизации, также может привести к потере контроля над управляемыми системами. Так, в конце ноября 2016 года транспортная система Сан-Франциско была заражена вредоносной программой-вымогателем, что привело в том числе к блокированию терминалов проверки оплаты проезда. За расшифровку файлов и разблокировку зараженных систем злоумышленники требовали перевести сумму в размере 100 единиц в криптовалюте Bitcoin (что равно примерно 73 000 долларов США).

Backdoor, Trojan-Spy и Trojan-PSW. Вредоносные программы классов Backdoor, Trojan-Spy и Trojan-PSW чаще всего являются агентами ботнет-сетей, управляемых через командные серверы злоумышленников (C&C). Такие программы не только собирают и передают злоумышленнику информацию о зараженном компьютере, его пользователях и системах в сети, но могут быть

использованы для целевой атаки, поскольку заложенные в них функции предоставляют злоумышленнику богатый выбор возможностей для удаленного управления.

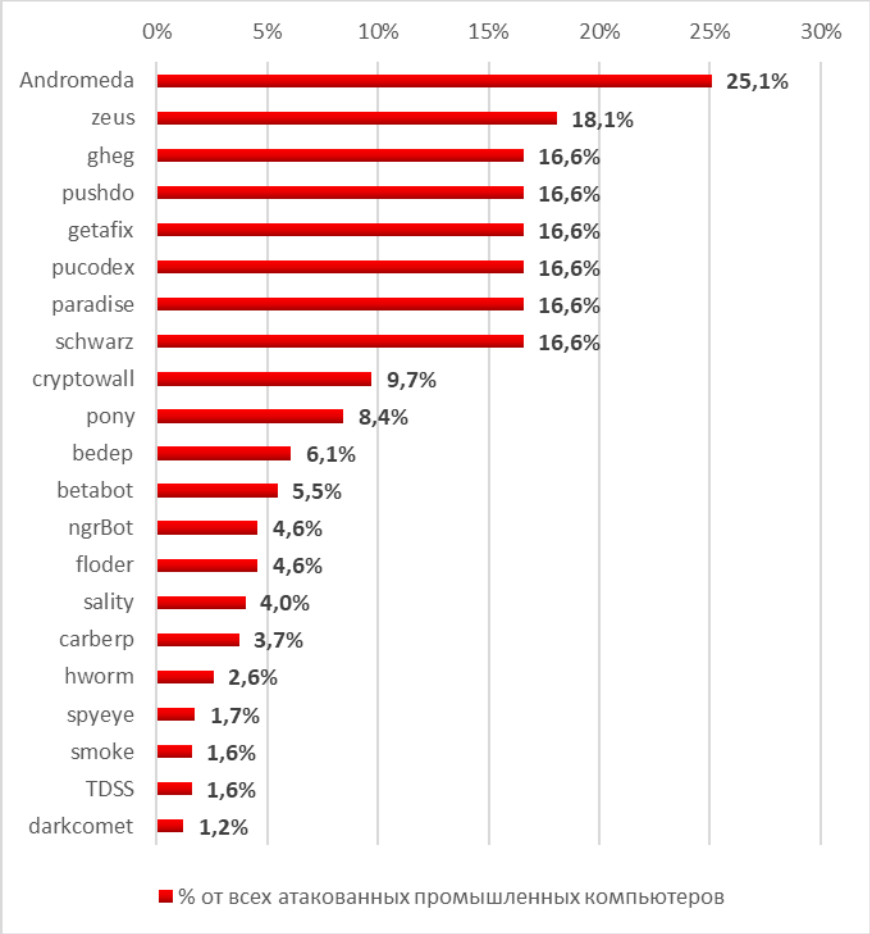
Ботнет-активность в промышленных сетях

По нашим данным, на 5% всех атакованных промышленных компьютеров были обнаружены ботнет-агенты (вредоносное ПО с функциями удаленного управления через командные серверы) и/или признаки их активности.

В большинстве случаев ботнет-агенты выполняют неспецифичные для промышленных систем действия, такие как поиск и кража финансовой информации, кража данных аутентификации для различных интернет-ресурсов и интернет-сервисов, перебор паролей, рассылка спама, а также атаки на заданные удаленные интернет-ресурсы, в частности, – атаки, направленные на отказ в обслуживании (DDoS).

Несмотря на то, что перечисленные действия не направлены явно на нарушение работы какой-либо промышленной системы, такое использование системных ресурсов, а также несовместимость и/или ошибки в коде вредоносных программ и промышленного ПО могут приводить к нарушению работы сети, отказу в обслуживании (DoS) зараженной системы и других устройств в сети. Примеры таких случаев нам довелось наблюдать в процессе выполнения анализа защищённости промышленных предприятий, проведённого в 2016 году. Кроме того, в случае если ботнет-агент производит атаку на сторонние интернет-ресурсы (с такими случаями мы также сталкивались), у компании - владельца IP-адресов могут возникнуть репутационные риски.

Большинство ботнет-агентов являются модульным вредоносным ПО, функциональность которого может изменяться динамически, в том числе на основе данных о системе, переданных на командные серверы злоумышленников. А тех данных, которые ботнет-агенты собирают о системе по умолчанию, достаточно для точного определения компании-владельца и типа системы. Кроме того, доступ к инфицированным ботнет-агентами машинам зачастую выставляется на продажу на специализированных биржах в даркнете.



Распределение промышленных компьютеров, атакованных ботнет-агентами, по семействам ботов

По нашим данным, во втором полугодии 2016 года наиболее распространенным семейством ботнет-агентов в промышленных сетях (25,1% от всех атакованных ботами промышленных компьютеров) оказалось вредоносное ПО Andromeda (Backdoor.Win32.Androm). Последнее время боты этого семейства часто используются для организации спам-рассылок, а также для загрузки на зараженный компьютер модулей, шифрующих файлы на жестком диске с целью получения денег за предоставление ключа для расшифровки.

На втором месте по количеству атакованных ботнет-агентами машин в промышленной сети (18,1% атакованных ботами машин) находятся агенты бот-сети ZeuS (Trojan-Spy.Win32.Zbot). Основной вредоносной функцией программ этого семейства является кража данных аутентификации для доступа к различным интернет-сервисам. Утечка исходного кода вредоносной программы семейства Zbot в 2011 году привела к появлению множества модификаций вредоносных программ этого семейства. Распространение ZeuS/Zbot обычно происходит через фишинговые письма и зараженные веб-сайты; с которых атакуются известные уязвимости в браузерах и плагинах, а также с использованием другого вредоносного ПО.

Вредоносные программы, составляющие ботнет Cryptowall (9,7% атакованных ботами машин) относятся к типу вредоносных программ-вымогателей семейства Trojan-Ransom.Win32.Cryptodef,

основной функцией которых является шифрование файлов на диске с целью получения денежных средств от пользователя в обмен на ключ для расшифровки файлов. Основным способом распространения вредоносного ПО этого семейства являются фишинговые сайты и письма, содержащие вложения с вредоносными файлами, написанными на языке программирования JavaScript. После запуска скрипт загружает на атакованную систему копию вредоносной программы семейства Cryptodef, которая шифрует файлы на зараженном компьютере и блокирует экран приветствия операционной системы. На заблокированном экране вредоносное ПО выводит сообщение с требованием перевода денег в обмен на предоставление ключа расшифровки файлов и разблокирование зараженной системы.

Целевые атаки на промышленные компании

По нашим данным, атаки на компании различных секторов промышленности все чаще становятся направленными (целевыми). Это организованные атаки, которые могут быть нацелены на одно конкретное предприятие, на несколько предприятий, компании одного промышленного сектора или на широкий круг промышленных предприятий, как в случае обнаруженной нами фишинговой атаки (см. ниже).

Задача защиты от целевых атак, как правило, более сложная, чем защита от случайных заражений. В целевых атаках помимо известных зловредов, распространяемых на киберкриминальном рынке, злоумышленники могут использовать уникальные вредоносные программы, разработанные для конкретной атаки, – в том числе 0-day эксплойты. Для запуска вредоносного ПО могут применяться и легитимные интерпретаторы кода (такие как Perl, Python, PowerShell), что также затрудняет выявление атак на ранних стадиях. Кроме того, как показывает практика последних лет, довольно часто в атаках, перенимающих методы APT-атак, стал использоваться инструментарий публично доступных фреймворков для тестирования на проникновение.

Целевые атаки практически всегда начинаются с атаки на самое слабое звено любой защиты – на пользователей. Чтобы повысить вероятность заражения компьютеров, злоумышленники используют атаки типа watering hole и отточенные методы социальной инженерии. В результате сотрудники сами загружают и запускают вредоносное ПО на компьютерах своей организации.

Помимо заражения машин в корпоративной сети, у злоумышленников есть способы проникнуть в изолированную технологическую сеть:

1. Таргетированное заражение USB с целью распространения зловредных программных модулей и переноса информации между компьютерами, преодоление «воздушного зазора». История знает немало примеров, где это реализовано – например, атаки Stuxnet, Flame, Equation, ProjectSauron.
2. Компрометация локального ресурса в интранете, к которому есть доступ из технологической сети, или компрометация сетевого оборудования. Вариантов тут у продвинутого атакующего много: размещение watering hole скрипта на внутреннем веб-ресурсе, подмена файлов на файловом сервере, файлов обновлений с сервера обновлений. При необходимости атакующие могут использовать какой-либо локальный сервер в качестве сервера управления для зараженного изолированного компьютера. В случае компрометации роутеров появляется возможность «слушать» трафик

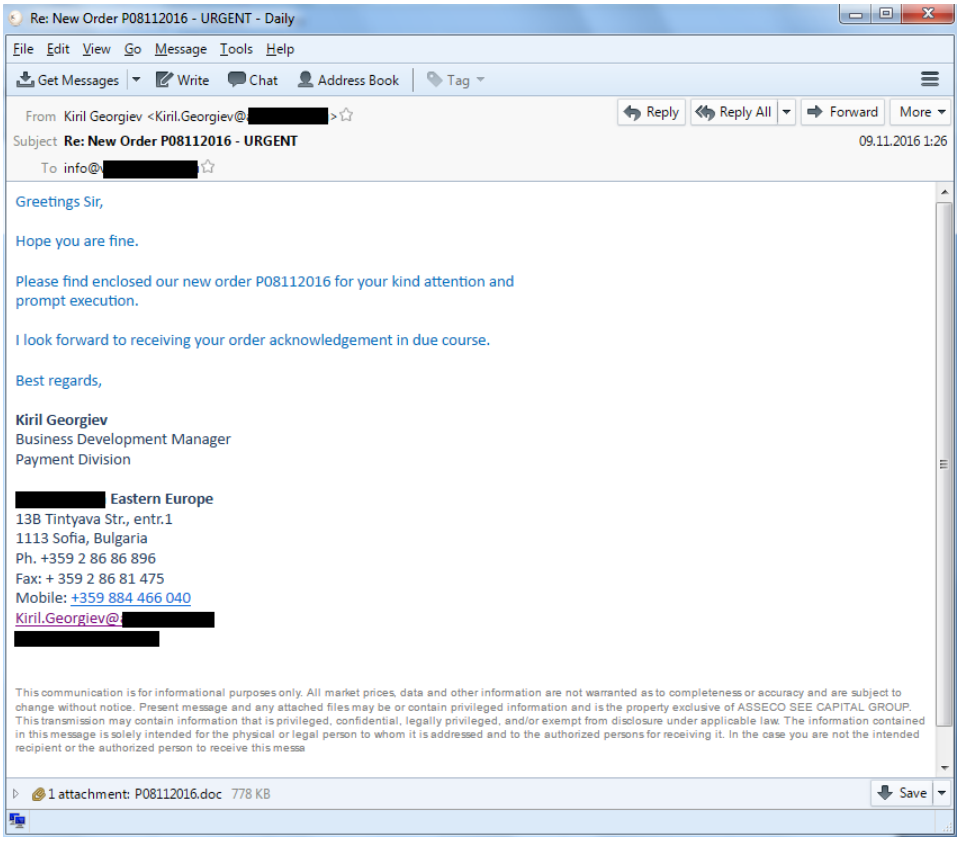
и извлекать различные учетные данные для дальнейшего доступа к компьютерам и ресурсам, как это было реализовано в атаках BlackEnergy2.

3. Заражение компьютеров подрядчиков промышленных компаний, которые подключают свои компьютеры в технологическую сеть.

Целевая фишинговая атака на промышленные компании

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) обнаружил серию фишинговых атак, начавшихся не позднее июня 2016 года и продолжающихся в настоящее время. Атаки направлены преимущественно на промышленные компании – металлургические, электроэнергетические, строительные, инжиниринговые и другие. По нашей оценке, в общей сложности атакам подверглись более 500 компаний более чем в 50 странах мира.

Во всех исследованных нами случаях фишинговые письма отправлялись от имени различных компаний-поставщиков, заказчиков, коммерческих организаций и служб доставки с предложением посмотреть обновленные списки цен на продукцию, требованием срочно проверить информацию по счету, уточнить расценки на продукцию, переслать якобы поврежденный файл или получить груз по накладной.



Одно из фишинговых писем

Документы, прикрепленные к письмам, представляли собой RTF-файлы, содержащие эксплойт к уязвимости CVE-2015-1641, архивы различных форматов, содержащие вредоносные

исполняемые файлы, а также документы с макросами и OLE-объектами, скачивающими вредоносные исполняемые файлы. Исполняемые файлы внутри документов, архивов, а также скачанные со стороннего сервера, представляют собой троянцев-шпионов и бэкдоры различных семейств, таких как ZeuS, Pony/FareIT, Luminosity RAT, NetWire RAT, HawkEye, ISR Stealer.

Анализ заголовков писем позволяет сделать вывод о том, что многие письма рассылались с почтовых серверов компаний, зараженных ранее шпионским вредоносным ПО, предназначенным для кражи учетных данных от почтовых аккаунтов.

Все вредоносные программы, используемые в атаке, не являются уникальными для данной вредоносной кампании, они весьма популярны у злоумышленников. Однако эти программы упакованы уникальными модификациями VB- и MSIL-упаковщиков, которые применяются только в данной операции.

На графиках ниже показано распределение атакованных компаний по отраслям промышленности. Наибольшее число атак на компании промышленного сектора приходится на долю различных компаний-производителей, в частности, промышленного оборудования, материалов и электроники. Также значительная часть атакованных компаний относится к сфере строительства и проектирования промышленных сооружений и систем автоматизации.

Распределение атакованных промышленных компаний по индустриям

Наш опыт расследования целевых атак показывает, что кибершпионаж часто является подготовкой к следующим этапам атаки. На основе имеющихся данных нам пока не удалось достоверно установить конечную цель и мотивацию злоумышленников. Расследование этой атаки продолжается.

Каждая четвертая целевая атака, обнаруженная «Лабораторией Касперского» в 2016 году, была нацелена в том числе на предприятия различных индустрий – машиностроительной, энергетической, химической промышленности, транспортной и других.

APT-атаки

APT-атаки (Advanced Persistent Threats) – наиболее опасный вид кибератак. Во многих случаях их отличает высокий уровень атакующих, техническая сложность и продолжительность – APT-атаки могут длиться годами. Это тщательно продуманные и организованные атаки, которые требуют больших ресурсов. Среди жертв APT-атак – высокопоставленные лица, службы разведок разных стран, правительственные, военные учреждения, научные организации, СМИ, промышленные компании. И предприятия, относящиеся к системам критической инфраструктуры разных стран.

В подавляющем большинстве случаев цель APT-атак – кража ценной информации (кибершпионаж). Однако известны случаи атак с использованием вредоносных программ - промышленных диверсантов – Stuxnet, Black Energy, Shamoon Wiper (1, 2), StoneDrill. Эти атаки были направлены на осуществление диверсий на атакованных предприятиях и, как следствие, нарушение производственного и бизнес-процессов.

Заключение

Выполненные во второй половине 2016 годя экспертами Kaspersky Lab ICS CERT исследования наглядно иллюстрируют ряд тенденций в развитии безопасности промышленных предприятий. Суммируем их здесь.

1. Стабильный рост процента атакуемых промышленных компьютеров фиксируется с начала наблюдения, что свидетельствует об актуальности проблемы кибербезопасности промышленных систем.
2. Ландшафт информационных угроз для промышленных систем становится все больше похожим на ландшафт угроз для корпоративных сетей. Необходимость повысить управляемость и, как следствие, эффективность производства приводит к появлению физических соединений сетей и сопряжению смежных информационных систем. Всё чаще применяются схожие наборы технологий, схожие архитектурные решения и сценарии использования. Вряд ли эта тенденция изменится. Как следствие, можно ожидать не только появления новых угроз, специально разработанных для промышленных предприятий, но и развития существующих, традиционных IT-угроз – их адаптацию для атак на промышленные предприятия и объекты физического мира.
3. Изоляция промышленных сетей больше не может рассматриваться как мера их защиты. Доля попыток заражений вредоносным ПО с участием переносных носителей, заражений резервных копий, использование в сложных атаках изощренных способов переноса данных из изолированных сетей свидетельствуют о том, что невозможно избежать рисков путем простого отключения системы от интернета.
4. Подход производителей промышленного ПО и оборудования к исправлению уязвимостей и ситуацию с устранением известных уязвимостей на предприятиях нельзя назвать обнадеживающими. Подавляющее большинство промышленных предприятий годами остаются уязвимыми к компьютерным атакам.
5. Появление масштабных вредоносных кампаний, нацеленных на промышленные предприятия, говорит о том, что злоумышленники расценивают это направление как перспективное для себя. Это – серьёзный вызов для всего сообщества разработчиков

промышленных систем автоматизации, владельцев и операторов этих систем, производителей средств защиты. Мы всё ещё по большей части удивительно медлительны и нерасторопны, что в сложившейся ситуации грозит опасными последствиями.

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**