Поток данных об угрозах для систем промышленной автоматизации

Проблема

Задача обеспечения эффективной киберзащиты промышленных предприятий постоянно усложняется растущими разнообразием и динамикой киберугроз. Это формирует острую потребность в актуальных данных, без которых затрудняются своевременное обнаружение атак, выявление и эффективное расследование киберинцидентов на компьютерах АСУ.

Решение

Ежедневно обновляемый поток данных об актуальных угрозах на основе информации, получаемой с компьютеров АСУ, и результатов расследований киберинцидентов на промышленных предприятиях.

Для кого

Службы информационной безопасности промышленных предприятий, поставщики услуг по управлению кибербезопасностью (MSSP), центры реагирования на компьютерные инциденты (CERT).

Проблематика

Заражение компьютеров технологической сети вредоносным ПО может привести к серьезными непредсказуемым последствиям для предприятия. Согласно нашим наблюдениям, разнообразие и количество вредоносного ПО, блокируемого продуктами Kaspersky на компьютерах АСУ, растет. К сожалению, не все узлы технологической сети возможно надежно защитить современным полноценным решением. И даже, если вредоносное ПО было заблокировано, сотрудникам предприятия часто не хватает контекстной информации, чтобы понять, является ли это признаком более серьезного инцидента. Для обнаружения атак, их классификации, быстрого выявления зараженных систем, предотвращения развития заражений в технологической сети и расследования инцидентов на предприятиях критически важно иметь максимально полную информацию об актуальных угрозах.

Что мы предлагаем

Постоянно обновляемый поток данных об угрозах, актуальных для систем промышленной автоматизации, который содержит индикаторы компрометации (IoC). Эти индикаторы позволяют выявлять вредоносное и

потенциально опасное ПО, обнаруженное на компьютерах АСУ по всему миру защитными решениями «Лаборатории Касперского», а также находить скомпрометированные системы в ходе расследования инцидентов в технологической сети промышленных предприятий.

Поток данных дает возможность обезопасить системы, которые по объективным причинам невозможно эффективно защитить другими способами.

С помощью потока данных можно:

- обнаруживать еще в офисной сети предприятия и на периметре угрозы, способные попасть на компьютеры АСУ, и таким образом надежнее защитить технологическую сеть;
- обнаруживать в режиме реального времени атаки на АСУ ТП и связанные с ними системы технологической сети;
- выявлять заражения компьютеров технологической сети вредоносным ПО в ходе проведения работ по реагированию на компьютерные инциденты;
- обогащать данные об угрозах и вредоносном ПО, обнаруженных в сети предприятия, дополнительной информацией от «Лаборатории Касперского».

Как мы работаем

Поток данных об угрозах обновляется каждые 60 минут на основе информации, получаемой через Kaspersky Security Network (KSN) от компьютеров АСУ, защищаемых продуктами «Лаборатории Касперского» по всему миру.

Все полученные данные верифицируются и обогащаются с помощью различных технологий и техник, таких как анализ на основе статистических критериев, анализ экспертными системами «Лаборатории Касперского» (песочницы, эвристический анализ, анализ подобия, профилирование поведения и т. д.), проверка аналитиками и проверка по «списку разрешенного ПО».

Что получает клиент

Данные об угрозах для систем промышленной автоматизации. Они предоставляются в открытом JSON-формате и могут быть использованы различными системами анализа и сопоставления данных или переформатированы в любой другой требуемый формат данных. Данные могут быть внедрены в сторонние SIEM-системы.

Первичный файл данных (его размер не превышает 100 МБ) формируется за период три месяца и содержит более 200 тыс. записей. Данные обновляются каждые 60 минут.

Данные об угрозах представлены в виде индикаторов компрометации (MD5-хеш-сумм) и связанных с ними метаданных, которые могут быть использованы для обогащения существующих данных, в частности информации о файлах, имеющих указанную MD5-хеш-сумму:

- SHA1 и SHA256 хеш-суммы файла;
- топ имен файлов, под которыми чаще всего распространяется вредоносное ПО;
- размер файла в байтах;
- тип формата файла;
- название вердикта в антивирусных базах «Лаборатории Касперского»;
- показатель распространенности файла;
- даты первого и последнего события регистрации файла в базе данных об угрозах;
- географическая распространенность файла;
- список из 10 IP-адресов, с которых наиболее часто загружались вредоносные объекты;
- список URL-адресов, с которых загружались вредоносные объекты.

Отличие от других источников данных об угрозах для АСУ ТП

Традиционно принято считать, что АСУ ТП отделены от офисной сети предприятия, изолированы от интернета и, соответственно, от угроз, так или иначе связанных с ним. Тем не менее, различные защитные продукты Kaspersky установлены по всему миру на компьютеры, относящиеся к АСУ ТП и прочим OT-системам, включая:

- 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;
- человеко-машинные интерфейсы (HMI);
- компьютеры администраторов технологических сетей и разработчиков ПО для систем промышленной автоматизации.

Данные анализа телеметрии, поступающие от этих защитных продуктов, и наши исследования указывают на существование многочисленных и разнообразных угроз, демонстрирующих способность добраться до OT-систем организаций различных секторов.

Разновидностей такого вредоносного ПО много, в том числе:

- шпионское ПО, программы-вымогатели, ботнет-агенты, бэкдоры, ПО для уничтожения данных и др.;
- ПО для майнинга криптовалют, различные типы самостоятельно распространяющегося ПО (черви и вирусы);
- вредоносное ПО, разработанное для популярных инженерных пакетов, таких как AutoCAD;
- потенциально опасное ПО для удаленного доступа;
- вредоносное ПО, используемое в целенаправленных атаках на промышленные компании.

Источниками проникновения этого вредоносного ПО на компьютеры АСУ ТП могут быть:

- специализированные онлайн-форумы, ориентированные на работающих на производстве инженеров, в том числе те, где распространяются патчи, программы для взлома инженерного и промышленного ПО, пропатченное/взломанное инженерное ПО и ПО для АСУ ТП;
- фишинговые атаки, нацеленные преимущественно на промышленные организации или организации определенного сектора, и целевые фишинговые атаки на конкретную организацию, включая вредоносные рассылки со скомпрометированных почтовых ящиков поставщиков, клиентов, технологических и бизнес-партнеров;
- незащищенные антивирусными решениями узлы технологической сети (становятся источниками многократных повторных заражений, в том числе и устаревшим вредоносным ПО, не встречающимся почти нигде более в ИТ-сетях);
- зараженные переносные источники данных (USB-накопители);
- атаки на подрядчиков и смежников, поставщиков специализированных услуг, имеющих удаленный и локальный доступ в контур технологической сети;
- атаки на цепочки поставок ПО и оборудования для АСУ ТП.

Все это делает ландшафт угроз технологических сетей промышленных предприятий отличающимся от ландшафта угроз ИТ-инфраструктур*, даже несмотря на то, что в атаках на промышленные предприятия в основном используется вредоносный инструментарий общего назначения. Обычно в атаках злоумышленники используют бинарно модифицированные экземпляры, применяя различные техники обфускации и модификации бинарного кода для снижения вероятности его детектирования.

*Так, более 70% обнаруживаемых нами на компьютерах АСУ ТП экземпляров вредоносного ПО редко встречается в ИТ-инфраструктурах или вовсе не встречаются на ИТ-системах, поэтому они не попадают в потоки данных об угрозах Enterprise. По той же причине сигнатуры для каких-то экземпляров такого

вредоносного ПО могут отсутствовать в некоторых неспециализированных защитных решениях.

Помимо общей специфичности ландшафта угроз для компьютеров АСУ ТП, в своих исследованиях мы наблюдаем региональную и отраслевую специфику. Данные потока включают угрозы, обнаруженные на компьютерах организаций из различных индустрий и сфер, включая (но не ограничиваясь):

- автомобильная промышленность;
- энергетика;
- пищевая промышленность;
- здравоохранение и фармацевтическая промышленность;
- производство;
- нефтегазовая отрасль;
- металлургия;
- добыча полезных ископаемых;
- транспорт и логистика;
- коммунальная сфера;
- переработка и утилизация отходов.

В поток также включены данные, полученные с атакованных OT-систем, относящихся к следующим типам инфраструктур:

- инжиниринг и интеграторы АСУ;
- разработка ПО для АСУ;
- автоматизация зданий;
- биометрические системы аутентификации в OT и контроля физического доступа.

Такие системы часто становятся промежуточными звеньями в цепочке атак на системы АСУ ТП и распространении атак на прочие OT-инфраструктуры.

Сценарии использования

Обнаружение вредоносного ПО и атак, имеющих потенциал достичь АСУ ТП

Сопоставление данных потока с данными SIEM-систем, собираемых с периметра сети, конечных узлов и песочниц.

- Сопоставление MD5-хеш-сумм, представленных в потоке данных об угрозах, с MD5-хеш-суммами файлов:
  - проходящих через периметр сети (прокси-сервера, SMTP, FTP, SMB);

  - обнаруживаемых/регистрируемых на конечных узлах (средствами антивирусной защиты, ПО для контроля запуска приложений и/или в ходе аудита);
  - анализируемых в песочницах.

- Сопоставление IP и URL, представленных в потоке данных об угрозах, с IP и URL:

  - входящих/исходящих соединений, регистрируемых на периметре сети (межсетевых экранах, IDS, IPS, прокси-серверах);
  - входящих/исходящих соединений, регистрируемых на конечных точках (локальным межсетевым экраном, IDS, IPS);
  - обнаруживаемых в результатах динамического анализа файлов в песочницах;
  - встречающихся в сообщениях электронной почты.

Выявление случаев заражения компьютеров АСУ ТП в ходе аудита ИБ или расследования инцидентов

Данные об угрозах подходят для выявления случаев заражения компьютеров систем промышленной автоматизации вредоносным ПО. Это данные, обнаруженные:

- при анализе файловой системы анализируемого компьютера;
- в журналах событий средств антивирусной защиты, ПО для контроля запуска приложений и др.;
- в копиях сетевого трафика;
- в журналах событий межсетевых экранов, IDS, IPS, прокси-серверов, песочниц;
- в снимках памяти процессов.

Обогащение данных об угрозах

При обнаружении инцидента или в ходе проведения расследования специалистам часто требуется дополнительная информация об обнаруженных угрозах. Метаданные об угрозах, которые наряду с индикаторами компрометации содержатся в потоке данных, существенно упрощают расследование, давая возможность:

- приоритизировать инцидент, оценив степень нацеленности атаки;
- связать между собой разрозненные факты о киберинциденте для получения более полной картины атаки;
- провести поиск связанных событий, компонентов вредоносного ПО, попыток атаки и/или случаев заражения прочих систем предприятия.

Запросить консультацию специалиста

Статьи по теме

- Динамика внешних и внутренних угроз АСУ. Второй квартал 2025 года
- Ландшафт угроз для систем промышленной автоматизации. Первый квартал 2026 года
- Атаки, использующие доверенную корпоративную инфраструктуру для кражи учетных данных в сетях АСУ

Рекомендуем дополнительно

- Аналитика известных уязвимостей АСУ для принятия критически важных решений в части информационной безопасности
- Информация об уязвимостях и угрозах для АСУ ТП
- Расследование киберинцидентов на промышленных предприятиях
- Цифровая криминалистика и расследование инцидентов в АСУ ТП. Тренинг
- Разработка руководства и обучение реагированию на инциденты

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com