Kaspersky ICS CERT

kaspersky

Секреты «успеха» APT-атак

Из опыта расследования инцидентов

Вячеслав Копейцев

06.06.2023 Version 1.0

«Антивирус Шрёдингера» — он как бы есть, но его как бы и нет

На первый взгляд, эта причина инцидента не кажется очевидной, ведь все говорят, что «решения для обеспечения кибербезопасности у нас везде установлены». Но, как показывает практика, — не всё так просто. Много раз, ища в процессе расследования инцидента ответ на вопрос «почему же так вышло?», мы обнаруживали множество проблем настройки и использования защитных решений.

Бывает так, что **люди, ответственные за информационную безопасность, месяцами не заходят в панель управления защитными решениями**. Надеяться на то, что автоматизированное средство защитит само ото всех угроз без вашего участия, — наивно. Злоумышленники изобретательны и настойчивы, а в вашем королевстве, скорее всего, не всё в порядке. В случае инцидента перекладывать всю ответственность на защитные решения (дескать, это продукт пропустил угрозу) непродуктивно. Во многих случаях успешные действия злоумышленника становятся результатом безответственного, халатного и некомпетентного отношения некоторых сотрудников атакованной организации к базовым принципам и правилам кибербезопасности. В 2022 году проблемы в настройках антивирусных решений были одной из причин «успешности» атак APT-группы на промышленные предприятия и государственные учреждения.

Изучая причины инцидента, мы часто видим:

- множество систем, которые давно не получали обновления баз защитных решений;
- систем, на которые забыли добавить лицензионный ключ, хотя он был куплен;
- систем, на которых пользователь имеет возможность удалить лицензионный ключ (и таких, где пользователь его на самом деле и удалил);
- систем, на которых защитное решение остановлено пользователем или выключены его компоненты, необходимые для защиты от современных угроз;
- систем, имеющих необоснованно большое количество исключений из проверки и защиты.

Ситуация, когда защитное решение работает с устаревшими сигнатурными базами и не имеет подключения к облачным сервисам проверки репутации файлов и URL в реальном времени, зачастую приводит к беспрепятственному и бесконтрольному распространению вредоносного

ПО, ведь в случае APT-атак злоумышленники тратят значительные ресурсы для того, чтобы «сбить детект». В прошлом, 2022-м, году мы провели расследование, в ходе которого установили, что APT-группа находилась в сети организации более трёх лет — и всё из-за устаревшего защитного решения, часть модулей которого к тому же была отключена.

Не стоит забывать и про **важность безопасной настройки защитных решений!** Чаще всего в ходе проведения атаки злоумышленники пытаются украсть логины и пароли доменных учётных записей, чтобы иметь возможность подключаться к другим системам и развивать атаку. Во многих случаях злоумышленники подключаются к системе по RDP и просто выключают защитное решение. Почему это становится возможным? Да потому, что сотрудник, ответственный за настройку защитного решения, забыл включить обязательный запрос ввода пароля администратора при попытке отключения защиты. Хотя настроить такой запрос в Kaspersky Security Center, например, — дело пары минут.

В 2022 году мы заметили новый тренд в тактике APT. В поиске средств продвижения по сети жертвы злоумышленники не останавливаются на захвате контроллера домена. Следующей целью становятся серверы управления защитными решениями. Задачи могут быть разными: получить доступ к собранной в одном месте детальной информации об атакованной инфраструктуре, добавить вредоносное ПО в исключения, отключить защитные решения, а иногда даже распространить вредоносное ПО встроенными средствами системы управления защитным решением, в том числе и на системы, не входящие в захваченный домен. Бывает так, что канал управления защитными средствами — единственный канал, связывающий сети различной степени защищённости, и через него можно добраться до сегментов сети, на бумаге изолированных (air gapped).

Чтобы справиться с этой проблемой, Kaspersky ICS CERT и Департамент исследований и разработки «Лаборатории Касперского» совместно разработали «Hardening Guide» — набор рекомендаций, который позволяет многократно укрепить защиту Kaspersky Security Center. Например, Hardening Guide описывает, как включить двухфакторную аутентификацию для входа в KSC и, тем самым, предотвратить захват защитных решений в ситуации, когда скомпрометирован даже контроллер домена. Найти Hardening Guide можно на нашем сайте технической поддержки.

Наконец, бывает так, что **в технологических сетях средства защиты вообще не установлены на многих конечных узлах**. Причины могут быть разные. Иногда инженеры думают, что их системы АСУ ТП полностью изолированы от других сегментов сети. В других случаях инженеры просто боятся что-либо внедрять по принципу «работает — не трогай».

Также выбор защитного решения может осложнять ситуация, когда производители промышленного оборудования требуют устанавливать на системы в АСУ ТП только сертифицированное ими программное обеспечение, в противном случае угрожая снять системы с гарантии.

Даже в случае, когда технологическая сеть на самом деле не связана с другими сетями и со внешним миром, у злоумышленников есть способы получить к ней доступ. Например, создавая специальные версии вредоносного ПО, которые распространяются через сменные носители. Только в прошлом, 2022-м, году мы видели такую тактику в действии в арсенале по меньшей мере двух APT-групп при атаках на промышленные организации. Выше мы упомянули один из типичных случаев, когда сотрудники промышленных предприятий на самом деле заблуждаются, считая технологическую сеть не связанной с офисной (сети оказываются на деле связаны каналом управления защитным решением). Ниже расскажем о других подобных типовых проблемах изоляции сети.

Проектируя систему информационной безопасности, всегда нужно исходить из предположения, что злоумышленникам удастся добраться до узлов АСУ ТП. Именно поэтому мы рекомендуем использовать Kaspersky Industrial CyberSecurity — специализированную промышленную XDR-платформу, продукт, который сертифицирован на совместимость и рекомендован ведущими мировыми и отечественными производителями промышленного оборудования и систем автоматизации, а также имеет сертификаты ФСБ и ФСТЭК России, что позволяет устанавливать его на объекты КИИ.

Проблемы изоляции технологической сети — мифический air gap и плоская сеть

Типичным примером нарушения требования изоляции технологической сети являются **машины с несколькими сетевыми интерфейсами**, например, рабочие станции инженеров, подключенные и к ИТ сети, и к сети АСУ ТП, а также компьютеры, которые в разное время подключены к разным сетям (в основном ноутбуки инженеров, но не только — мы видели случаи, когда заражение технологической сети происходило через сервер, временно введенный в состав офисной сети для технического обслуживания, а затем снова подключенный к сети АСУ ТП). В некоторых случаях мы наблюдали ситуации, когда инженер с одного и того же компьютера общался в социальных сетях и вносил изменения в программу ПЛК. Заразив такую машину вредоносным ПО, злоумышленник фактически получал доступ к оборудованию в технологической сети. Именно таким

образом несколько лет назад вредоносная программа WannaCry попала в технологическую сеть одного нефтеперерабатывающего завода. Это имело весьма неприятные последствия (перебои в работе системы отгрузки продукта).

Удалённый доступ в технологическую сеть для сотрудников предприятия и подрядных организаций тоже далеко не всегда организован с соблюдением всех необходимых мер ИБ. Часто это делается через утилиты удалённого администрирования, такие как TeamViewer или Anydesk. Многие из упомянутых каналов связи, обнаруженных в ходе расследования того или иного инцидента, разрешались как «временные», но прижились навсегда. О некоторых из них сотрудники предприятия и вовсе забыли — а злоумышленники такие каналы связи с лёгкостью находят.

Буквально несколько месяцев назад мы расследовали инцидент, в котором сотрудник подрядной организации использовал удалённый доступ в сеть АСУ ТП, предоставленный ему на легитимной основе несколькими годами ранее, в попытке совершить диверсию. Эта история ещё раз показала, что никогда **нельзя исключать человеческий фактор**, ведь сотрудник может оказаться недоволен оценкой своей работы, оплатой или может быть политически или идеологически мотивирован.

Если **изоляция технологической сети сводится к конфигурации сетевого оборудования,** квалифицированные хакеры почти всегда смогут его переконфигурировать под свои нужды. Например, сделают из него прокси для трафика управления вредоносным ПО и/или сервер по его хранению и доставке в «изолированную» (ранее) сеть — такое мы тоже видели не раз.

Когда инженеры проектируют технологические сети, чаще всего они исходят из соображений простоты (чтобы точно работало, с минимальными трудозатратами на настройку) и дешевизны проекта, не учитывая при этом риски информационной безопасности. В результате получается, как правило, **«плоская сеть» — ни разбиения на VLANы, ни демилитаризованных зон, ни межсетевых экранов внутри сети**. Попав на один из узлов, злоумышленники, как правило, легко могут распространить своё присутствие на всю технологическую сеть, а иногда даже и добраться из неё до сети смежных предприятий, материнской организации или даже до систем государственной структуры.

Kaspersky Industrial CyberSecurity for Nodes позволяет создавать правила, запрещающие запуск определённых программ на системах АСУ ТП, что помогает предотвратить несанкционированное использование утилит

удалённого администрирования. Более того, это решение EPP/EDR класса, которое обеспечивает безопасность всего компьютерного оборудования на базе операционных систем Windows и Linux и немедленно уведомляет другие компоненты платформы о любом подозрительном поведении ПО. В свою очередь, карта сети, построенная при помощи Kaspersky Industrial CyberSecurity for Networks, поможет выявить нарушения сегментации сети, позволяя проследить все цепочки развития атаки — от точки первоначального вторжения и путей продвижения атакующих по сети до применяемых злоумышленниками методов.

Устаревшие операционные системы и прикладное ПО

Интересно, что даже подключенные к интернету **системы промышленных предприятий, обновление которых не представляет большой сложности, могут оставаться уязвимыми в течение длительного времени**, делая технологическую сеть открытой для атак и создавая значительные риски. Об этом свидетельствуют сценарии реальных атак.

В некоторых случаях **установка обновлений оказывается фактически невозможной**. Например, когда обновление операционной системы на сервере вызывает необходимость замены специализированного ПО (например, сервера SCADA), а замена специализированного ПО, в свою очередь, требует модернизации оборудования. В результате **каких только древностей не увидишь в АСУ ТП** — и станок с ЧПУ на Windows XP SP1, и сервер на Windows NT 4.0, и даже технологический процесс под управлением MS DOS!

Однако, даже если оставить в стороне подобные экстремальные сценарии, специфика большинства систем АСУ ТП такова, что **для того, чтобы просто установить обновления безопасности операционной системы** на рабочие станции и серверы, **требуется проведение тщательной процедуры тестирования**, часто выполнение работ возможно только в специально отведённое время — в рамках запланированного технологического простоя. Соответственно, установка обновлений ОС и прикладного ПО, как правило, выполняется очень редко, и злоумышленники долгое время могут пользоваться известными уязвимостями во время проведения атак. В таких случаях на фоне большой стоимости проекта модернизации вопросы информационной безопасности зачастую отходят на второй план.

Если предприятие столкнулось с такой ситуацией, инженерам АСУ ТП и специалистам по информационной безопасности требуется совместно разработать набор компенсирующих мер, которые бы позволили

предотвратить эксплуатацию уязвимостей без обновления системы. Например, могут быть внесены изменения в настройки используемого ПО, уязвимая служба или компонент могут быть попросту отключены, если они не используются, уязвимая система может быть отключена от сети, или может быть реализована дополнительная сегментация, или на сетевом экране может быть настроено специальное правило.

К сожалению, инженеру или специалисту по безопасности не всегда легко определить, уязвима ли конкретная система в технологической сети, насколько в реальности велик риск, имеет ли смысл пытаться устанавливать обновление, закрывающее уязвимость, и какие возможности минимизации риска имеются, если установка обновления невозможна. Все популярные общедоступные базы уязвимостей, включая национальные, предоставляют в лучшем случае информацию, взятую из бюллетеней безопасности, выпущенных производителями уязвимых продуктов. Проблема в том, что бюллетени производителей систем АСУ ТП часто содержат неполные или, что еще хуже, неверные данные.

Как следствие, широко используемые источники сведений об уязвимостях содержат разнообразные несоответствия и ошибки, включая: неверные показатели критичности уязвимостей, которые могут значительно влиять на восприятие риска; списки уязвимых продуктов, не включающие часть продуктов, содержащих данную уязвимость, или включающие продукты, которые ее не содержат. В результате легко сделать неправильные выводы о проблемах безопасности, имеющихся в данной технологической системе и, соответственно, принять необоснованные решения.

Часты и ситуации, когда описания и оценки уязвимостей верны, однако предлагаемые компенсирующие меры, такие как установка более свежих версий, никак не исправляют проблему, поскольку уязвимость представляет собой серьезную ошибку, допущенную при проектировании, которая требует полного пересмотра и перепроектирования уязвимого ПО или прошивки, что на деле производителем при «закрытии уязвимости» не выполнено.

Один из недавних примеров подобных проблем, с которыми нам пришлось столкнуться, — проприетарный протокол UMAS, применяемый компанией Schneider Electric для настройки, мониторинга, сбора данных и управления наиболее популярными промышленными контроллерами Schneider Electric. В 2022 году исследователи Kaspersky ICS CERT опубликовали подробный отчет об обнаруженных в протоколе проблемах и серьезных недостатках, которые оказывают критическое влияние на безопасность систем автоматизации, основанных на решениях Schneider Electric.

Еще сильнее усугубляет проблему то, что в большинстве систем АСУ ТП использованы сторонние технологии и общие компоненты, содержащие уязвимости. В качестве примеров можно привести операционные системы, решения по управлению лицензиями, веб-серверы, протоколы сетевого взаимодействия, системы инжиниринга и среды выполнения кода (например, такие широко применяемые в АСУ ТП технологии как Codesys и IsaGRAPH, которые были подробно проанализированы экспертами Kaspersky ICS CERT) и многое другое. Подобные уязвимости слишком часто ускользают от внимания как производителей технологических систем, которые не считают их своей зоной ответственности, так и производителей сторонних компонентов, которые зачастую не знают, кто применяет их технологии или не считают себя обязанными информировать всех своих конечных пользователей о соответствующих рисках. Это отсутствие ответственного подхода и доступной информации — огромный риск кибербезопасности, представляющий собой мину замедленного действия.

Чтобы получить более адекватное представление о рисках, связанных с уязвимостями в технологических решениях, а также возможность принимать информированные решения, связанные с компенсацией этих рисков, рекомендуем подписаться на аналитические отчеты об угрозах и уязвимостях АСУ ТП на портале Kaspersky Threat Intelligence в виде человекочитаемых отчетов или машиночитаемых потоков данных в зависимости от ваших технических возможностей и потребностей.

Решение Kaspersky Industrial Cybersecurity использует данные Kaspersky Threat Intelligence для автоматического обнаружения и оценки уязвимостей. Оно помогает выявлять устаревшее и уязвимое программное обеспечение, детектирует и блокирует попытки эксплуатации уязвимостей, в том числе в системах АСУ ТП и других решениях.

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