Угрозы использования RAT в ICS

Кирилл Круглов
Kaspersky Lab ICS CERT

Евгений Гончаров
Kaspersky Lab ICS CERT

20.09.2018

Оглавление

В процессе проведения аудитов, тестов на проникновение и расследований инцидентов мы не раз обращали внимание на наличие установленных легитимных средств удаленного администрирования ПК (Remote Administration Tool – RAT) в технологических сетях промышленных предприятий. В ряде расследованных нами инцидентов RAT были использованы злоумышленниками для атаки на промышленные организации. В некоторых случаях это были RAT, скрыто установленные злоумышленниками на компьютеры атакованных организаций, в других случаях злоумышленники могли использовать средства RAT, которые уже присутствовали в организации на момент атаки. Эти наблюдения побудили нас проанализировать масштаб угрозы, включая частоту и причины использования RAT в технологической сети.

Методология

Статистические данные, представленные в этом исследовании, были получены через KSN (Kaspersky Security Network) с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky Lab ICS CERT относит к технологической инфраструктуре организаций. 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).

В данном исследовании мы рассмотрели и проанализировали все популярные RAT для ОС Windows за исключением Remote Desktop, являющегося частью в ОС Windows, – исследование этого RAT еще не закончено и будет представлено в следующей статье этой серии.

Использование RAT в ICS

По данным KSN за первое полугодие 2018 года, легитимные RAT (программы класса not-a-virus: RemoteAdmin) установлены и используются на каждом третьем компьютере АСУ.

Процент компьютеров АСУ, на которых легитимно установлены RAT

Статистика подтверждает наши наблюдения. RAT, действительно, часто используются в технологических сетях промышленных предприятий. По нашему мнению, это может

быть обусловлено попытками удешевить обслуживание АСУ и уменьшить время реагирования в случае возникновения неполадок.

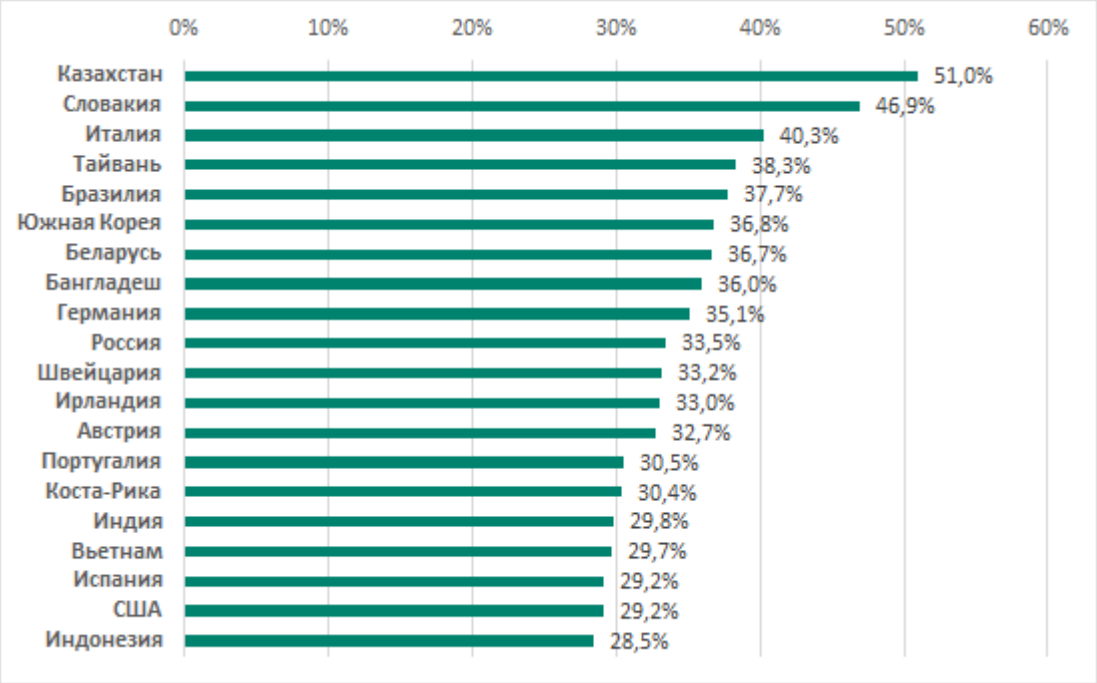
Как нам удалось выяснить, удаленный доступ к компьютерам в технологической сети может использоваться не только администраторами и инженерами внутри периметра сети предприятия, но и предоставляется пользователям, находящимся вне периметра сети организации, – через сеть Интернет. В число таких пользователей могут входить представители сторонних предприятий – специалисты интегратора или производителя средств АСУ ТП, – которые используют RAT для выполнения работ по диагностике, обслуживанию и устранению сбоев АСУ. Как показали проведенные нами обследования безопасности промышленных сетей, часто такой доступ плохо контролируется ответственными сотрудниками предприятия, а подключающийся удалённый пользователь обладает избыточными правами – например, правами локального администратора, – что, очевидно, является серьезной проблемой обеспечения информационной безопасности систем промышленной автоматизации.

Из интервью с инженерами и операторами различных промышленных систем, которые мы обследовали, и на основе анализа пользовательской документации средств АСУ мы выяснили, что RAT чаще всего используются в промышленных сетях в следующих сценариях:

1. Для управления/мониторинга HMI с АРМ оператора (в том числе для вывода информации на большой экран);
2. Для управления/обслуживания HMI с АРМ инженера;
3. Для управления SCADA с АРМ оператора;
4. Для обслуживания SCADA с АРМ инженера или компьютера подрядчика/вендора (из внешней сети);
5. Для подключения множества операторов к одному АРМ оператора (архитектура а-ля тонкий клиент для экономии расходов на лицензии софта для АРМ);
6. Для подключения из технологической сети через HMI к компьютеру в офисной сети с целью выполнения на нем различных задач (просмотр почты, доступ в интернет, работа с офисными документами).

Часть из описанных сценариев указывает на то, что использование RAT в технологической сети может быть объяснено производственной необходимостью, т.е. отказ от использования RAT так или иначе потребует некоторых изменений рабочих процессов. В то же время надо понимать, что атака на плохо защищенный RAT легко может стать причиной нарушения технологического процесса, и принимать решения по использованию RAT в технологической сети с учётом этой угрозы. Пристальный контроль за использованием RAT в технологической сети позволит уменьшить поверхность атаки и снизить риск заражения систем, администрируемых удаленно.

ТОП 20 стран по проценту компьютеров АСУ (по отношению ко всем компьютерам АСУ в стране), на которых в течение первого полугодия 2018 года хотя бы раз использовались RAT



Сценарии установки RAT на компьютеры АСУ

Согласно результатам нашего исследования, чаще всего встречаются три сценария установки RAT на компьютеры АСУ:

1. Установка дистрибутивов ПО для АСУ, содержащих RAT (из отдельных дистрибутивов или из инсталляционного пакета ПО АСУ). RAT, входящие в дистрибутивы ПО для АСУ, составляют 18,6% от всех обнаруженных нами RAT на компьютерах АСУ, защищаемых продуктами «Лаборатории Касперского».

Процент RAT, установленных вместе с продуктами АСУ, среди всех обнаруженных RAT на компьютерах АСУ

2. Умышленная установка RAT персоналом или подрядчиками – сетевыми администраторами, инженерами, операторами, сотрудниками компаний-интеграторов. Мы не берёмся судить о легитимности данных установок. По опыту проведённых обследований технологической сети и расследования инцидентов можем сказать, что далеко не все из них согласуются с политикой ИБ организации, и не обо всех из них известно ответственным лицам на предприятиях.
3. Скрытая установка RAT вредоносным ПО. Например, как это было в недавней атаке, которую мы расследовали (см. ниже).

Угрозы RAT для ICS

Угрозы, связанные с использованием RAT в промышленных сетях, не всегда так же очевидны, как и причины, по которым их используют.

Большинство RAT, обнаруженных нами на промышленных системах, обладают следующими характеристиками, значительно снижающими уровень защищенности системы-хоста:

- Используются повышенные привилегии – серверная часть RAT часто запускается в виде сервиса с привилегиями системы, т.е. NT SYSTEM;
- Отсутствует возможность ограничения локального доступа к системе / действий клиента;
- Однофакторная аутентификация;
- Отсутствует логирование действий клиента;
- Наличие уязвимостей (наш отчёт о результатах поиска уязвимостей нулевого дня в популярных системах RAT, используемых, в том числе, в продуктах многих производителей средств АСУ, будет опубликован до конца года);
- Используются Relay серверы (для обратного подключения), позволяющие RAT обходить ограничения NAT и межсетевого экрана на периметре сети.

Наиболее критичной проблемой RAT является использование повышенных привилегий и отсутствие возможности их ограничения (или ограничения локального доступа удаленного пользователя). На практике это означает, что, если злоумышленник (или вредоносное ПО) получит доступ к компьютеру удаленного пользователя, украдет данные аутентификации (логин/пароль), внедрится в активную сессию удаленного управления или успешно атакует уязвимость в серверной части RAT, то в результате получит безграничный контроль над системой АСУ. Использование Relay серверов для обратного подключения также открывает злоумышленникам возможность для подключения к этим RAT из любой точки мира.

Для RAT, встроенных в дистрибутивы ПО для ICS, характерны и другие проблемы:

- Используемые компоненты и дистрибутивы RAT редко обновляются (даже при выпуске новых версий ICS дистрибутивов), что увеличивает вероятность наличия в них уязвимостей;
- В подавляющем большинстве случаев используется пароль «по умолчанию», либо жестко внедренный в код RAT производителем ПО для ICS, либо указанный в документации как «рекомендованный».

RAT являются легитимным ПО и часто используются в промышленной сети, поэтому атаки с использованием RAT крайне трудно отличить от легитимной активности. Кроме того, поскольку об установленных средствах RAT часто не известно службе ИБ и прочим лицам, ответственным за безопасность АСУ, конфигурация RAT в большинстве случаев не анализируется при проверках безопасности промышленной сети. Поэтому очень важно контролировать кто, когда и зачем использует RAT в промышленной сети, полностью исключив возможность использования RAT без ведома сотрудников, ответственных за информационную безопасность технологической сети.

Атаки злоумышленников с использованием RAT

Все, что было описано выше, относится к потенциальным угрозам, связанным с использованием RAT.

Проанализировав статистику KSN, нам удалось выявить ряд случаев атак и попыток заражения вредоносным ПО с использованием RAT, установленных на компьютерах АСУ. Чаще всего атаки происходили следующим образом (в порядке уменьшения частоты атак):

1. Сетевая атака типа «bruteforce» из локальной сети или интернета, направленная на подбор логина/пароля;
2. Злоумышленник или вредоносное ПО через RAT загружает и запускает вредоносное ПО, используя украденные или подобранные данные аутентификации;
3. Удаленный пользователь (скорее всего, введенный в заблуждение злоумышленниками легитимный пользователь) через RAT загружает и запускает на компьютере АСУ троянское ПО, замаскированное под офисные документы, непроизводственное ПО (игры, ПО для мультимедиа и т.д.), Crack/Keygen для офисного, прикладного или промышленного ПО;
4. Сетевая атака из локальной сети или интернета на серверную часть RAT с использованием эксплойтов.

Сетевые атаки типа «bruteforce» (подбор логина/пароля) встречаются чаще всего – для их реализации не требуется специфичных знаний и навыков, а необходимое для атаки ПО находится в открытом доступе.

На основе имеющихся данных невозможно судить о том, кто именно и с какой целью подключается к серверной части RAT, установленной на компьютере АСУ, – легитимный пользователь, злоумышленник или вредоносное ПО. Поэтому мы можем лишь догадываться о том, является ли эта активность направленной атакой, попыткой саботажа или ошибкой клиента.

Сетевые атаки из интернета, скорее всего, производились злоумышленниками с использованием вредоносного ПО, инструментов для проведения тестирования на проникновение или ботнет-сетей.

Сетевые атаки из локальной сети могут указывать на присутствие в сети злоумышленника (в том числе инсайдера). Или на то, что в локальной сети находится скомпрометированный компьютер, который либо заражен вредоносным ПО, либо используется злоумышленником в качестве точки присутствия (в случае, если данные аутентификации были скомпрометированы ранее).

Атаки на промышленные предприятия с использованием RMS и TeamViewer

В первой половине 2018 года Kaspersky Lab ICS CERT зафиксировал очередную волну рассылок вредоносных фишинговых писем, замаскированных под легитимные коммерческие предложения. Атаки были нацелены преимущественно на промышленные компании на территории РФ, но такая же тактика и инструменты могут использоваться в атаках на промышленные компании в любой стране мира.

Вредоносная программа, используемая в этих атаках, устанавливает в систему легитимное ПО для удаленного администрирования — TeamViewer или Remote Manipulator System/Remote Utilities (RMS). В обоих случаях для внедрения вредоносного кода в процесс легитимного ПО системную DLL подменяют на вредоносную. Это позволяет злоумышленникам получать удаленный контроль над зараженными системами. Используются различные техники, позволяющие скрыть заражение системы и активность установленного ПО.

При необходимости злоумышленники загружают на систему дополнительный набор вредоносного ПО, сформированный с учетом особенности атаки на каждую жертву. Такой набор может содержать шпионские программы (Spyware), дополнительные утилиты удаленного администрирования, расширяющие контроль злоумышленников на зараженных системах, вредоносное ПО для эксплуатации уязвимостей в ОС и прикладном ПО, а также утилиту Mimikatz, позволяющую получить данные аккаунтов учетных записей Windows.

По имеющимся данным, основной целью атакующих является кража денежных средств со счетов организации, но возможные сценарии атаки не ограничиваются похищением денежных средств. Злоумышленники в процессе атаки крадут конфиденциальные данные организации, её партнёров и клиентов, скрыто наблюдают за действиями сотрудников компании, проводят запись аудио- и видео- данных с устройств, подключенных к зараженной машине. Очевидно, что, помимо финансовых потерь, данные атаки приводят к утечке конфиденциальных данных организации.

Множественные атаки на автомобилестроительную компанию

Весьма показательным примером атак по сценарию 2 были атаки, направленные на технологическую сеть автомобилестроительной/сервисной компании, в частности – компьютеры, предназначенные для диагностики двигателей и бортовых систем грузовиков и тяжелой техники. Множественные попытки таких атак были предотвращены продуктами «Лаборатории Касперского».

По меньшей мере на одном из компьютеров в технологической сети компании был установлен и периодически использовался RAT. Начиная с конца 2017 года на этом компьютере было заблокировано множество попыток запуска различных вредоносных программ, запускаемых через RAT. В течение нескольких месяцев регулярно – 2-3 раза в неделю в различное время – производились попытки заражения. С учётом другой косвенной информации, имеющейся в нашем распоряжении, мы полагаем, что данные аутентификации RAT были скомпрометированы и использовались злоумышленниками (или вредоносным ПО) для атаки на компьютеры этой компании из интернета.

Злоумышленники, получив доступ через RAT к инфраструктуре потенциальной жертвы, упорно пытались подобрать упаковщик вредоносного кода таким образом, чтобы обойти антивирусную защиту.

Часть заблокированных объектов являются модификациями сетевого червя, детектируемого продуктами «Лаборатории Касперского» как Net-Worm.Win32.Agent.pm. Примечательно, что при запуске данный червь незамедлительно начинает распространение по локальной сети, используя эксплойты для уязвимостей MS17-010 – те самые, которые были опубликованы ShadowBrokers весной 2017 и использовались в атаках нашумевших шифровальщиков WannaCry и ExPetr.

Другая часть заблокированных вредоносных объектов относится к троянскому ПО семейства Nymaim. Вредоносные программы данного семейства часто являются загрузчиками модификаций ботнет-агента семейства Necus, который, в свою очередь, часто использовался для заражения компьютеров вымогателями семейства Locky.

Заключение

Средства удаленного администрирования широко используются в промышленных сетях для мониторинга, управления и обслуживания АСУ. Возможность проводить манипуляции удаленно существенно снижает стоимость обслуживания АСУ, но, в то же время, неконтролируемый удаленный доступ, невозможность 100% верификации легитимности удаленного клиента, а также наличие уязвимостей в коде и конфигурации RAT значительно увеличивают поверхность атаки. Вместе с тем, RAT, наряду с другими легитимными инструментами, всё чаще используются злоумышленниками для сокрытия вредоносной активности и затруднения атрибуции.

Для снижения рисков кибератак с использованием RAT мы рекомендуем в первую очередь:

- Провести аудит использования прикладных и системных средств удалённого администрирования внутри технологической сети, таких как VNC, RDP, TeamViewer, RMS/Remote Utilities. Удалить все средства удалённого администрирования, не обусловленные производственной необходимостью.
- Провести аудит и отключить средства удалённого администрирования, поставляемые вместе с ПО АСУ ТП (обратитесь к документации на соответствующее ПО за детальными инструкциями), если в их использовании нет производственной необходимости.
- Обеспечить пристанный контроль и логирование событий для каждого сеанса удаленного управления, обусловленного производственной необходимостью, – по умолчанию, удаленный доступ должен быть запрещен, включать удаленный доступ необходимо только по заявке и только на определенный промежуток времени.

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