

APT-атаки на топливно- энергетический комплекс России

Обзор тактик и техник

2019

Содержание

Что такое АРТ-атака	2
Об исследовании	4
Не только фишинг	5
Получение привилегий	5
Закрепление в сети	6
Как хакеры обходят защиту	7
В поисках администратора домена	7
На пути к технологической сети	8
Кража данных	9
Связь с командным центром	10
Разрушительные последствия	10
Как распознать АРТ-атаку	11
Тепловая карта тактик и техник АРТ-атак (группировки, атакующие компании топливно- энергетического комплекса в России)	12
Тепловая карта тактик и техник АРТ-атак (все группировки, атакующие компании в России)	13

Что такое АРТ-атака

Организации топливно-энергетического комплекса (ТЭК) поддерживают работу промышленных и оборонных производств, других стратегических объектов. Энергетика обеспечивает жизнедеятельность городов, а это больницы, телекоммуникационные станции, правительственные учреждения, другие социально значимые объекты. Нарушение энергоснабжения таких объектов может привести к дестабилизации обстановки в отдельно взятом городе или даже стране в целом. Аварии на объектах ТЭК всегда имеют широкий общественный резонанс и могут привести к экологическим катастрофам и человеческим жертвам.

Разрушительное воздействие на инфраструктуру и промышленный шпионаж — это основные цели киберпреступников, атакующих ТЭК. Для осуществления подобных операций злоумышленникам требуется высокая техническая квалификация и правильная организация. Целевые атаки, которые проводятся хорошо подготовленными преступными группировками, принято называть атаками типа *advanced persistent threat* (APT), а группы киберпреступников, которые стоят за ними, — АРТ-группировками.

Атака типа *advanced persistent threat* (АРТ-атака) — это хорошо организованная, тщательно спланированная кибератака, которая направлена на конкретную компанию или целую отрасль. За АРТ-атакой как правило стоят преступные группировки, имеющие значительные финансовые ресурсы и технические возможности.

При подготовке исследования мы попросили специалистов рассказать, какие средства используются в их организациях для защиты от кибератак, и оценить, смогут ли организации справиться со сложными угрозами¹. Опрос проводился на сайте компании Positive Technologies, среди аудитории портала SecurityLab.ru² и в ряде отраслевых сообществ, в которые входят эксперты по ИТ и ИБ из различных сфер отечественного бизнеса. По мнению 60% респондентов, представляющих ТЭК и промышленность, риск успешной кибератаки является критически опасным для их компаний, но при этом всего 11% участников опроса уверены, что компания сможет противостоять АРТ. Большинство полагает, что целями АРТ-группировки при атаке на их компании будут являться нарушение технологических процессов и вывод из строя инфраструктуры. Больше половины респондентов (55%) сообщили, что организации, в которых они работают, уже становились жертвами кибератак. Каждый четвертый участник отметил, что одним из последствий таких атак становились простые инфраструктуры.

-
1. В опросе приняли участие 306 респондентов. Доля представителей ТЭК и промышленности составила 18,6%.
 2. Сайт SecurityLab.ru — один из лидеров российского интернета в сфере информационной безопасности. Ежемесячная аудитория портала насчитывает около полумиллиона посетителей, большая часть из которых — программисты, специалисты по ИТ и ИБ, руководители соответствующих отделов.

По каким причинам ваша компания может стать целью АРТ-группировок?

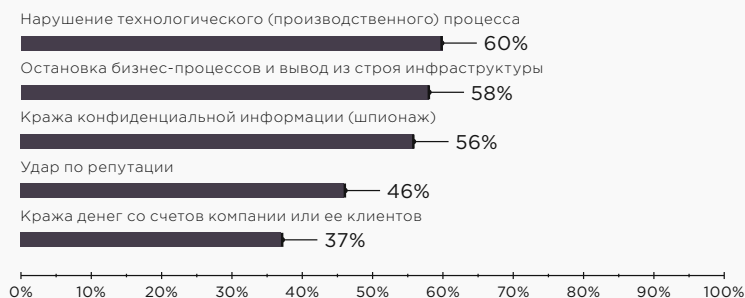


Рисунок 1. Топ-5 предполагаемых целей АРТ-группировок
(доля респондентов, представляющих ТЭК и промышленность)

С какими последствиями кибератак сталкивалась компания?

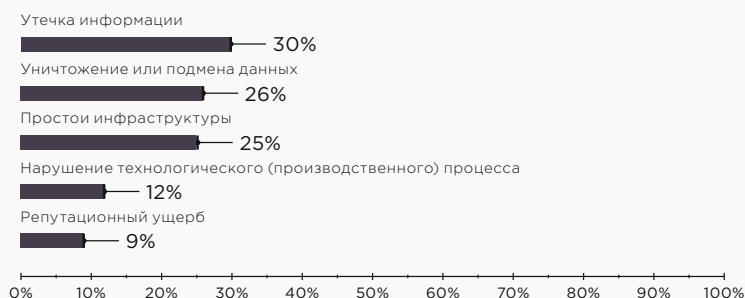


Рисунок 2. Топ-5 последствий кибератак
(доля респондентов, представляющих ТЭК и промышленность)

Исходя из результатов опроса можно также сделать вывод, что во многих компаниях используются базовые средства защиты, которые не дают возможности провести тщательный анализ происходящих в инфраструктуре событий и распознать подозрительную активность.

Какие технические средства защиты информации применяются в компании?

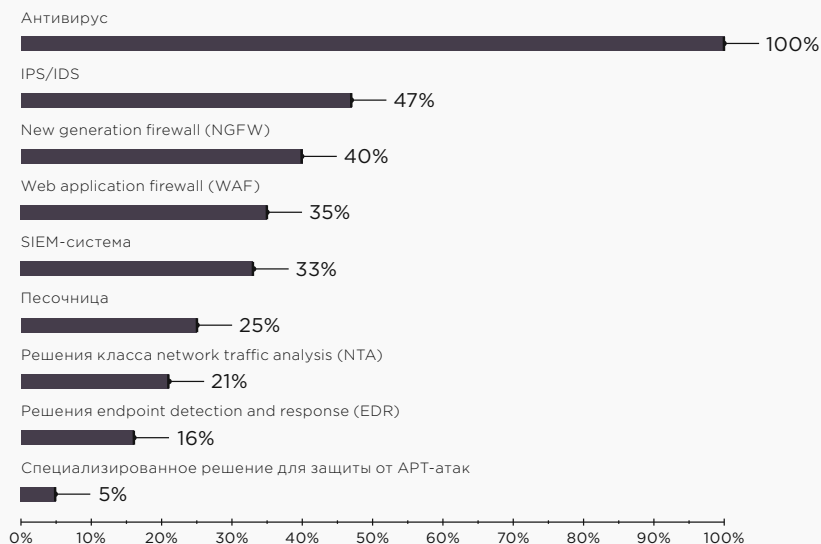


Рисунок 3. Используемые средства защиты
(доля респондентов, представляющих ТЭК и промышленность)

Для того, чтобы построить эффективную стратегию защиты, необходимо понимать, как действуют АРТ-группировки и какие мотивы лежат в основе их поведения. В одном из последних [исследований](#) мы рассказывали об инструментах злоумышленников и посчитали примерную стоимость проведения атаки. В этом отчете мы рассмотрим, как именно АРТ-группировки атакуют российские компании из топливно-энергетического комплекса: какие техники используют, чтобы проникнуть в инфраструктуру, как действуют внутри, а также выясним, на каких этапах можно выявить атаку.

Об исследовании

По нашим оценкам, в последние два года³ кибератаки в отношении российских компаний проводили 22 АРТ-группировки. Девять из этих группировок атаковали организации топливно-энергетического комплекса.



Рисунок 4. Распространенные категории жертв
(доля атакующих АРТ-группировок)

В целом атаки развиваются по одному сценарию и похожи между собой. Но у каждой преступной группировки формируется собственный шаблон поведения. Он зависит от состава участников, их навыков, предыдущего опыта, наличия доступа к конкретным инструментам. По мере развития группировка совершенствует свои методы, отбирая наиболее подходящие и отказываясь от бесперспективных стратегий.

Поведение АРТ-группировок описано в соответствии с [MITRE ATT&CK](#) (Enterprise). В конце отчета мы привели тепловые карты (heat maps), основанные на матрице MITRE ATT&CK, где отражены наиболее часто используемые техники атак на топливно-энергетические компании.

MITRE ATT&CK — это база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных АРТ-атак. Представляет собой структурированный в виде наглядной таблицы список тактик, для каждой из которых указан список возможных техник. Позволяет структурировать знания об АРТ-атаках и категоризировать действия злоумышленников.

Данные для анализа получены в ходе расследований киберинцидентов и работ по ретроспективному анализу событий безопасности в инфраструктуре различных компаний, а также в ходе постоянного отслеживания активности действующих сегодня АРТ-группировок экспертами PT Expert Security Center. Дополнительно использовалась информация из общедоступных отчетов о деятельности АРТ-группировок, подготовленных ведущими компаниями в области ИБ.

3. Опыт экспертов Positive Technologies показывает, что интервал до двух лет позволяет составить наиболее актуальную картину тактик и техник атаки.

Не только фишинг

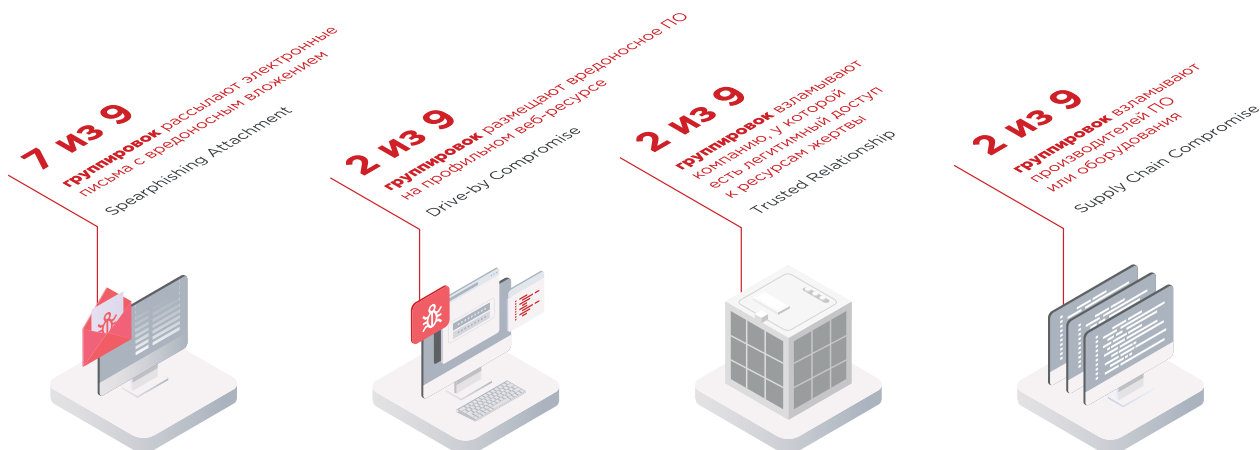
Семь из девяти рассматриваемых группировок проникают в инфраструктуру компаний путем рассылки фишинговых писем. Злоумышленники отправляют сотрудникам компании электронные письма, которые замаскированы под обычную деловую переписку или рассылку, например под официальное приглашение на профильную конференцию или письмо от партнера. Письмо содержит документ в одном из популярных форматов. При открытии этого документа на компьютере сотрудника начинает выполняться вредоносный код.

Перед атакующими стоит задача проникнуть в инфраструктуру конкретной компании, поэтому они будут применять разные методы до тех пор, пока не достигнут своей цели. Если по каким-то причинам фишинг не срабатывает, группировка переходит к другим техникам. Более сложные техники требуют больше времени, усилий или денежных вложений, но нужно учитывать, что за киберпреступниками, атакующими компании ТЭК, могут стоять организации, обладающие значительными финансовыми возможностями.

Пять из девяти группировок начинают атаку с компрометации ресурсов сторонних организаций, уровень защищенности которых ниже, чем у целевых. Это техники drive-by compromise, supply chain compromise и trusted relationship.

При проведении атаки методом drive-by compromise, или watering hole, злоумышленники взламывают отраслевой сайт, который часто посещают сотрудники компании, и размещают на нем вредоносный код. Когда пользователь заходит на зараженный сайт, на его компьютер загружается хакерская программа. Схожая по своей сути техника supply chain compromise (атака через цепочку поставщиков) — это внедрение вредоносного кода в программные или аппаратные компоненты известного производителя, например распространение вредоносного кода вместе с обновлениями ПО.

Под техникой trusted relationship понимается взлом инфраструктуры сторонней компании, у сотрудников которой имеется легитимный доступ к ресурсам жертвы. К примеру, дочерние предприятия могут стать первым звеном в цепочке атаки на головную организацию, а в других случаях атака может начинаться со взлома компании, обеспечивающей техническую поддержку.



Получение привилегий

После проникновения в инфраструктуру дальнейшими шагами злоумышленников будут установка канала связи с командным центром, закрепление в инфраструктуре, сбор информации о сети и поиск ключевых узлов. Но для всех этих действий привилегий обычного сотрудника недостаточно. Чтобы продвигаться в сети, нужно сначала повысить привилегии локально на зараженной рабочей станции. Часто используемый способ — внедрение кода

вредоносной программы в память легитимного процесса, запущенного с максимальными правами. Злоумышленники могут также воспользоваться уязвимостями, которые присутствуют в установленном ПО или ОС.

Привилегии локального администратора дают возможность запускать любые программы, в том числе для извлечения учетных записей из памяти ОС, и выполнять другие действия, необходимые для успешного развития атаки и сокрытия ее следов.

Закрепление в сети

APT-группировки проводят деструктивные атаки не сразу после проникновения. Они могут годами контролировать все системы предприятия, не предпринимая никаких разрушительных действий, а лишь похищая важные сведения и ожидая подходящего момента, чтобы приступить к атаке. Поэтому основная цель таких группировок — длительное скрытое присутствие в инфраструктуре. Так, в ходе расследования одного из инцидентов наши эксперты выяснили, что группировка TaskMasters находилась в инфраструктуре компании-жертвы как минимум 8 лет.

Преступникам необходимо как можно надежнее закрепиться на узлах сети, чтобы обычные действия пользователей вроде перезагрузки ОС или смены паролей не повлекли за собой потерю доступа к захваченным ресурсам. Чаще всего (89% случаев) злоумышленники добавляют свои программы в автозагрузку (registry run keys / startup folder) под видом легитимных, создавая для этого новые сервисы (new service) либо модифицируя существующие (modify existing service). Таким образом они обеспечивают запуск вредоносного ПО при каждой перезагрузке компьютера. Создание новых задач, выполняющихся по расписанию (scheduled task), — тоже распространенный способ закрепления, который применяют четыре из девяти группировок.

Злоумышленники предусматривают также резервные варианты для восстановления доступа на случай, если основные каналы связи будут потеряны. Например, группировки TaskMasters и APT27 оставляли с этой целью веб-шеллы на внешних ресурсах компаний. Запасные пути могут быть хорошо замаскированы. В случае TaskMasters окно доступа к управлению веб-шеллом выглядело как стандартная страница ошибки веб-сервера. Чтобы получить доступ и выполнять команды, необходимо было ввести пароль, но поле для ввода пароля было скрыто и отображалось только при двойном нажатии на определенное слово из текста ошибки.



APT-группировки отличаются высоким уровнем технической подготовки, поэтому способы закрепления бывают неординарными. Комплект инструментов группы Equation содержал модули, предназначенные для модификации прошивок жестких дисков (component firmware) и внедрения в них вредоносного кода. Такие закладки способны пережить даже форматирование жесткого диска и переустановку ОС.

Как хакеры обходят защиту

Преступные группировки используют многочисленные техники для того, чтобы их присутствие оставалось незамеченным. Данные, передаваемые между командным сервером и зараженными узлами, шифруются и обфусцируются, чтобы избежать обнаружения по известным сигнатурам. В 67% случаев в этих целях используются стандартные алгоритмы, например группировки TaskMasters и Lazarus применяли алгоритм шифрования RC4 и алгоритм кодирования Base64. В ходе кампании Poking the Bear злоумышленники разбивали управляющие команды символом «_», чтобы обмануть системы обнаружения вторжений (IDS), и передавала их в таком виде: «ST_A_RT_FI_LE». Обфускация применяется и с целью обхода антивирусного ПО на рабочих станциях: во втором квартале 2019 года TaskMasters использовала VMProtect для защиты своего трояна.

Распространенной практикой стало использование бестелесных скриптов, которые запускаются сразу в оперативной памяти, не оставляя следов на жестком диске. Как минимум пять из девяти группировок запускают вредоносные скрипты при помощи инструмента PowerShell.

В поисках администратора домена

Злоумышленникам необходимо выявить в корпоративной сети ключевые узлы, то есть компьютеры администраторов, руководства, инженеров, а также рабочие станции и сетевое оборудование, с которых возможно настроить доступ в технологические сети предприятия, чтобы управлять промышленным оборудованием. Для этого нужна возможность свободно перемещаться между компьютерами и даже между разными сегментами сети, а значит, нужны высокие привилегии в системе.



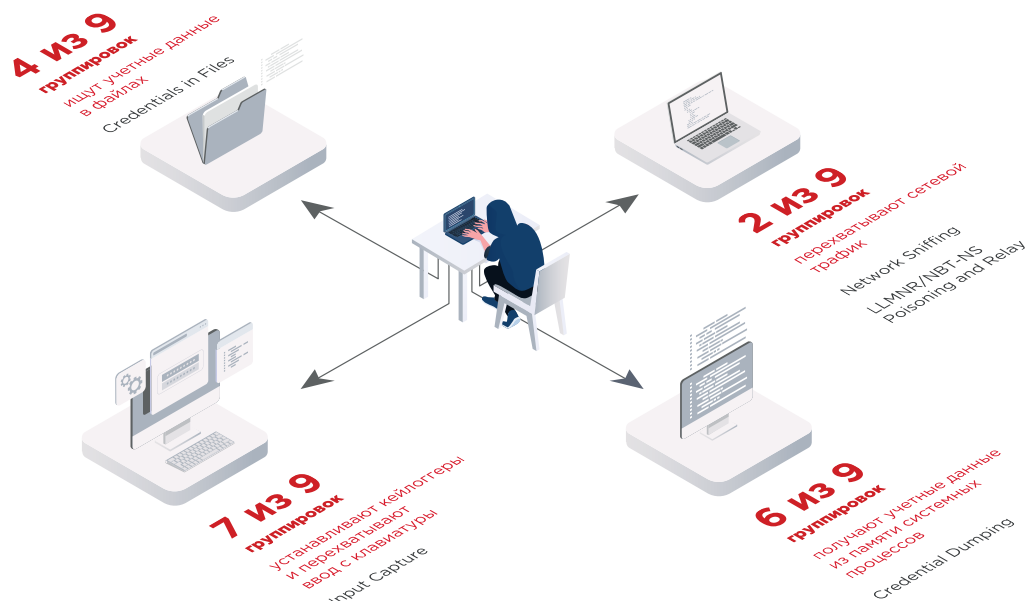
У кого в сети самые высокие привилегии

Компьютеры в инфраструктуре объединены в группы — домены. В каждом домене максимальными привилегиями обладают администраторы: они имеют доступ к любому компьютеру и могут производить любые изменения в сети. Поэтому злоумышленники попытаются получить привилегии администратора домена, то есть скомпрометировать его учетную запись.

В поисках администратора домена злоумышленники будут последовательно перемещаться между узлами сети и собирать учетные данные всех пользователей. Подключение к рабочим станциям производится чаще всего по протоколу RDP или при помощи распространенных утилит для администрирования.

Существует множество способов узнать учетные данные пользователей. Семь из девяти группировок устанавливают на компьютеры кейлоггеры — специальные программы для перехвата введенной с клавиатуры информации. Пароли пользователей могут также

храниться в служебных файлах или ключах реестра. Учетные данные можно получить и непосредственно из памяти системных процессов, используя технику credential dumping, которая заключается в копировании памяти процессов и извлечении из нее хеш-сумм паролей. Причем для получения доступа к рабочим станциям не обязательно иметь пароль в открытом виде: техники pass the hash и pass the ticket позволяют подключиться к удаленному узлу при наличии хеш-суммы. В ход могут пойти и более сложные методы; так, среди инструментов группировки TaskMasters наши эксперты обнаружили ПО для перехвата сетевого трафика, в том числе передаваемых по сети учетных данных.



Рано или поздно злоумышленники доберутся до компьютера, на котором авторизовался администратор домена, и его учетная запись будет скомпрометирована. С этого момента они смогут подключаться к любому компьютеру, беспрепятственно перемещаться по сети и даже вносить изменения в ее конфигурацию.

На пути к технологической сети

В компаниях топливно-энергетического комплекса сеть, как правило, разделена на корпоративный сегмент и технологический. В корпоративном сегменте находятся рабочие станции сотрудников, чья деятельность не связана непосредственно с управлением промышленным оборудованием. Именно здесь, скорее всего, окажутся злоумышленники сразу после проникновения в инфраструктуру. В корпоративной сети АРТ-группировку будут интересовать компьютеры, на которых хранится конфиденциальная информация — научные разработки, производственные регламенты, финансовая информация.

Но на корпоративном сегменте группировка не остановится, ведь основная цель при атаке на топливно-энергетический комплекс — возможность влиять на производственные процессы. Соответственно, злоумышленники постараются проникнуть в технологический сегмент сети, откуда осуществляется управление промышленными системами. Они попытаются получить доступ к АСУ ТП, SCADA, промышленным контроллерам, системам автоматических блокировок, терминалам релейной защиты и прочим технологическим ресурсам, в зависимости от преследуемых целей. Например, при атаке на электрическую

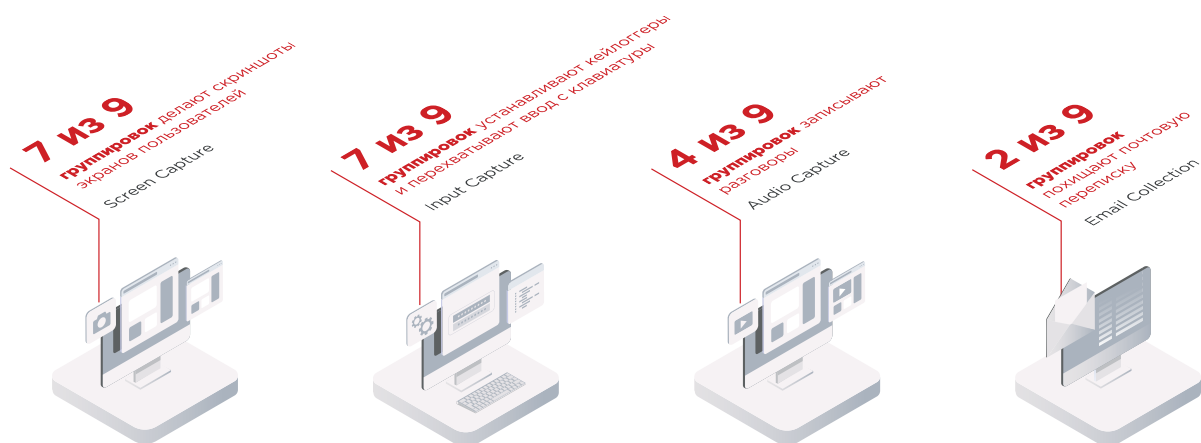
подстанцию вмешательство злоумышленников в логику работы защитной автоматики в случае нештатной ситуации может привести к отключению подачи электроэнергии потребителям. Взяв под контроль ключевые узлы сети, группировка скорее всего будет сохранять скрытое присутствие до тех пор, пока от организаторов кибератаки не поступит команда перейти к активным действиям. Однако не исключено, что изучив надежные пути доступа к целевым объектам, злоумышленники покинут сеть, чтобы снизить риск обнаружения, и вернуться позже.

Технологический сегмент должен быть изолирован от корпоративной сети, но на практике так бывает не всегда. Удаленный доступ в изолированные сегменты может осуществляться с отдельных компьютеров администраторов, которые создают специальные каналы связи для упрощения своих задач. Также доступ может быть предоставлен и другим сотрудникам: директорам, инженерам. Согласно [нашему исследованию](#), в 64% компаний существуют каналы подключения к технологической сети с компьютеров администраторов или руководства. Не исключены и ошибки при настройке межсетевых экранов, например наличие открытых нестандартных портов, по которым можно подключиться к промышленным ресурсам. Недостаточная фильтрация сетевого трафика выявлялась в 45% промышленных компаний. Изучая инфраструктуру, злоумышленники собирают информацию о сетевой конфигурации (system network configuration discovery) и сетевых соединениях (system network connections discovery), чтобы выявить узлы, с которых есть доступ к компонентам технологической сети. Кроме того, обладая высокими привилегиями в инфраструктуре, злоумышленники могут самостоятельно изменять параметры межсетевых экранов и строить сложные тоннели между узлами в разных подсетях — для создания собственных каналов подключения к технологическому сегменту.

В некоторых компаниях технологическая сеть полностью отделена от корпоративной. Это значительно осложняет ход атаки, но отнюдь не означает, что доступ киберпреступников к технологической сети исключен. В таком случае злоумышленники могут перейти к другим методам. Техника replication through removable media, то есть перемещение по сети с использованием съемных устройств, применялась в атаках [группировки Equation](#). Троян Fanny создавал на USB-накопителе скрытый раздел, куда записывались команды, полученные от управляющего сервера. Когда сотрудник подключал флешку к компьютеру в изолированной сети, эти команды выполнялись автоматически. Группировка использовала уязвимость нулевого дня в обработчике LNK-файлов, поэтому отключение автозапуска на съемных устройствах не могло остановить распространение трояна. Собранные данные снова записывались в скрытый раздел флешки, а затем, при подключении к компьютеру, имеющему выход в интернет, данные передавались на сервер злоумышленников.

Кража данных

Получив доступ к важным узлам сети, преступники приступают к сбору ценной информации. Если компьютер является рабочей станцией оператора промышленной системы, то злоумышленники попытаются найти пароли для подключения к системам управления оборудованием. В комплекте инструментов хакеров обязательно присутствуют модули, которые выполняют шпионские функции — делают скриншоты и видеозаписи экрана, записывают звук с микрофона и перехватывают ввод данных с клавиатуры. Впрочем, необязательно использовать сложные инструменты для того, чтобы подключиться к системам управления. Как показывает [наше исследование](#), в 82% компаний пароли хранятся в файлах конфигурации, резервных копиях систем или обычных документах Microsoft Word, а в 36% компаний можно обнаружить сохраненные сессии для удаленного подключения.



На компьютерах руководства, бухгалтеров или инженеров злоумышленники будут искать научные разработки, информацию о промышленных системах, договоры, финансовую документацию, деловую переписку. К примеру, утилита Pst из инструментария группировки [TaskMasters](#) умеет извлекать электронные письма из файлов формата .pst, который используется в Microsoft Exchange Client, Windows Messaging и Microsoft Outlook.

Связь с командным центром

Управление ходом атаки осуществляется с внешнего сервера, который принято называть командным или управляющим. Обмен данными с командным сервером должен оставаться незаметным для администраторов и средств защиты. Для связи в 89% случаев используются распространенные протоколы прикладного уровня (standard application layer protocol), поскольку такой трафик проще скрыть в общем потоке. Также чаще используются стандартные сетевые порты (commonly used port), которые обычно не заблокированы межсетевым экраном. Чтобы внешние адреса, с которыми осуществляется соединение, не вызывали подозрений, в ходе киберкампании [Poking the Bear](#) злоумышленники регистрировали для командных серверов доменные имена, схожие с названиями ведущих российских энергетических компаний.

Командные серверы могут быть установлены и внутри инфраструктуры для снижения объема внешнего сетевого трафика и сокрытия управляющего трафика внутри сети. Группировка [TaskMasters](#) автоматизировала выполнение задач при помощи утилиты AtNow, которая позволяет запускать команды локально или на удаленных узлах по прошествии заданного интервала времени.

Разрушительные последствия

Конечной целью APT-группировки может являться разрушительное деструктивное воздействие на инфраструктуру в определенный момент, связанный с политическими или военными событиями. Главная опасность заключается в том, что атака может не просто вывести оборудование из строя, но и спровоцировать серьезную аварию, которая нанесет ущерб экологии или приведет к человеческим жертвам. Например, во время атаки на [нефтехимический завод](#) в Саудовской Аравии злоумышленники собирались не просто нарушить работу завода, а устроить на нем взрыв, и только ошибки в коде ПО помешали им это сделать.

Вернуться к нормальному функционированию после кибератаки может быть непросто. Злоумышленники могут намеренно осложнить восстановление инфраструктуры, например уничтожить резервные копии систем. Так, среди инструментов группировки [Lazarus](#)

присутствуют модули, которые специально предназначены для шифрования данных, удаления загрузочных записей, уничтожения структуры файловых систем и данных на жестких дисках.

Как распознать АРТ-атаку

Компании топливно-энергетического комплекса становятся целью АРТ-группировок, участники которых имеют высокую техническую квалификацию и хорошую финансовую поддержку, поэтому рано или поздно они найдут способ проникнуть в инфраструктуру. Так как предотвратить атаку крайне сложно, стратегия защиты должна строиться на том, чтобы выявить действия злоумышленников в сети до того, как они смогут причинить ущерб. Ситуация осложняется тем, что видимые признаки компрометации отсутствуют: из организации не исчезают деньги, технологические процессы не прерываются. Очень долго компания даже не подозревает о том, что находится под контролем АРТ-группировки. Злоумышленники могут годами тайно находиться в инфраструктуре, не предпринимая никаких действий и ожидая дальнейших указаний от организаторов кибератаки.

Базовых средств защиты, антивирусов или IDS, уже недостаточно для противодействия современным АРТ-атакам. На момент проведения кибератаки сопутствующие ей индикаторы компрометации могут быть еще неизвестны. Поэтому важно не только проводить мониторинг событий ИБ в реальном времени, но и при появлении информации о новых угрозах пересматривать события в инфраструктуре, которые происходили ранее. Такой подход называется ретроспективным, он позволяет выявить скрытое присутствие злоумышленников в системе и проанализировать цепочку атаки даже по прошествии нескольких лет.

Особый подход требуется и при защите технологического сегмента сети. Корректная сегментация, отсутствие каналов управления из корпоративной сети и строгое разграничение привилегий пользователей уже значительно усложняют проведение атаки. Чем надежнее защищена промышленная сеть, тем больше техник будут вынуждены применять злоумышленники, оставляя за собой следы в сетевом трафике и системных журналах. А в том, чтобы вовремя обнаружить эти следы и избежать разрушительных последствий кибератаки, могут помочь технические решения для мониторинга защищенности сети АСУ ТП, для своевременного выявления нарушения сегментации, нелегитимного трафика и попыток неавторизованного управления промышленными системами.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Stored Data Manipulation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Transmitted Data Manipulation
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Firmware Corruption
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Resource Hijacking
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Network Denial of Service
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Endpoint Denial of Service
	Mshtra	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshtra							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

80-100%60-80%40-60%20-40%0-20%

Тепловая карта тактик и техник АРТ-атак

(группировки, атакующие компании топливно-энергетического комплекса в России)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	AppCert DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Appinit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Ligon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Stored Data Manipulation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Transmitted Data Manipulation
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Firmware Corruption
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Resource Hijacking
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Network Denial of Service
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Endpoint Denial of Service
	Mshsta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Security Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Ligon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshsta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							



Тепловая карта тактик и техник АРТ-атак

(все группировки, атакующие компании в России)

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.