Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 11

habr.com/ru/articles/449654

Андрей Макеев

Командование и управление (Command and Control)

Ссылки на все части:

Раздел «Командование и управление» (*аббрев. — C2, C&C*) является заключительным этапом цепочки атаки, представленной в ATT&CK Matrix for Enterprise.

Командование и управление включает техники, с помощью которых противник коммуницирует с системами, подключенными к атакуемой сети и находящимися под его управлением. В зависимости от конфигурации систем и топологии целевой сети известно множество способов организации скрытого канала C2. Наиболее распространенные техники описаны под катом. Общие рекомендации по организации мер по предотвращению и обнаружению C2 выделены в отдельный блок и размещены в конце раздела.

Автор не несет ответственности за возможные последствия применения изложенной в статье информации, а также просит прощения за возможные неточности, допущенные в некоторых формулировках и терминах. Публикуемая информация является свободным пересказом содержания MITRE ATT&CK.

Распространенные порты (Commonly Used Port)

Система: Windows, Linux, macOS
Описание: Для того чтобы обойти брандмауэры и смешать вредоносный трафик с обычной сетевой активностью противник может поддерживать связь с атакуемой

системой через стандартные порты, обычно используемые штатными приложениями:

```
TCP: 80 (HTTP)
TCP: 443 (HTTPS)
TCP: 25 (SMTP)
TCP/UDP: 53 (DNS)
```

Примерами портов для организации сетевых соединений внутри вражеского анклава, например, между прокси-сервером и другими узлами) являются:

```
TCP/UDP: 135 (RPC)
TCP/UDP: 22
TCP/UDP: 3389
```

Связь через съемные носители (Communication Through Removable Media)

Система: Windows, Linux, macOS
Описание: Противник может организовать инфраструктуру C2 между физически изолированными узлами, используя съемные носители информации для передачи команд из системы в систему. Обе системы должны быть скомпрометированными. Система с интернет-соединением, вероятнее всего, будет скомпрометирована первой, а вторая система компрометируется в ходе бокового перемещения с помощью тиражирования вредоносного ПО через съемный носитель (см. Часть 8). Команды и файлы будут ретранслироваться из изолированной системы в систему с интернет-соединением, к которой противник имеет прямой доступ.

Рекомендации по защите: Отключите автозапуск съемных устройств. Запретите или ограничьте использование съёмных носителей на уровне политики организации. Организуйте аудит процессов, которые выполняются при подключении съемного носителя.

Подключение через прокси (Connection Proxy)

Система: Windows, Linux, macOS
Описание: Прокси-сервер может использоваться злоумышленником для перенаправления сетевого трафика между системами или в качестве посредника сетевых коммуникаций. Множество инструментов (например, HTRAN, ZXProxy и ZXPortMap) позволяют перенаправлять трафик или переадресовывать порты.

Понятие прокси может также охватывать доверительные отношения в одноранговых (p2p), ячеистых (mesh) сетях или доверенных соединениях между сетями. Сеть может быть внутри организации или между организациями с доверительными отношениями. Противник может использовать доверительные отношения в сети для

управления каналом C2, уменьшения числа одновременных исходящих сетевых подключений, обеспечения отказоустойчивости или использования доверенных соединений во избежание подозрений.

Собственный протокол командования и управления (Custom Command and Control Protocol)

Система: Windows, Linux, macOS
Описание: Злоумышленник может организовать канал C2 с помощью собственного сетевого протокола вместо инкапсуляции команд/данных в существующий стандартный протокол прикладного уровня. Вражеская реализация протокола C2 может имитировать известные протоколы или пользовательские протоколы (включая raw-sockets) поверх базовых протоколов, представленных в TCP/IP или ином стандартном сетевом стэке.

Собственный криптографический протокол (Custom Cryptographic Protocol)

Система: Windows, Linux, macOS
Описание: В целях скрытия трафика, передаваемого по каналу C2, противник может использовать собственный криптографический протокол или алгоритм шифрования. Простая схема, такая как XOR-шифрование простого текста с фиксированным ключом, даст шифротекст (хотя и очень слабый).

Собственные схемы шифрования злоумышленников могут различаться по сложности. Анализ и реверс-инжиниринг образцов вредоносного ПО может применятся для успешного обнаружения используемого алгоритма и ключа шифрования. Некоторые злоумышленники могут попытаться реализовать собственную версию хорошо известного криптографического алгоритма вместо реализации с помощью известной библиотеки, что может привести к непреднамеренным ошибкам в работе вражеского ПО.

Рекомендации по защите: Если вредоносное ПО использует собственное шифрование с симметричными ключами, то существует возможность получения алгоритма и ключа из образцов ПО с целью их использования для декодирования сетевого трафика и выявления сигнатур вредоносного ПО.

Кодировка данных (Data Encoding)

Система: Windows, Linux, macOS
Описание: Информация, передаваемая по каналу C2, кодируется с использованием стандартных систем кодировки данных. Использование кодировки данных заключается в соблюдении существующих спецификаций протокола и включает использование ASCII, Unicode, Base64, MIME, UTF-8 или других кодировок

двоичного текста и символов. Некоторые системы кодировки, например, gzip, дополнительно могут сжимать данные.

Обфускация данных (Data Obfuscation)

Система: Windows, Linux, macOS
Описание: Данные в канале C2 могут скрываться (но не обязательно с помощью шифрования) для того чтобы затруднить обнаружение и расшифровку передаваемого контента, а также сделать процесс коммуникации менее заметным и скрыть передаваемые команды. Существует множество методов обфускации, таких как добавление ненужных данных в трафик протокола, использование стеганографии, объединение легитимного трафика с трафиком C2 или использование нестандартной системы кодировки данных, например, модифицированной Base64 в теле сообщения HTTP-запроса.

Скрытие конечного адреса соединения (Domain Fronting)

Система: Windows, Linux, macOS
Описание: Суть Domain Fronting заключается в возможности скрытия реального адреса назначения HTTPs-пакета в CDNs-сетях (Content Delivery Netwoks).

Пример: Есть домен X и домен Y, которые являются клиентами одной CDNs. Пакет, в котором в TLS-заголовке указан адрес домена X, а в заголовке HTTP — адрес домена Y, скорее всего будет доставлен адресу домена Y, даже если сетевое взаимодействие между адресом источника и адресом назначения запрещено.

HTTPs-пакет содержит два набора заголовков: первый, TLS, находится в открытой части пакета, второй, HTTP — относится к шифрованной части пакета. При этом каждый заголовок имеет собственное поле для указания IP-адреса назначения. Суть Domain Fronting заключается в преднамеренном использовании разных доменных имен в поле «SNI» заголовка TLS и поле «Host» заголовка HTTP. Таким образом, в поле «SNI» указывается разрешенный адрес назначения, а в поле «Host» указывается целевой адрес доставки. Если оба адреса принадлежат одной CDNs, то при получении такого пакета маршрутизирующий узел может ретранслировать запрос на целевой адрес.

Существует ещё одна разновидность данной техники, называемая domainless fronting. В этом случае поле «SNI» (TLS-заголовок) преднамеренно оставляется пустым, что позволяет пакету достичь цели даже если CDN будет проверять совпадение полей «SNI» и «HOST» (если пустые поля «SNI» игнорируются).

Рекомендации по защите: Если есть возможность инспекции HTTPS трафика, то соединения, похожие на Domain Fronting, могут быть захвачены и проанализированы. Если осуществляется SSL-инспекция или трафик не

зашифрован, то поле «HOST» может быть проверено на совпадение с полем «SNI» или наличие указанного адреса в белых или черных списках. Чтобы реализовать Domain Fronting, противнику, вероятно, потребуется развернуть дополнительные инструменты в скомпрометированной системе, инсталляцию которых можно предотвратить с помощью установки локальных средств защиты хоста.

Запасные каналы (Fallback Channels)

Система: Windows, Linux, macOS
Описание: В целях обеспечения надежности канала управления и во избежание превышения пороговых значений передаваемых данных злоумышленники могут использовать резервные или альтернативные каналы связи, если основной канал C2 скомпрометирован или недоступен.

Многоступенчатые каналы (Multi-Stage Channels)

Система: Windows, Linux, macOS
Описание: Злоумышленники могут создать многоступенчатые каналы C2, которые используются в различных условиях или для определенных функций. Использование нескольких ступеней может запутать и обфусцировать канал C2 тем самым затруднив его обнаружение.

Средства RAT, запущенные на целевом хосте, инициируют соединение с сервером C2 первой ступени. Первая ступень может иметь автоматизированные возможности для сбора основной информации о хосте, запуска инструментов обновления и загрузки дополнительных файлов. Далее может быть запущен второй инструмент RAT для перенаправления хоста на сервер C2 второй ступени. Вторая ступень C2, вероятнее всего, будет полнофункциональной и позволит противнику взаимодействовать с целевой системой через revers shell и дополнительные функции RAT.

Ступени C2, скорее всего, будут размещены отдельно друг от друга без пересечения их инфраструктуры. Загрузчик также может иметь резервную обратную связь первой ступени или запасные каналы на случай, если исходный канал первой ступени обнаружен и заблокирован.

Рекомендации по защите: Инфраструктура C2, используемая для организации многоступенчатых каналов может быть заблокирована, если о ней заранее известно. Если в трафике C2 присутствуют уникальные сигнатуры, то они могут быть использованы для идентификации и блокирования канала.

Многократное проксирование (Multi-hop Proxy)

Система: Windows, Linux, macOS

Описание: Чтобы замаскировать источник вредоносного трафика противник может использовать цепочку из нескольких прокси-серверов. Как правило, защищающая сторона сможет определить только последний прокси. Применение мультипроксирования делает идентификацию исходного источника вредоносного трафика более сложной, требуя от защищающейся стороны отслеживания вредоносного трафика через несколько прокси-серверов.

Рекомендации по защите: Трафик к известным анонимным сетям (типа Tor) и инфраструктурам C2 может быть заблокирован посредством организации черного и белого списков. Однако, стоит обратить внимание, что такой способ блокировки можно обойти с помощью техник подобных Domain Fronting.

Многополосная связь (Multiband Communication)

Система: Windows, Linux, macOS
Описание: Некоторые противники могут разделить канал передачи данных C2 между различными протоколами. Входящие команды могут передаваться по одному протоколу, а исходящие данные по-другому, что позволяет обойти определенные ограничения брандмауэра. Разделение может быть и случайным, чтобы избежать предупреждений о превышении пороговых значений для любого отдельного сообщения.

Рекомендации по защите: Анализируйте содержимое пакетов, чтобы обнаружить соединения, которые не соответствуют ожидаемому поведению протокола для используемого порта. Сопоставление предупреждений между несколькими каналами связи может также помочь в обнаружении C2.

Многоуровневое шифрование (Multilayer Encryption)

Система: Windows, Linux, macOS
Описание: Противник может применять несколько уровней шифрования трафика C2. Как правило (но не исключены другие варианты), в рамках шифрования HTTPS или SMTPS применяется дополнительное туннелирование собственной схемой шифрования.

Рекомендации по защите: Использование протоколов шифрования может усложнить типичное обнаружение C2 на основе сигнатурного анализа трафика. Если вредоносная программа использует стандартный криптографический протокол, инспекция SSL/TLS может использоваться для обнаружения трафика C2 в некоторых зашифрованных каналах. Проверка SSL/TLS сопряжена с определенными рисками, которые следует учитывать перед внедрением, чтобы избежать потенциальных проблем безопасности, таких как неполная проверка сертификата. После проверки SSL/TLS может потребоваться дополнительный криптографический анализ для шифрования второго уровня.

Port Knocking

Система: Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут применять методы Port Knocking для скрытия открытых портов, которые они используют для соединения с системой.

Рекомендации по защите: Применение stateful-брандмауэров может предотвратить реализацию некоторых вариантов Port Knocking.

Средства удаленного доступа (Remote Access Tools)

Система: Windows, Linux, macOS
Описание: Чтобы установить интерактивный режим командования и управления злоумышленник может использовать легитимное ПО, предназначенное для тех. поддержки рабочих станций и софт для удаленного доступа, например, TeamViewer, Go2Assist, LogMain, AmmyAdmin и т.п., которые обычно используются службами технической поддержки и могут быть внесены в белый список. Инструменты удаленного доступа, такие как VNC, Ammy и Teamviewer наиболее часто используются инженерами технической поддержки и обычно используются злоумышленниками.

Средства удаленного доступа могут устанавливаться после компрометации системы для использования в качестве альтернативного канала C2. Они также могут использоваться в качестве компонента вредоносного ПО для установки обратного соединения с сервером или системой, контролируемыми противником.

Средства администрирования, такие как TeamViewer, использовались несколькими группами, ориентированными на государственные учреждения в странах, представляющих интерес для Российских государственных и криминальных компаний.

Рекомендации по защите: Средства удаленного доступа могут использоваться совместно с техниками скрытия конечного адреса (Domain Fronting), поэтому целесообразно предотвратить установку противником инструментов RAT с помощью средств защиты хоста.

Удаленное копирование файлов (Remote File Copy)

Система: Windows, Linux, macOS
Описание: Файлы могут быть скопированы из одной системы в другую для развертывания инструментов противника или других файлов. Файлы могут быть скопированы из внешней системы, контролируемой злоумышленником, через канал C&C или с помощью других инструментов по альтернативным протоколам,

например FTP. Файлы также можно копировать на Mac и Linux с помощью встроенных инструментов, таких как scp, rsync, sftp.

Противники могут также копировать файлы в боковом направлении между внутренними системами-жертвами для поддержки перемещения по сети и удаленного выполнения команд. Это можно сделать с помощью протоколов предоставления общего доступа к файлам, подключая сетевые ресурсы через SMB или используя аутентифицированные соединения с Windows Admin Shares или RDP.

Рекомендации по защите: В качестве средств обнаружения рекомендуется мониторинг создания и передачи файлов по сети через протокол SMB. Необычные процессы с внешними сетевыми подключениями, создающие файлы внутри системы, также должны вызывать подозрение. Нетипичное использование утилит подобных FTP, также может быть подозрительным.

Стандартный протокол прикладного уровня (Standard Application Layer Protocol)

Система: Windows, Linux, macOS
Описание: Чтобы избежать обнаружения и смешать трафик C2 с существующим сетевым трафиком злоумышленники могут использовать стандартные протоколы прикладного уровня такие как HTTP, HTTPS, SMTP или DNS. Для соединений внутри канала C2 (анклава), например, между прокси-сервером и сводным узлом и другими узлами, обычно используются протоколы RPC, SSH или RDP.

Стандартный криптографический протокол (Standard Cryptographic Protocol)

Система: Windows, Linux, macOS
Описание: Для скрытия трафика C2 противники могут использовать известные алгоритмы шифрования. Несмотря на использование стойкого алгоритма, если секретные ключи шифруются и генерируются вредоносным ПО и/или хранятся в файлах конфигурации, то трафик C2 может быть раскрыт с помощью обратного инжиниринга.

Стандартный протокол не прикладного уровня (Standard Non-Application Layer Protocol)

Система: Windows, Linux, macOS
Описание: Для связи между зараженным хостом и сервером или взаимодействия зараженных хостов в сети могут использоваться протоколы не прикладного уровня модели OSI. В известных реализациях применялись протокол сетевого уровня — ICMP, транспортного уровня — UDP, сеансового уровня — SOCKS, а также протоколы типа redirected/tunneled, например Serial over LAN (SOL).

ICMP часто используется злоумышленниками для скрытия связи между хостами. Поскольку ICMP является частью Internet Protocol Suite и должен быть реализован всеми IP-совместимыми устройствами, он не так часто контролируется как другие протоколы, например, TCP или UDP.

Необычные порты (Uncommonly Used Port)

Система: Windows, Linux, macOS
Описание: Противники могут осуществлять связь по C2 через нестандартный порт, чтобы обойти прокси-серверы и межсетевые экраны, которые были неправильно сконфигурированы.

Web-сервис (Web Service)

Система: Windows
Права: Пользователь
Описание: Злоумышленники могут использовать запущенный, легитимный внешний Web-сервис в качестве средства передачи команд для управления зараженной системой. Серверы управления называют Command and control (C&C или C2). Популярные веб-сайты и социальные сети могут выступать в качестве механизма для C2, также могут применяться различные общедоступные сервисы типа Google или Twitter. Всё это способствует скрытию вредоносной активности в общем потоке трафика. Веб-сервисы обычно используют SSL/TLS, таким образом противники получают дополнительный уровень защиты.

Рекомендации по защите: Брандмауэры и веб-прокси могут использоваться для реализации политик ограничения внешних сетевых коммуникаций.

Общие рекомендации по организации мер по предотвращению и обнаружению C2

• IDS/DLP-системы, использующие сигнатурный анализ трафика, могут применяться для выявления и блокирования известных конкретных средств C2 и вредоносных программ, поэтому противник, вероятнее всего, со временем изменит используемые инструменты или настроит протокол передачи данных так, чтобы избежать обнаружения известными ему средствами защиты;

• Применяйте антивирусные средства защиты конечных точек для блокирования известных конкретных средств C2, вредоносных программ;

• Убедитесь, что хосты внутренней сети доступны только через авторизованные интерфейсы;

• Ограничивайте исходящий трафик, разрешая на межсетевых экранах и прокси-серверах только необходимые порты через соответствующие сетевые шлюзы;

• Блокируйте домены и IP-адреса известных инфраструктур C2. Однако, следует отметить, что это не является эффективным и долгосрочным решением, т.к. противники могут часто менять инфраструктуру C2;

• Используйте инструменты организации белых списков приложений, чтобы затруднить инсталляцию и запуск стороннего ПО;

• С помощью межсетевого экранирования, брандмауэров приложений и прокси-серверов ограничьте исходящий трафик для сайтов и служб, используемых известными инструментами удаленного доступа (TeamViewer, Go2Assist, LogMain, AmmyAdmin и т.п.);

• Если вредоносное ПО использует собственное шифрование с симметричными ключами, то с помощью реверс-инжиниринга образцов ПО возможно получение алгоритма и ключа с целью декодирования сетевого трафика и выявления сигнатур вредоносного ПО;

• Организуйте мониторинг вызовов API-функций, связанных с включением или использованием альтернативных каналов связи;

• Анализируйте сетевой трафик на наличие сообщений ICMP или других протоколов, которые содержат аномальные данные или которые обычно не видны в сети или не выходят из неё;

• Анализируйте сетевые потоки на предмет выявления аномальных потоков, например, когда клиент отправляет значительно больше данных, чем получает от сервера или когда процесс, который обычно не использует сеть, открывает сетевые соединения;

• Анализируйте сетевые потоки с целью выявления пакетов, которые не соответствуют стандарту протокола в части используемого порта.