Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 10

habr.com/ru/articles/447240

Андрей Макеев

Эксфильтрация или утечка данных (Exfiltration)

Ссылки на все части:

В данном разделе ATT&CK Enterprise Tactics описываются техники передачи данных, применяемые злоумышленниками/вредоносным ПО для изъятия/кражи/утечки целевой информации из скомпрометированной системы.

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.

Автоматизированная эксфильтрация (Automated Exfiltration)

Система: Windows, Linux, macOS
Описание: Эксфильтрация данных, содержащих конфиденциальные сведения, может выполнятся с использованием средств автоматизированной обработки информации и скриптов после или во время сбора целевой информации. Совместно со средствами автоматизации эксфильтрации для передачи данных по сети также могут применятся методы эксфильтрации через канал управления (C2) или альтернативный протокол.

Рекомендации по защите: Выявление и блокировка потенциально-опасного и вредоносного ПО с помощью инструментов создания белых списков приложений таких как AppLocker или Software Restriction Policies.

Сжатие данных (Data Compressed)

Система: Windows, Linux, macOS
Описание: В целях уменьшения объема данных противник может сжимать целевые данные, собранные для эксфильтрации. Сжатие выполняется вне канала передачи с помощью пользовательского ПО, алгоритма сжатия или распространенной библиотеки/утилиты, например 7zip, RAR, ZIP или zlib.

Рекомендации по защите: В целях обхода IPS или DLP, блокирующих передачу по незашифрованным каналам связи файлов определенного типа или содержащих определённый заголовок, злоумышленник может перейти на использование шифрования канала эксфильтрации. ПО для сжатия и сжатые файлы могут быть заблаговременно обнаружены с помощью мониторинга процессов и аргументов командной строки, связанных с вызовом известных утилит сжатия данных, однако такой подход подразумевает анализ большого количества ложных событий.

Шифрование данных (Data Encrypted)

Система: Windows, Linux, macOS
Описание: Перед эксфильтрацией целевые данные могут быть зашифрованы для того чтобы скрыть похищаемую информацию, ускользнуть от обнаружения или сделать процесс менее заметным. Шифрование выполняется с помощью утилиты, библиотеки или пользовательского алгоритма и выполняется вне канала управления (C2) и протокола передачи файлов. Распространенные архивные форматы с поддержкой шифрования данных — RAR и zip.

Рекомендации по защите: Запуск общеизвестного ПО для шифрования файлов может быть обнаружен посредством мониторинга процессов и аргументов командной строки, однако такой подход подразумевает анализ большого количества ложных событий. Процессы, загружающие Windows DLL crypt.32.dll, могут использоваться противником для выполнения шифрования, дешифрования или проверки подписей файлов. Выявление факта передачи зашифрованных данных может выполнятся путем анализа энтропии сетевого трафика. Если канал не зашифрован, то передача файлов известных типов может быть обнаружена системами IDS или DLP, анализирующими заголовки файлов.

Ограничение размера передаваемых данных (Data Transfer Size Limits)

Система: Windows, Linux, macOS
Описание: В целях укрытия от средств защиты и возможных предупреждений о превышении допустимого порога передаваемых по сети данных злоумышленник может разбить эксфильтруемые файлы на множество фрагментов одинакового размера либо ограничить размеры сетевых пакетов ниже порогового значения.

Рекомендации по защите: IDS и DLP, использующие сигнатурный анализ трафика, могут использоваться для выявления и блокирования только известных конкретных средств управления и контроля (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.

В качестве техники обнаружения рекомендуется анализ сетевого трафика на предмет необычных потоков данных (например, клиент отправляет значительно больше данных, чем получает с сервера). Зловредный процесс может длительное время поддерживать соединение последовательно отправляя пакеты фиксированного размера или открывать соединение и выполнять передачу данных через фиксированные промежутки времени. Подобная активность процессов, которые обычно не используют сеть, должна вызывать подозрение. Несоответствие используемого при передаче данных номера порта и номера порта, установленного в сетевом протоколе по умолчанию, может также указывать на вредоносную активность.

Эксфильтрация через альтернативный протокол (Exfiltration Over Alternative Protocol)

Система: Windows, Linux, macOS
Описание: Эксфильтрация данных, как правило, выполняется по альтернативному протоколу, отличному от протокола, используемого противником для организации канала управления (C2). Альтернативные протоколы включают в себя FTP, SMTP, HTTP/S, DNS и другие сетевые протоколы, а также внешние веб-сервисы, например, облачные хранилища.

Рекомендации по защите: Следуйте рекомендациям по настройке брандмауэров, ограничив вход и выход трафика из сети только по разрешенным портам. Например, если вы не используете службу FTP для отправки информации за пределы сети, то заблокируйте порты, связанные с протоколом FTP по периметру сети. В целях уменьшения возможности организации канала управления и эксфильтрации применяйте прокси-серверы и выделенные серверы для таких служб как DNS, разрешайте взаимодействие систем только через соответствующие порты и протоколы.

Для обнаружения и предотвращения известных способов организации канала управления и эксфильтрации данных применяйте системы IDS/IPS, использующие сигнатурный анализ трафика. Однако злоумышленники, вероятнее всего, со временем и изменят протокол управления и эксфильтрации так, чтобы избежать обнаружения средствами защиты.

В качестве техники обнаружения также рекомендуется анализ сетевого трафика на предмет необычных потоков данных (например, клиент отправляет значительно больше данных, чем получает с сервера). Не соответствие используемого номера порта и номера порта, установленного в сетевом протоколе по умолчанию, может также указывать на вредоносную активность.

Эксфильтрация через канал управления C2 (Exfiltration Over Command and Control Channel)

Система: Windows, Linux, macOS
Описание: Эксфильтрация данных может осуществляться по тому же протоколу, который используется злоумышленником в качестве канала управления (C2).

Рекомендации по защите: Используйте системы IDS/IPS с целью организации сигнатурного анализа трафика на предмет выявления известных средств организации канала управления и эксфильтрации. Проводите анализ трафика на предмет необычных потоков данных (например, клиент отправляет значительно больше данных, чем получает с сервера). Не соответствие используемого номера порта и номера порта, установленного в сетевом протоколе по умолчанию, может также указывать на вредоносную активность.

Эксфильтрация через альтернативную сетевую среду (Exfiltration Over Other Network Medium)

Система: Windows, Linux, macOS
Описание: Эксфильтрация данных может проходить в сетевой среде отличной от среды в которой организован канал управления (C2). Если канал управления использует проводное подключение к Интернету, то эксфильтрация может происходить через беспроводное подключение — WiFi, сотовую сеть, Bluetooth-подключение или другой радиоканал. При наличии доступности и близости, противник будет использовать альтернативную среду передачи данных, поскольку трафик в ней не будет маршрутизироваться через атакуемую корпоративную сеть, а сетевое соединение может быть как защищенным, так и открытым.

Рекомендации по защите: Убедитесь, что сенсоры средств защиты на хостах поддерживают аудит использования всех сетевых адаптеров и, по возможности, предотвращают подключение новых. Отслеживайте и анализируйте изменения в настройках сетевого адаптера, связанных с добавлением или репликацией сетевых интерфейсов.

Эксфильтрация через альтернативную физическую среду (Exfiltration Over Physical Medium)

Система: Windows, Linux, macOS

Описание: При определенных обстоятельствах, например физической изоляции скомпрометированной сети, эксфильтрация может происходить через физический носитель или устройство, подключенное пользователем. Такими носителями могут быть внешний жесткий диск, USB-накопитель, сотовый телефон, mp3-плеер или любое другое съемное устройство хранения или обработки информации. Физическая среда или устройство могут быть использованы противником в качестве конечной точки эксфильтрации или для переходов между изолированными системами.

Рекомендации по защите: Отключите автозапуск съемных устройств хранения информации. Запретите или ограничьте использование съемных устройств на уровне политики безопасности организации, если они не требуются для бизнес-операций.

В качестве меры по обнаружению эксфильтрации через физическую среду рекомендуется организация мониторинга доступа к файлам на съемных носителях, а так же аудит процессов, запускающихся при подключении съемных носителей.

Запланированная передача (Scheduled Transfer)

Система: Windows, Linux, macOS
Описание: Эксфильтрация данных может выполняться только в определенное время суток или через определенные промежутки времени. Такое планирование применяется для того чтобы смешать эксфильтруемые данные с нормальным трафиком в сети. При использовании запланированной эксфильтрации также применяются другие методы утечки информации, такие как эксфильтрация по каналу управления (C2) и альтернативному протоколу. *Рекомендации по защите:* Применение систем IDS/IPS с сигнатурным анализом трафика. В качестве мер по обнаружению вредоносной активности рекомендуется мониторинг моделей доступа процессов к файлам, а процессов и сценариев, сканирующих файловую систему с последующей отправкой сетевого трафика. Сетевые подключения к одному и тому же адресу, происходящие в одно и тоже время суток в течение нескольких дней должны вызывать подозрение.