Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 9

habr.com/ru/articles/441896

Андрей Макеев

Сбор данных (Collection)

Ссылки на все части:

Техники сбора данных в скомпрометированной среде включают способы идентификации, локализации и непосредственно сбора целевой информации (например, конфиденциальных файлов) с целью её подготовки к дальнейшей эксфильтрации. Описание методов сбора информации также охватывает описание мест хранения информации в системах или сетях, в которых противники могут осуществлять её поиск и сбор.

Индикаторами реализации большинства представленных в ATT&CK техник сбора данных являются процессы, использующие API, WMI, PowerShell, Cmd или Bash для захвата целевой информации с устройств ввода/вывода либо множественного открытия файлов на чтение с последующим копированием полученных данных в определенное место в файловой системе или сети. Информация в ходе сбора данных может шифроваться и объединяться в архивные файлы.

В качестве общих рекомендаций по защите от сбора данных предлагаются выявление и блокировка потенциально-опасного и вредоносного ПО с помощью инструментов организации белых списков приложений, таких как AppLocker и Sofware Restriction Policies в Windows, шифрование и хранение «чувствительной» информации вне локальных систем, ограничение прав доступа пользователей к сетевым каталогам и корпоративным информационным хранилищам, применение в защищаемой среде парольной политики и двухфакторной аутентификации.

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.

Захват аудио (Audio Capture)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Противник может использовать периферийные устройства компьютера (например, микрофон или веб-камеру) или приложения (например, сервисы голосовых и видео-вызовов) для захвата аудиозаписей с целью дальнейшего прослушивания конфиденциальных переговоров. Вредоносное ПО или сценарии могут использоваться для взаимодействия с периферийными устройствами через API-функции, предоставляемые операционной системой или приложением. Собранные аудиофайлы могут записываться на локальный диск с последующей эксфильтрацией.

Рекомендации по защите: Прямое противодействие вышеописанной технике может быть затруднено, поскольку требует детального контроля использования API. Обнаружение вредоносной активности также может быть также затруднено из-за разнообразия функций API.

В зависимости от предназначения атакуемой системы, данные об использовании API могут быть абсолютно бесполезны или напротив предоставлять контент для выявления иной вредоносной деятельности, происходящей в системе. Индикатором активности противника может быть неизвестный или необычный процесс доступа к API, связанного с устройствами или ПО, которые взаимодействуют с микрофоном, записывающими устройствами, программами записи или процесс, периодически записывающий на диск файлы, которые содержат аудиоданные.

Автоматизированный сбор (Automated Collection)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленник может использовать средства автоматизации сбора внутренних данных, таких как скрипты для поиска и копирования информации, соответствующей определенным критериям — тип файла, местоположение, имя, временные интервалы. Эта функциональность также может быть встроена в утилиты удаленного доступа. В процессе автоматизации сбора данных с целью идентификации и перемещения файлов дополнительно могут применятся техники обнаружения файлов и каталогов (File and Directory Discovery) и удаленного копирования файлов (Remote File Copy).

Рекомендации по защите: Шифрование и хранение конфиденциальной информации вне системы является одним из способов противодействия сбору файлов, однако если вторжение продолжается длительное время противник может обнаружить и получить доступ к данным другими способами. К примеру, кейлоггер, установленный в системе, путем перехвата ввода способен собрать пароли для расшифровки защищенных документов. Для предотвращения взлома зашифрованных документов в автономном режиме путем брутфорса необходимо использовать надежные пароли.

Данные буфера обмена (Clipboard Data)

Система: Windows, Linux, macOS
Описание: Противники могут собирать данные из буфера обмена Windows, хранящиеся в нём в ходе копирования пользователями информации внутри или между приложениями.

Windows
Приложения могут получать доступ к данным буфера обмена с помощью Windows API.

MacOS
OSX имеет встроенную команду *pbpast* для захвата содержимого буфера обмена.

Рекомендации по защите: Не стоит блокировать ПО, основываясь на выявлении поведения, связанного с захватом содержимого буфера обмена, т.к. доступ к буферу обмена является штатной функцией многих приложений в Windows. Если организация решит отслеживать такое поведение приложений, то данные мониторинга следует сопоставлять с другими подозрительными или не пользовательскими действиями.

Подготовка данных (Data Staged)

Система: Windows, Linux, macOS
Описание: Перед эксфильтрацией собранные данные, как правило, размещаются в определенном каталоге. Данные могут храниться в отдельных файлах или объединяться в один файл с помощью сжатия или шифрования. В качестве инструментов могут использоваться интерактивные командные оболочки, функционал cmd и bash может быть использован для копирования данных в промежуточное месторасположение.

Данные из хранилищ информации (Data from Information Repositories)

Система: Windows, Linux, macOS
Права: Пользователь

Описание: Противники могут извлекать ценную информацию из хранилищ информации — инструментов, позволяющих хранить информацию, как правило, для оптимизации совместной работы или обмена данными между пользователями. Информационные хранилища могут содержать огромный спектр данных, которые могут помочь злоумышленникам в достижении других целей или обеспечении доступа к целевой информации.

Ниже приведен краткий список информации, которая может быть найдена в хранилищах информации и иметь потенциальную ценность для злоумышленника:

- Политики, процедуры и стандарты;
- Схемы физических/логических сетей;
- Схемы системной архитектуры;
- Техническая системная документация;
- Учетные данные для тестирования/разработки;
- Планы работы/проектов;
- Фрагменты исходного кода;
- Ссылки на сетевые каталоги и другие внутренние ресурсы.

Распространенные хранилища информации:

Microsoft SharePoint
Находится во многих корпоративных сетях и часто используется для хранения и обмена значительным объемом документации.

Atlassian Confluence
Часто встречается в средах разработки наряду с Atlassian JIRA. Confluence обычно используется для хранения документации, связанной с разработкой.

Рекомендации по защите: Меры, рекомендуемые для предотвращения сбора данных из информационных репозиториев:

- Разработка и публикация политик, определяющих приемлемую информацию, подлежащую записи в хранилища информации;
- Реализация механизмов контроля доступа, которые включают в себя как аутентификацию, так и соответствующую авторизацию;
- Обеспечение принципа наименьших привилегий;
- Периодический пересмотр привилегий аккаунтов;
- Предотвращение доступа к действительным учетным записям (Valid Accounts), которые могут использоваться для доступа к информационным репозиториям.

Поскольку информационные репозитории обычно имеют достаточно большую пользовательскую базу, обнаружение их злонамеренного использования может быть нетривиальной задачей. Как минимум, доступ к хранилищам информации, выполняемым привилегированными пользователями (например, Domain, Enterprise

или Shema Admin) должен тщательно контролироваться и предотвращаться, поскольку эти типы учетных записей не должны использоваться для доступа к данным в хранилищах. Если существует возможность мониторинга и оповещения, то необходимо отслеживать пользователей, которые извлекают и просматривают большое количество документов и страниц. Такое поведение может указывать на работу ПО, извлекающего данные из хранилища. В средах с высоким уровнем зрелости для обнаружения отклонений в поведении пользователя могут применяться системы поведенческого анализа пользователей (User-Behavioraln Analytics (UBA)).

В Microsoft SharePoint может быть настроено журналирование доступа пользователей к определенным страницам и документам. В Confluence Atlassian аналогичное журналирование может быть настроено через AccessLogFilter. Для более эффективного обнаружения, вероятно, потребуется дополнительная инфраструктура хранения и анализа логов.

Данные из локальной системы (Data from Local System)

Система: Windows, Linux, macOS
Описание: Конфиденциальные данные могут быть получены из локальных системных источников, таких как файловая система или база данных, с целью дальнейшей эксфильтрации.

Злоумышленники часто ищут файлы на компьютерах, которые они взломали. Они могут делать это с помощью интерфейса командной строки (cmd). Так же могут использоваться способы автоматизации процесса сбора данных.

Данные из общедоступных сетевых дисков (Data from Network Shared Drive)

Система: Windows, Linux, macOS
Описание: Чувствительные данные могут быть собраны с удаленных систем, на которых есть общедоступные сетевые диски (локальная сетевая папка или файловый сервер), доступные противнику.

С целью обнаружения целевых файлов злоумышленник может выполнять поиск сетевых ресурсов на компьютерах, которые были скомпрометированы. Для сбора информации могут использоваться как интерактивные командные оболочки, так и распространенные функции командной строки.

Данные со съемных носителей (Data from Removable Media)

Система: Windows, Linux, macOS
Описание: Чувствительные данные могут быть собраны с любого съемного

носителя (оптический диск, USB-накопитель и т.д.), подключенного к скомпрометированной системе.

С целью обнаружения целевых файлов злоумышленник может выполнять поиск съемных носителей на скомпрометированных компьютерах. Для сбора информации могут использоваться как интерактивные командные оболочки, так и распространенные функции командной строки, а также средства автоматизации сбора данных.

Email Collection

Система: Windows
Описание: В целях сбора конфиденциальной информации злоумышленники могут использовать пользовательские электронные ящики. Данные, содержащиеся в электронной почте, можно получить из файлов данных Outlook (.pst) или файлов кэша (.ost). Имея учетные данные пользователя противник может взаимодействовать с Exhange-сервером напрямую и получить доступ к внешнему почтовому веб-интерфейсу, например Outlook Web Access.

Рекомендации по защите: Использование шифрования обеспечивает дополнительный уровень защиты конфиденциальной информации, передаваемой по электронной почте. Использование ассиметричного шифрования потребует от противника получения закрытого сертификата с ключом шифрования. Использование двухфакторной аутентификации в общедоступных почтовых веб-системах является наилучшей практикой минимизации возможности использования злоумышленником чужих учетных данных.

Существует несколько способов получения злоумышленником целевой электронной почты, каждый из которых имеет свой механизм обнаружения. Индикаторами вредоносной активности могут быть: доступ к локальным системным файлам данных электронной почты для последующей эксфильтрации, необычные процессы, подключающиеся к серверу электронной почты в сети, а также атипичные шаблоны доступа и попытки аутентификации на общедостпных почтовых веб-серверах. Отслеживайте процессы и аргменты командной строки, которые могут использоваться для сбора файлов данных электронной почты. Инстурменты удаленого доступа могут взаимодействовать напрямую с Windows API. Данные так же могут быть получены с помощью различных инструментов управления Windows, например WMI или PowerShell.

Захват ввода (Input Capture)

Система: Windows, Linux, macOS
Права: Администратор, System
Описание: Злоумышленники могут применять средства захвата пользовательского

ввода с целью получения учетных данных действующих аккаунтов. Кейлоггинг — это наиболее распространенный тип захвата пользовательского ввода, включающий множество различных способов перехвата нажатий клавиш, однако существуют и другие методы получения целевой информации такие как вызов UAC-запроса или написание оболочки для поставщика учетных данных по умолчанию (Windows Credential Providers). Кейлоггинг является наиболее распространенным способом кражи учетных данных, когда применение техник дампинга учетных данных неэффективно и злоумышленник вынужден оставаться пассивным в течение определенного периода времени.

В целях сбора учетных данных пользователей злоумышленник также может установить программный кейлоггер на внешних корпоративных порталах, например на странице входа через VPN. Это возможно после компрометации портала или сервиса посредством получения легитимного административного доступа, который в свою очередь мог быть организован для обеспечения резервного доступа на этапах получения первоначального доступа и закрепления в системе.

Рекомендации по защите: Обеспечьте выявление и блокирование потенциально-опасного и вредоносного ПО с помощью средств подобных AppLocker или политик ограничения использования ПО. Предпринимайте меры, направленные на уменьшение ущерба в случае получения злоумышленниками учетных данных. Следуйте рекомендациям Microsoft по разработке и администрированию корпоративной сети.

Кейлоггеры могут изменять реестр и устанавливать драйверы. Обычно используются API функции SetWindowsHook, GetKeyState, GetAsyncKeyState. Одни только вызовы API-функций не могут являться индикаторами кейлоггинга, но в совокупности с анализом изменений реестра, обнаружения установки драйверов и появлением новых файлов на диске могут свидетельствовать о вредоносной активности. Отслеживайте появление в реестре пользовательских поставщиков учетных данных (Custom Credential Provider):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication
\Credential Providers
```

Человек в браузере (Man in the Browser (MitB), Browser Pivoting)

Система: Windows
Права: Администратор, System
Описание: В ходе различных методов атаки MitB противник, воспользовавшись уязвимостью браузера жертвы, с помощью вредоносной программы может изменить веб-контент, например, добавить поля ввода на страницу, модифицировать пользовательский ввод, перехватить информацию. Конкретным примером является случай, когда злоумышленник внедряет в браузер ПО, которое позволяет наследовать файлы cookie, сеансы HTTP, клиентские SSL-сертификаты

пользователя и использовать браузер как способ аутентификации и перехода в интрасеть.

Для совершения атаки требуются привилегии SeDebugPrivilege и выполнения процессов высокой целостности (Understanding Protected Mode). С помощью настройки HTTP-прокси, HTTP и HTTPS трафик перенаправляется из браузера злоумышленника через пользовательский браузер. При этом пользовательский трафик ни как не меняется, а прокси-соединение разрывается как только закрывается браузер. Это позволяет противнику в том числе просматривать веб-страницы в качестве атакуемого пользователя.

Обычно для каждой новой вкладки браузер создает новый процесс с отдельными разрешениями и сертификатами. С помощью таких разрешений противник может перейти к любому ресурсу в интрасети, доступному через браузер с имеющимися правами, например Sharepoint или Webmail. Browser pivoting так же ликвидирует защиту двухфакторной аутентификацией.

Рекомендации по защите: Вектор защиты рекомендуется направить на ограничение разрешений пользователей, предотвращение возможности эскалации привилегий и обхода UAC. Регулярно закрывайте все сеансы браузера и когда они больше не нужны. Обнаружение MitB крайне затруднено, т.к. трафик противника маскируется под обычный пользовательский трафик, не создаются новые процессы, не используется дополнительное ПО и не затрагивается локальный диск атакуемого хоста. Журналы аутентификации могут использоваться для аудита входов пользователя в определенные веб-приложения, однако выявление среди них вредоносной активности может быть затруднено, т.к. активность будет соответствовать обычному поведению пользователя.

Захват экрана (Screen Capture)

Система: Windows, Linux, macOS
Описание: В ходе сбора информации противники могут пытаться сделать скриншоты рабочего стола. Соответствующая функциональность может быть включена в инструменты удаленного доступа, используемых после компрометации.

Mac
В OSX для захвата скриншотов используется встроенная команда screencapture.
Linux
В Linux имеется команда xwd.

Рекомендации по защите: В качестве метода обнаружения рекомендуется мониторинг процессов, использующих API для получения снимков экрана с последующей записью файлов на диск. Однако, в зависимости от легитимности такого поведения в конкретной системе, для выявления вредоносной активности вероятнее всего потребуется дополнительна корреляция собираемых данных с другими событиями в системе.

Захват видео (Video Capture)

Система: Windows, macOS
Описание: Противник может использовать периферийные устройства компьютера (например, встроенные камеры и вебкамеры) или приложения (например, сервисы видеовызовов) для захвата видео или изображения. Захват видео, в отличие методов снятия снимков экрана, предполагает использование устройств и приложений для записи видео, а не для захвата изображения с экрана жертвы. Вместо видеофайлов через определенные промежутки могут захватываться изображения.
Вредоносное ПО или сценарии могут использоваться для взаимодействия с устройствами через API, предоставляемый операционной системой или приложением для захвата видео или изображений. Собранные файлы могут быть записаны на диск и позже эксфильтрованы.

Известно несколько различных вредоносных программ для macOS, например Proton и FriutFly, который может осуществлять запись видео с веб-камеры пользователя.

Рекомендации по защите: Прямое противодействие вышеописанной технике может быть затруднено, поскольку требует детального контроля API. Усилия по защите должны быть направлены на предотвращение нежелательного или неизвестного кода в системе.

Идентифицируйте и блокируйте потенциально-опасное и вредоносное ПО, которое можно использовать для записи звука, используя AppLocker и Software Restriction Policies.

Обнаружение вредоносной активности может быть также затруднено из-за различных API. В зависимости от того как используется атакуемая система данные телеметрии, касающиеся API, могут быть бесполезны или напротив предоставлять контент для другой вредоносной деятельности, происходящей в системе. Индикатором активности противника может быть неизвестный или необычный процесс доступа к API, связанного с устройствами или ПО, которые взаимодействуют с микрофоном, записывающими устройствами, программами записи или процесс, периодически записывающий файлы на диск, которые содержат аудиоданные.