# Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 8

habr.com/ru/articles/439026

Андрей Макеев

## Боковое перемещение (Lateral Movement)

**Ссылки на все части:**


Тактика бокового движения (*англ. «Lateral Movement» — боковое, поперечное, горизонтальное перемещение*) включает методы получения противником доступа и контроля над удаленными системами, подключенными к атакованной сети, а так же, в некоторых случаях, запуска вредоносных инструментов на удаленных системах, подключенных к атакованной сети. Боковое перемещение по сети позволяет злоумышленнику получать информацию из удаленных систем без использования дополнительных инструментов, таких как утилиты удаленного доступа (RAT).

*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.*

## AppleScript

*Система:* macOS
*Права:* Пользователь
*Описание:* Язык AppleScript предоставляет возможность работы с Apple Event — сообщениями, которыми обмениваются приложения в рамках межпроцессного взаимодействия (IPC). С помощью Apple Event можно взаимодействовать практически с любым приложением, открытым локально или удаленно, вызывать такие события как открытие окон и нажатие клавиш. Скрипты запускаются с

помощью команды: `Osascript -e [скрипт]`.
Злоумышленники могут использовать AppleScript для скрытого открытия SSH-соединений с удаленными хостами, предоставления пользователям поддельных диалоговых окон. AppleScript также может использоваться в более распространенных типах атак, например, организации Reverse Shell.

*Рекомендации по защите:* Обязательная проверка запускаемых сценариев AppleScript на наличие подписи доверенного разработчика.

## Программное обеспечение для развертывания приложений (Application Deployment Software)

*Система:* Windows, Linux, macOS
*Описание:* Средства развертывания приложений, используемые администраторами сети предприятия, могут применяться злоумышленниками для установки вредоносных приложений. Разрешения, необходимые для совершения этих действий зависят от конфигурации системы: для доступа к серверу установки программного обеспечения могут потребоваться определенные доменные учетные данные, а может быть достаточно и локальных прав, однако для входа в систему установки приложений и запуска процесса развертывания может потребоваться учетная запись администратора системы. Доступ к централизованной корпоративной системе установки приложений позволяет противнику удаленно выполнять код во всех системах атакуемой сети. Такой доступ может использоваться для продвижения по сети, сбора информации или вызова специфического эффекта, например, очистки жестких дисков на всех хостах.

*Рекомендации по защите:* Предоставляйте доступ к системам развертывания приложений только ограниченному числу авторизованных администраторов. Обеспечьте надежную изоляцию и ограничение доступа к критически важным сетевым системам с помощью брандмауэров, ограничьте привилегии учетных записей, настройте групповые политики безопасности и многофакторную аутентификацию. Убедитесь, что данные учетных записей, имеющих доступ к системе развертывания софта, уникальны и не используются во всей сети. Регулярно устанавливайте исправления и обновления систем установки приложений, чтобы предотвратить возможность получения к ним несанкционированного удаленного доступа с помощью эксплуатации уязвимостей. Если система установки приложений настроена на дистрибьюцию только подписанных двоичных файлов, то убедитесь, что доверенные сертификаты подписи размещены не в ней, а хранятся в системе, удаленный доступ к которой невозможен или ограничен и контролируется.

## DCOM (Distributed Component Object Model)

*Система:* Windows

*Права:* Администратор, System
*Описание:* DCOM — это протокол, который расширяет функциональность Component Object Model (COM), позволяя компонентам программного обеспечения взаимодействовать не только в рамках локальной системы, но и по сети, используя технологию удаленного вызова процедур (RPC), с компонентами приложений других систем. COM является компонентом Windows API. Посредством COM клиентский объект может вызвать метод серверного объекта, обычно это DLL-библиотеки или Exe-файлы. Разрешения на взаимодействие с локальным или удаленным серверным COM-объектом определяются с помощью ACL-листов в реестре. По умолчанию, только администраторы могут удаленно активировать и запускать COM-объекты посредством DCOM.

Противники могут использовать DCOM в целях бокового перемещения по сети. Через DCOM злоумышленник, работающий в контексте пользователя с соответствующими привилегиями может удаленно вызывать выполнение произвольного кода через приложения Office и другие объекты Windows, содержащие небезопасные методы. DCOM также может выполнять макросы в существующих документах, а также вызывать Dynamic Data Exchange (DDE) напрямую через COM-объект, созданный в Microsoft Office, минуя необходимость создания вредоносного документа. DCOM также может предоставлять противнику функциональные возможности, которые можно использовать на других этапах атаки, таких как повышение привилегий или закрепление доступа.

*Рекомендации по защите:* С помощью реестра настройте индивидуальные параметры безопасности COM-приложений:
code>HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID.
Рассмотрите возможность отключения поддержки DCOM с помощью утилиты *dcomcnfg.exe* или в реестре:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\EnableDCOM=SZ:N`
Включите брандмауэр Windows, который по умолчанию предотвращает создание экземпляров DCOM. Включите режим защищенного просмотра и оповещения о запуске COM-объектов в документах MS Office.

## Эксплойты удаленных сервисов (Exploitation of Remote Services)

*Система:* Windows, Linux, macOS
*Права:* Пользователь
*Описание:* Для выполнения произвольного кода злоумышленники могут применять эксплойты, которые используют ошибки в программах, службах, программном обеспечении операционной системы или даже в самом ядре операционной системы. Целью эксплуатации уязвимостей удаленных сервисов после первичной компрометации является обеспечение удаленного доступа к системам для перемещения по сети.

Предварительно противнику необходимо определить системы, имеющие уязвимости. Это может быть выполнено путём сканирования сетевых служб или других методов обнаружения, таких как поиск распространенного уязвимого программного обеспечения и отсутствующих исправлений, что служит индикатором наличия уязвимостей, или поиск средств безопасности, которые используется для обнаружения и блокирования удаленной эксплуатации уязвимостей. Серверы, вероятнее всего, будут являться ценной целью для использования при перемещения по сети, но рабочие станции также подвержены риску если они предоставляют противнику какое-либо преимущество или доступ к дополнительным ресурсам.

Известны уязвимости в службах общего доступа, таких как SMB, RDP, а также приложениях, которые могут использоваться во внутренних сетях, таких как MySQL и службы web-серверов. В зависимости от разрешений уязвимой службы, противник, осуществляя боковое перемещение, с помощью эксплойта может дополнительно получить повышение привилегий.

*Рекомендации по защите:* Сегментируйте сети и системы, чтобы уменьшить доступ к критически важным системам и услугам. Минимизируйте доступность сервисов, предоставляя права только тем, кому они необходимы. Регулярно проверяйте внутреннюю сеть на наличие новых и потенциально уязвимых сервисов. Минимизируйте разрешения и доступ для учетных записей служб, чтобы ограничить зону поражения.

Регулярно обновляйте программное обеспечение, внедрите процесс управления установкой исправлений приложений на внутренних хостах и серверах. Разработайте процедуры анализа киберугроз, чтобы определить типы и уровни угроз, в ходе которых против вашей организации могут применяться эксплойты, включая эксплойты уязвимостей нулевого дня. Применяйте песочницы, чтобы усложнить противнику выполнение операций с помощью использования неизвестных вам или неисправленных уязвимостей. Другие типы микросегментации и виртуализации приложений также могут смягчить последствия некоторых типов эксплойтов. Программные средства безопасности, такие как Windows Defender Exploit Guard (WDEG) и Enhanced Mitigation Experience Toolkit (EMET), которые нацелены на поиск поведения, используемого во время эксплуатации уязвимостей, могут использоваться для защиты от эксплойтов. Проверка целостности потока управления — это ещё один способ идентификации и блокирования эксплуатации уязвимостей программного обеспечения. Многие из перечисленных средств защиты могут работать не для всех программ и служб, совместимость зависит от архитектуры и двоичного файла целевого приложения.

В зависимости от имеющегося инструментария обнаружение защищающейся стороной эксплуатации уязвимостей может быть затруднено. Программные эксплойты могут не всегда успешно выполниться или привести к нестабильной работе или аварийному завершению атакуемого процесса. Обращайте внимание на

индикаторы компрометации, например, ненормальное поведение процессов, появление на диске подозрительных файлов, необычный сетевой трафик, признаки запуска средств обнаружения, инъекции процессов.

## Сценарии входа в систему (Logon Scripts)

*Система:* Windows, macOS
*Описание:* Противник может использовать возможность создания новых или изменения существующих logon-скриптов — сценариев которые выполняются всякий раз когда конкретный пользователь или группа пользователей выполняет вход в систему. Если злоумышленник получил доступ к logon-скрипту на контроллере домена, то он может модифицировать его для исполнения кода во всех системах домена в целях бокового перемещения по сети. В зависимости от настроек прав доступа сценариев входа в систему могут потребоваться локальные или административные учетные данные.
В Mac, logon-скрипты (Login/Logout Hook), в отличие от Login Item, которые запускаются в контексте пользователя, могут запускаться от имени root.

*Рекомендации по защите:* Ограничение прав администраторов на создание сценариев входа в систему. Идентификация и блокирование потенциально-опасного ПО, которое может использоваться для модификации сценариев входа. AppLocker в Windows может блокировать запуск неизвестных программ.

## Pass the Hash

*Система:* Windows
*Описание:* Pass the Hash (PtH) — это метод аутентификации пользователя без доступа к его паролю в открытом виде. Метод заключается в обходе стандартных этапов аутентификации на которых требуется ввод пароля и переходе непосредственно к той части аутентификации, которая использует хэш пароля. Хэши действительных паролей захватываются противником с помощью техник доступа к учетным данным (Credential Access), далее хэши используются для PtH-аутентификации, которая может использоваться для выполнения действий в локальных или удаленных системах.

Для осуществления атаки Pass the Hash в Windows 7 и выше с установленным обновлением *KB2871997* требуются действительные учетные данные пользователя домена или хэши администратора (RID 500).

*Рекомендации по защите:* Проводите мониторинг системных и доменных журналов в целях выявления необычной активности входов учетных записей. Предотвращайте доступ к действующим учетным записям. В системах версии Windows 7 и выше установите исправление KB2871997, чтобы ограничить доступ учетных записей в группах локальных администраторов по умолчанию.

В целях минимизации возможности реализации Pass the Hash отключите удаленный запуск UAC при входе пользователя по сети с помощью редактирования соответствующего ключа в реестре или групповых политик:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolice`

`GPO:Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigation: Apply UAC restriction to local accounts on network logons`

Ограничивайте совпадение учетных записей в различных системах, чтобы помешать их компрометации и снизить способность перемещения противника между системами. Убедитесь, что встроенные и созданные учетные данные локальных администраторов имеют сложные уникальные пароли. Не допускайте, чтобы доменный пользователь входил в группу локальных администраторов на нескольких системах. В целях обнаружения атак Pass the Hash применяется аудит всех событий входа и использования учетных данных с проверкой на расхождение (например, одна учетная запись использовалась одновременно на нескольких системах). Необычные входы в систему, связанные с подозрительными действиями (например, создание и выполнение двоичных файлов) могут также указывать на вредоносную активность. Подозрение также должны вызывать события аутентификации типа NTLM LogonType 3 (сетевой вход), несвязанные с доменными и не анонимными учетными записями (пользователи с SID S-1-5-7).

## Pass the Ticket

*Система:* Windows
*Описание:* Pass the Ticket (PtT) — это способ аутентификации с помощью билетов Kerberos без доступа к паролю учетной записи. Kerberos-аутентификация может быть использована в качестве первого шага к перемещению противника в удаленную систему.
В ходе PtT, действующие билеты Kerberos для действующих учетных записей фиксируются противником с помощью техник дампинга учетных данных. В зависимости от уровня доступа могут быть получены пользовательские билеты служб (service tickets) или билеты на выдачу билетов (ticket granting ticket (TGT)). Билет службы позволяет получить доступ к конкретному ресурсу, тогда как TGT может быть использован для запроса билетов служб у службы предоставления билетов (TGS) для доступа к любому ресурсу к которому пользователь имеет доступ.

Silver Ticket (поддельный TGS) может быть получен для сервисов, которые используют Kerberos как механизм аутентификации, и использован для генерации билетов для доступа к конкретному ресурсу и системе, в которой размещен ресурс (например, SharePoint).

Golden Ticket (билет Kerberos для неограниченного доступа к ресурсам в контексте любого пользователя, включая несуществующих пользователей) может быть получен путем использования NTLM-хэша учетной записи службы распределения ключей — KRBTGT, который даёт возможность генерировать TGT для любой учетной записи в AD.

*Рекомендации по защите:* Проводите мониторинг наличие в системе необычных учетных данных. Ограничивайте совпадение учетных данных в разных системах тем самым предотвращая повреждения в случае компрометации. Убедитесь, что локальные учетные записи администраторов имеют сложные, уникальные пароли. Не позволяйте пользователю быть локальным администратором нескольких систем. Ограничивайте разрешения учетной записи администратора домена для контроллеров домена и ограниченных серверов. Делегируйте прочие функции администратора отдельным аккаунтам.

Для противодействия ранее сгенерированному Gold Ticket дважды сбросьте пароль встроенной учетной записи KRBTGT, что сделает недействительными все Golden Ticket, созданные с помощью хэша пароля KRBTGT, и другие билеты Kerberos, полученные из Golden Ticket.

С помощью инструментов создания белых списков приложений, таких как Applocker или Software Restriction Policies попытайтесь идентифицировать и заблокировать неизвестное или вредоносное ПО, которое может быть использовано для получения билетов Kerberos и дальнейшей аутентификации.

В целях обнаружения атак PtT рекомендуется аудит всех событий Kerberos-аутентификации и использования учетных данных с анализом расхождений. Необычные события удаленной аутентификации, коррелирующие с другой подозрительной активностью (такой как запись и запуск бинарников) может служить индикатором вредоносной активности.
Событие ID4769 генерируется на контроллере домена при использовании Golden Ticket после двойного сброса пароля KRBTGT. Код состояния 0x1F свидетельствует о неудачной проверке целостности зашифрованного поля и указывает на попытку использования недействительного Golden Ticket.

## Протокол удаленного рабочего стола (Remote Desktop Protocol)

*Система:* Windows
*Права:* Пользователи удаленного рабочего стола, пользователи
Описание: Удаленный рабочий стол — типовая функция операционных систем, которая позволяет пользователю осуществлять вход в интерактивный сеанс с графическим интерфейсом на удаленном компьютере. Microsoft называет свою реализацию протокола RDP как Remote Desktop Servoce (RDS). Есть и другие реализации и сторонние инструменты предоставляющие графический доступ к удаленным сервисам, подобным RDS. Противники могут подключаться к удаленной

системе через RDP/RDS для расширения доступа если соответствующая служба включена и разрешает доступ с известными злоумышленнику учетными данными. Предварительно, противник, вероятно, будет использовать техники доступа к учетным данным для получения учетных данных, которые можно использовать с RDP. Противники могут также использовать RDP в сочетании с техникой злоупотребления «специальными возможностями Windows» для закрепления в системе.

Злоумышленник также может пытаться захватить RDP сессии, включающие удаленные сеансы легитимных пользователей. Обычно, при попытке кражи сессии пользователь получает уведомление и запрос на подтверждение, однако имея разрешения уровня System с помощью консоли службы терминалов можно перехватить сеанс без предоставления учетных данных и подтверждения пользователя: `C:\Windows\system32\tscon.exe [номер сеанса, который нужно украсть]`.
Это может быть выполнено удаленно или локально с активными или прерванными сеансами. Это также может привести к повышению привилегий путем захвата сеанса администратора домена или более привилегированного пользователя. Всё вышеописанное может быть сделано с помощью встроенных команд Windows, либо соответствующий функционал может быть добавлен в инструментарий для пентестинга, например RedSnarf.

*Рекомендации по защите:* Отключите службу RDP если она не нужна, удалите ненужные учетные записи и группы из группы *Remote Desktop Users*, включите правило блокировки трафика RDP между зонами безопасности в брандмауэре. Регулярно проверяйте членов группы *Remote Desktop Users*. Удалите группу администраторов из списка групп, которым разрешен вход через RDP. Если удаленный доступ необходим, то ограничьте права удаленного пользователя. Используйте *Remote desktop gateways* и многофакторную аутентификацию для удаленного входа. Не оставляйте RDP доступным из интернета. Измените GPO, определив таймауты и максимальное время, в течение которого может быть активен удаленный сеанс. Измените GPO, указав максимальное время в течение которого отключенный удаленный сеанс остается активным на хост-сервере.

В связи с тем, что использование RDP может быть вполне легитимным процессом индикаторами вредоносной активности могут служить шаблонны доступа и действия, которые происходят после удаленного входа в систему, например, вход пользователей в системы к которым они обычно не обращаются или вход в несколько систем в течение относительно короткого промежутка времени. В целях предотвращения перехвата сеансов RDP рекомендуется мониторинг использования tscon.exe и создания служб, использующих `cmd.exe /k` или `cmd.exe /c` в своих аргументах.

## Удаленное копирование файлов (Remote File Copy)

*Система:* Windows, Linux, macOS
*Права:* Пользователь
*Описание:* Файлы могут быть скопированы из одной системы в другую для развертывания инструментов противника или других файлов в ходе операции. 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:* Применение IDS/IPS-систем, которые используют сигнатуры для идентификации вредоносного трафика или необычной передачи данных посредством известных инструментов и протоколов, подобных FTP, которые могут быть использованы для снижения активности на сетевом уровне. Сигнатуры, как правило, используются для обнаружения уникальных индикаторов протоколов и основаны на конкретной технике обфускации, используемой конкретным злоумышленником или инструментом, и, вероятнее всего, будут отличаться для разных семейств и версий вредоносных программ. Злоумышленники, скорее всего, изменят сигнатуру инструментов C2 или создадут протоколы так, чтобы избежать обнаружения общеизвестными защитными инструментами.

В качестве средств обнаружения рекомендуется мониторинг создания и передачи файлов по сети через SMB. Необычные процессы с внешними сетевыми подключениями, создающие файлы внутри системы могут вызывать подозрения. Нетипичное использование утилит подобных FTP, также может быть подозрительным. Так же рекомендуется анализировать сетевые данные на предмет необычных потоков данных, например клиент отправляет значительно больше данных, чем получает с сервера. Процессы, использующие сеть, которые обычно не имеют сетевого взаимодействия также являются подозрительными. Проанализируйте содержимое пакета с целью обнаружения соединений, которые не соответствуют протоколу и используемому порту.

## Удаленные сервисы (Remote Services)

*Система:* Windows, Linux, macOS
*Описание:* Злоумышленники могут использовать действительные учетные записи для входа в службу, предназначенную для приема сетевых подключений, например telnet, SSH или VNC. После этого противник сможет выполнять действия от имени вошедшего в систему пользователя.

*Рекомендации по защите:* Ограничьте количество учетных записей, которые могут использовать удаленные службы. По возможности используйте многофакторную аутентификацию. Ограничьте разрешения для учетных записей, которые подвергаются более высокому риску компрометации, например, настройте SSH, чтобы пользователи могли запускать только определенные программы. Предотвращайте использование техник доступа к учетным данным, которые могут позволить злоумышленнику приобрести действительные учетные данные. Соотносите активность использования входа в систему, связанную с удаленными службами, с необычным поведением или другой вредоносной или подозрительной активностью. Прежде чем предпринимать продвижение по сети злоумышленнику, скорее всего, потребуется узнать об окружающей среде и взаимосвязях между системами с помощью техник обнаружения.

## Тиражирование через съемные носители (Replication Through Removable Media)

*Система:* Windows
*Описание:* Техника предполагает исполнение вредоносной программы с помощью функции автозапуска в Windows. Чтобы обмануть пользователя «законный» файл может быть предварительно модифицирован или заменён, а затем скопирован на съемное устройство злоумышленником. Так же полезная нагрузка может быть внедрена в прошивку съемного устройства или через программу первоначального форматирования носителя.

*Рекомендации по защите:* Отключение функций автозапуска в Windows. Ограничение использования съемных устройств на уровне политики безопасности организации. Применение антивирусного программного обеспечения.

## Захват SSH (SSH Hijacking)

*Система:* macOS, Linux
*Описание:* Secure Shell (SSH) — стандартное средство удаленного доступа в Linux и macOS, которое позволяет пользователю подключаться к другой системе через шифрованный туннель, обычно с аутентификацией по паролю, сертификату или пары ключей ассиметричного шифрования. Для продвижения по сети со скомпрометированного хоста противники могут воспользоваться доверительными отношениями, установленными с другими системами посредством аутентификации по открытому ключу в активных SSH-сессиях путем перехвата существующего соединения с другой системой. Это может произойти из-за компрометации самого агента SSH или наличия доступа к сокету агента. Если противник сможет получить root-доступ в системе, то дальнейший захват SSH-сессий будет тривиальной задачей. Компрометация SSH-агента также позволяет перехватить учетные данные SSH. Техника захвата SSH (SSH Hijacking) отличается от использования техники Удаленных сервисов (Remote Services) потому что происходит внедрение в

существующий SSH-сеанс, а не создание нового сеанса с использованием действительных учетных записей.

*Рекомендации по защите:* Убедитесь, что пары SSH-ключей имеют надежные пароли и воздержитесь от использования таких технологий хранения ключей как ssh-agent, если они не защищены должным образом. Убедитесь, что все закрытые ключи надежно хранятся в местах, к которым имеет доступ только законный владелец со сложным, часто меняющимся паролем. Убедитесь в правильности файловых разрешений и укрепите систему, чтобы предотвратить возможность повышения привилегий root. Не разрешайте удаленный доступ через SSH с правами root или другими привилегированными учетными записями. Убедитесь, что функция переадресации агента (Agent forwarding) отключена в системах, в которых она явно не требуется. Учитывая, что само по себе использование SSH может быть легитимно, в зависимости от сетевой среды и способа её использования, индикаторами подозрительного или злонамеренного использования SSH могут выступать различные шаблоны получения доступа и последующего поведения. Например, учетных записи, осуществляющие вход в системы, к которым они обычно не обращаются или подключение к нескольким системам в течение короткого промежутка времени. Так же рекомендуется отслеживать файлы сокетов пользовательских SSH-агентов, которые используются разными пользователями.

## Общедоступный Webroot (Shared Webroot)

*Система:* Windows
*Описание:* Противник может разместить во внутреннем сегменте сети вредоносный контент на веб-сайте, имеющем общедоступный каталог webroot или другой общедоступный каталог подачи веб-контента, а затем перейти к этому контенту с помощью веб-браузера, чтобы заставить сервер выполнить его. Обычно вредоносный контент запускается в контексте процесса веб-сервера, часто, в зависимости от того как настроен веб-сервер, это приводит к получению локальных системных или административных привилегий. Такой механизм общего доступа и удаленного выполнения кода может быть использован для перемещения в систему, на которой работает веб-сервер. Например, веб-сервер под управлением PHP с общедоступным webroot может позволить злоумышленнику загрузить инструменты RAT в ОС веб-сервера при посещении определенной страницы.

*Рекомендации по защите:* Сети, в которых пользователям разрешено вести открытую разработку, тестирование контента и запуск собственных веб-серверов, особенно уязвимы если системы и веб-серверы должным образом не защищены: неограниченно использование привилегированных учетных записей, доступ к сетевым ресурсам возможен без проверки подлинности, а также нет сетевой изоляции сети/системы. Обеспечьте правильность разрешений для каталогов, доступных через веб-сервер. Запретите удаленный доступ к корневой директории сайта (webroot) или другим каталогам, используемым для подачи веб-контента. Отключите выполнение в каталогах webroot. Убедитесь, что разрешения процесса

веб-сервера только те что требуются. Не используйте встроенные учетные записи, вместо этого создайте определенные учетные записи для ограничения ненужного доступа или пересечения разрешений в нескольких системах.

Используйте мониторинг процессов, чтобы определить когда когда файлы были записаны на веб-сервер процессом, которые не является обычным для веб-сервера или когда файлы были записаны вне административных периодов времени. Используйте мониторинг процессов, чтобы определить нормальные процессы и в последующем обнаруживать аномальные процессы, которые обычно не выполняются на веб-сервере.

## Порча общедоступного содержимого (Taint Shared Content)

*Система:* Windows
*Права:* Пользователь
*Описание:* Содержимое общедоступных сетевых дисков и других хранилищ может быть испорчено путем добавления в размещенные файлы вредоносных программ, сценариев или кода эксплойта. Как только пользователь откроет испорченный контент, вредоносная часть может быть выполнена для запуска кода злоумышленника в удаленной системе. Противники могут использовать вышеописанный метод для бокового продвижения.

Есть ещё одна разновидность техники, использующей несколько другие методы распространения вредоносных программ при получении пользователями доступа к общему сетевому каталогу. Суть её заключается в модификации ярлыков (Shortcut Modification) каталогов (.lnk) с применением маскарадинга таким образом, чтобы ярлыки выглядели как реальные каталоги, которые предварительно были скрыты. Вредоносные .lnk имеют встроенную команду, которая выполняет скрытый вредоносный файл, а затем открывает реальный каталог, ожидаемый пользователем. Реализация этой техники в часто используемых сетевых каталогах может привести к частым повторным заражениям и, как следствие, получению злоумышленником широкого доступа к системам и, возможно, к новым более привилегированным учетным записям.

*Рекомендации по защите:* Защищайте общие папки, сводя к минимум количество пользователей, имеющих права на запись. Используйте утилиты, которые могут обнаруживать или предотвращать эксплойты по первым признакам, например Microsoft Mitigation Experience Toolkit (EMET). Снижайте потенциальный риск бокового продвижения посредством использования веб-служб управления документами и совместной работы, которые не используют обмен файлами и каталогами.

Идентифицируйте и блокируйте потенциально-опасное и вредоносное программное обеспечение, которое может быть использовано для порчи содержимого, с помощью таких инструментов как AppLocker или Software Restriction Policies.

Рекомендуется частое сканирование общих сетевых каталогов на наличие вредоносных файлов, скрытых файлов .LNK и других типов файлов, наличие которых не типично для конкретного каталога. Подозрения должны вызывать процессы, записывающие или перезаписывающие множество файлов в общий сетевой каталог, а также процессы выполняемые со съемных носителей.

## Third-party Software (Стороннее ПО)

*Система:* Windows, Linux, macOS
*Права:* Пользователь, администратор, System
*Описание:* Стороннее ПО и системы развертывания ПО (SCCM, VNC, HBSS, Altris и т.п.), используемые в сети для нужд администрирования, могут использоваться злоумышленником для удаленного запуска кода на всех хостах, подключенных к таким системам. Права, необходимые для реализации данной техники зависят от конкретной конфигурации систем. Локальных учетных данных может быть достаточно для доступа к серверу развертывания ПО, однако для запуска развертывания ПО может потребоваться учетная запись администратора.

*Рекомендации по защите:* Проверяйте уровень безопасности применяемых систем развертывания ПО. Убедитесь, что доступ к системам управления ПО ограничен, контролируется и защищен. Строго используйте политики обязательного предварительного одобрения удаленного развертывания ПО. Предоставляйте доступ к системам развертывания ПО ограниченному числу администраторов, обеспечьте изоляцию системы развертывания ПО. Убедитесь, что учетные данные для доступа к системе развертывания ПО уникальны и не используются в других сервисах корпоративной сети. Если система развертывания ПО настроена на запуск только подписанных двоичных файлов, то проверьте, что доверенные сертификаты не хранятся в самой системе развертывания ПО, а расположены в системе, удаленный доступ к которой невозможен.

## Windows Admin Shares

*Система:* Windows
*Права:* Пользователь
*Описание:* Системы Windows имеют скрытые сетевые папки, доступные только администраторам и предоставляющие возможность удаленного копирования файлов и другие административные функции. Примеры Windows Admin Shares: C$, ADMIN$, IPC$.
Противники могут использовать эту технику в сочетании с действующими учетными записями уровня администратора для удаленного доступа к системе через server messege block (SMB), взаимодействуя с системами с помощью RPC, передавать файлы и запускать перенесенные двоичные файлы с помощью техник Выполнения (Execution). Примерами методов выполнения, основанных на аутентифицированных сеансах через SMB/RPC являются назначенные задания, запуск служб и WMI.

Противники также могут использовать NTLM-хэши для получения доступа к Admin Shares посредством Pass-the-Hash. Команда net use при наличии действующих учетных данных может быть использована для подключения к Windows Admin Shares удаленной системы.

*Рекомендации по защите:* Не используйте одинаковые пароли учетных записей локальных администраторов в разных системах. Обеспечьте сложность и уникальность паролей, чтобы их нельзя было угадать или взломать. Запретите удаленный вход в систему встроенной учетной записи локального администратора. Не допускайте, чтобы учетные записи пользователей входили в локальную группу администраторов нескольких систем.

Идентифицируйте и блокируйте потенциально-опасное и вредоносное программное обеспечение, которое можно использовать для эксплуатации SMB и Admin Shares, с помощью AppLocker или Software Restriction Policies.

Обеспечьте централизованный сбор и хранение журналов использования учетных данных для входа в системы. Windows Event Forwarding позволяет собирать данные об успешном/неуспешном использовании учетных записей, которые могли быть использованы для перемещения по сети. Отслеживайте действия удаленных пользователей, которые подключаются к Admin Shares. Отслеживайте использование инструментов и команд, которые используются для подключения к общим сетевым ресурсам, таких как утилита Net, или осуществляют поиск систем, доступных удаленно.

## Windows Remote Management (WinRM)

*Система:* Windows
*Права:* Пользователь, администратор
*Описание:* WinRM — это имя службы и протокола, который позволяет удаленное взаимодействие пользователя с системой (например, запуск файла, изменение реестра, изменение службы. Для запуска используется команда winrm и другие программы, такие как PowerShell. *Рекомендации по защите:* Отключите службу WinRM, если она необходима, то изолируйте инфраструктуру с WinRM с отдельными учетными записями и разрешениями. Следуйте рекомендациям WinRM по настройке методов проверки подлинности и использованию брандмауэров хоста, чтобы ограничить доступ к WinRM и разрешить доступ только с определенных устройств.