Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 6

habr.com/ru/articles/433566

Андрей Макеев

Получение учетных данных (Credential Access)

Ссылки на все части:

Заполучив учетные данные злоумышленник получает доступ или даже контроль над системой, доменом или служебными (технологическими) учетными записями. Противник, вероятно, будет пытаться заполучить легитимные учетные данные пользовательских и административных учетных записей, чтобы идентифицироваться в системе и получить все разрешения захваченной учетной записи, тем самым усложняя защищающей стороне задачу по обнаружению вредоносной активности. Противник также, при наличии возможности, может создавать учетные записи с целью их последующего использования в атакуемой среде.

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.

Манипулирование учетными записями (Account Manipulation)

Система: Windows
Права: Администратор
Описание: Манипулирование учетными записями направлено на подержание определенного уровня прав доступа в атакуемой среде. Манипуляции предполагают изменение разрешений, параметров учетной записи и способа проверки её

подлинности, добавление или изменение групп доступа. Действия злоумышленника могут быть направлены на подрыв политик безопасности, таких как срок действия пароля, с целью продления срока жизни скомпрометированных учетных записей. Для создания или управления учетными записями у противника уже должны быть достаточные разрешения в системе или домене.

Рекомендации по защите: Используйте многофакторную аутентификацию. Защищайте контроллеры домена, обеспечив ограничения доступа к этим системам. Исключите использование учетных записей администраторов домена в непривилегированных системах и для повседневных операций, которые могут способствовать их компрометации.

Bash History

Система: Linux, macOS
Права: Пользователь
Описание: Bash отслеживает команды, выполняемые пользователем с помощью утилиты History. Когда пользователь выходит из системы история сохраняется в файл *~/.bash_history*. Как правило, этот файл содержит 500 последних команд пользователя. Зачастую, в параметрах команд пользователь указывает имя пользователя и пароль, которые также сохранятся в *~/.bash_history* при выходе пользователя из системы. Атакующие могут просматривать файлы *~/.bash_history* различных пользователей системы в надежде заполучить учетные данные.

Рекомендации по защите: Существует несколько способов предотвращения записи истории команд в файл *~/.bash_history*:
• *set +o history* — отключить запись;
• *set -o history* — возобновить запись;
• *unset HISTFILE* — добавление в файл bash_rc;
• *ln -s /dev/null ~/.bash_history* — записать историю команд в */dev/null*.

Метод грубой силы или полный перебор (Brute Force)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Противник может применять средства подбора паролей когда учетные данные неизвестны или когда ему не удаётся получить хэш пароля. Противники могут применять техники систематизированного подбора, вычисляя подходящий кэш или используя радужные таблицы. Взлом хэшей обычно осуществляется вне атакуемой системы. Не зная пароль злоумышленники могут пытаться логиниться используя пустое значение пароля либо значение из списка возможных паролей. В зависимости от парольной политики такие действия могут привести к многочисленным ошибками аутентификации и блокировке учетной записи, поэтому противник может применять так называемое распыление паролей (password

sraying), суть которого заключается в переборе наиболее популярных или вероятных паролей с разными учетными записями. Это уменьшает вероятность блокировки, которая возникает при переборе множества паролей только с одной учетной записью.

Рекомендации по защите: Применяйте политики блокирования учетных записей после определенного количества неудачных попыток входа в систему. Рассмотрите возможность применения многофакторной аутентификации. Следуйте рекомендациям по предотвращению несанкционированного доступа к действующим учетным записям *(см. рекомендации по защите к технике «Действующие учетные записи (Valid accounts))*.

Дампинг учетных данных (Credential Dumping)

Система: Windows, Linux, macOS
Права: Администратор, System, root
Описание: Дампинг учетных данных (*англ. dumping — »захоронение отходов"*) — процесс получения логинов и паролей, как правило, в форме хэша или текстового пароля из операционной системы или программного обеспечения. Инструменты для дампинга учетных данных могут использоваться как злоумышленниками, так и тестировщиками безопасности.

Windows
SAM (Диспетчер учетных записей)
SAM — это база данных локальных учетных записей хоста. Как правило, в SAM хранятся учетные записи, которые показывает команда "*net user*". Для чтения SAM требуется доступ системного уровня. Существует множество инструментов для извлечения данных SAM из памяти:
• *pwdumpx.exe*;
• *gsecdump*;
• *Mimikatz*;
• *secretdump.py*.

Файл SAM можно извлечь из реестра с помощью утилиты REG:
```
reg save HKLM\sam sam;
reg save HKLM\system system.
```

Далее *Creddump7* поможет извлечь хэши из базы данных SAM.
Примечание:Rid 500 — это учетная запись встроенного локального администратора. *Rid 501* — гостевая учетная запись. Учетные записи пользователей начинаются с *Rid 1000+*.

Кэшированные учетные данные (DCC2)
Domain Cached Credentials v2 (DCC2) — это кэш учетных данных, используемый в Windows Vista и более поздних версиях для аутентификации пользователя, когда контроллер домена недоступен. Количество кэшированных учетных записей может

быть индивидуально для каждой системы. Этот хэш не подвержен атакам типа *pass-the-hash*. Для извлечения файла SAM из памяти применяются сл. инструменты:
• *pwdumpx.exe*;
• *gsecdump*;
• *Mimikatz*;
• *secretdump.py*
В качестве альтернативы также могут использоваться утилита Reg или Creddump7. Кэширование учетных данных в Windows Vista выполняется с использованием *PBKDF2* (стандарт формирования ключа из пароля).

Local Security Authority (LSA) Secrets
LSA Secrets — это хранилища кэшированных учетных, в которых система хранит учетные данные, включая пароли пользователей, учетных записей служб, пароли InternetExpolorer, SQL и другие приватные данные, например ключи шифрования кэшированных доменных паролей. Имея разрешения уровня System можно получить доступ к LSA Secrets, хранящихся в реестре: *HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets*.
Когда сервисы стартуют в контексте локальной или доменной учетной записи их пароли хранятся в реестре. Если включен автоматический вход в систему, приватные данные учетной записи так же хранятся в реестре. По аналогии с предыдущими методами дампинга для атаки на LSA Secret применяются всё те же инструменты:
• *pwdumpx.exe*;
• *gsecdump*;
• *Mimikatz*;
• *secretdump.py*
Файл SAM можно извлечь из реестра с помощью утилиты REG, а учетные данные с помощью Creddump7. Извлеченные из LSA Secret пароли закодированы в UTF-16, т.е. открытым текстом. В Windows 10 применяются дополнительные средства защиты LSA Secret.

NTDS from Domain Controller
Для аутентификации и авторизации в AD хранится информация о членах домена — устройствах и пользователях. База данных AD по умолчанию хранится на контроллере домена в файле *%SystemRoot%\NTDS\Ntds.dit*.
Для извлечения хэшей из базы данных AD применяются следующие методы и инструменты:
• *Volume Shadow Copy (теневая копия тома);*
• *ntdsutil.exe;*
• *secretdump.py;*
• *Invoke-NinjaCopy*.

Group Policy Preference (GPP) Files
GPP или предпочтения групповой политики — это XML файлы, описывающие различные параметры доменных политик, например, подключение сетевого диска в контексте определённой учетной записи или предустановка локальных учетных записей в доменных системах. Такие файлы могут содержать учетные данные. Групповые политики хранятся в SYSVOL контроллера домена, поэтому любой пользователь может прочитать файлы GPP и попытаться дешифровать содержащиеся в них пароли с помощью сл. инструментов:
• *Metasploit (post/windows/gather/credentials/gpp);*
• *Get-GPPPassword;*
• *gpprefdecrypt.py.*
Для идентификации всех XML-файлов на ресурсе SYSVOL можно использовать команду:
`dir /s *.xml`.

Service Principal Names (SPNs)
см. технику Kerberoasting

Plaintext Credentials
После того как пользователь вошел в систему генерируется множество учетных данных, которые сохраняются в память процесса Local Authority Subsystem Service (LSASS). Эти учетные данные могут быть собраны администратором или System.

SSPI (Security Support Provider Interface) предоставляет общий интерфейс для нескольких Security Support Providers (SSPs). SSP — программные модули (DLL), содержащие одну или несколько схем аутентификации и криптографии, которые загружаются в процесс LSASS при запуске системы.

Некоторые SSP могут быть использованы для получения учетных данных:
• Msv: интерактивный вход в систему, вход в качестве пакетного задания (batch logon), например, запуск заданий службы планировщика заданий, вход в систему в качестве службы осуществляется через пакет аутентификации MSV;
• Wdigest: Digest Authentication Protocol разработан для аутентификации в сети при использовании HTTP и SASL (Simple Authentication Security Layer);
• Kerberos: обеспечивает доменную аутентификацию в Windows 2000 и более поздних версиях;
• CredSSP: SSO (Single Sign-On — единый вход позволяет пользователям пройти проверку подлинности один раз и получать доступ к ресурсам без ввода учетных данных) и Network Level Authentication (применяется для аутентификации в Remote Desktop Services).

Инструменты для получения учетных данных:
• *Windows credential Editor;*
• *Mimikatz.*

Дамп процесса LSASS может быть сохранен для последующего анализа в другой системе.
На целевом хосте выполняется команда:
`procdump -ma lsass.exe lsass_dump`

Далее, в другой системе запускается Mimikatz:
`securlsa::Minidump lsassdump.dmp`
`sekurelsa::logonPasswords`.

DCSync
DCSync — разновидность дампинга учетных данных с контроллера домена. Злоупотребляя API-интерфейсом контроллера домена вместо использования вредоносного кода, который может быть опознан, злоумышленник может имитировать процесс репликации с удаленного контроллера домена. Члены групп Administrators, Domain Admins, Enterprise Admins или учетные записи компьютеров могут запускать DCSync для получения парольной информации из AD, которая может включать хэши доменных аккаунтов таких как KRBTGT (Key Distribution Center Service Account, использовалась в Windows 2000 для работы службы Key Distribution Center) и Administrator. Затем хэши могут быть использованы для создания Golden Ticket и проведения атаки Pass the Ticket или изменения пароля в рамках манипуляций с аккаунтами (Account Manipulation). Функциональность DCSync включена в модуль lsadump, входящий в состав Mimikatz. Lsadump также поддерживает NetSync для выполнения репликации по устаревшему протоколу.

Linux
Файловая система Proc
Proc — это специальная файловая система в Unix-подобных ОС, которая представляет информацию о процессах и другую системную информацию в виде иерархической псевдофайловой структуры (файлы существуют не на диске, а в оперативной памяти), которая действует как интерфейс для взаимодействия с пространством ядра ОС. Процессы, запущенные с правами root, могут выполнять очистку памяти других запущенных программ. Если программа хранит в своей памяти пароли в открытом виде или в виде хэш, то эти значения могут быть извлечены из \Proc для дальнейшего использования или попытки восстановления пароля из хэш. Gnome Keyring, sshd и Apache используют память для хранения таких аутентификационных «артефактов». Вышеописанная функциональность реализована в инструменте с открытым кодом — MimiPenguin, который выгружает память процесса и затем ищет пароли и хэши в текстовых строках и regex-шаблонах.

Рекомендации по защите:
Windows
Пытайтесь отслеживать доступ к LSASS и SAM, осуществляемый разрешенными в защищаемой системе инструментами. Ограничивайте права учетных записей в различных системах и сегментах сети, чтобы предотвратить возможность продвижения злоумышленника по защищаемой сети в случае получения паролей и

хэшей. Убедитесь, что учетные данные локального администратора имеют сложные и уникальные пароли во всех системах и сегментах сети. Не помещайте учетные записи пользователей или администраторов домена в группы локальных администраторов в различных системах, т.к. это эквивалентно тому, что у всех администраторов есть один и тот же пароль. Следуйте рекомендациям Microsoft по разработке и администрированию корпоративной сети. В Windows 8.1 и Windows Server 2012 R2 включите защиту процесса LSA (Protected Process Light).

Идентифицируйте и блокируйте потенциально-опасное и вредоносное программное обеспечение, которое может быть использовано для получения дампов учетных данных.

В Windows 10 для защиты LSA Secrets применяется новый механизм — Credential Guard в Защитнике Windows. С его появлением процесс LSA не хранит приватные данные в памяти, а взаимодействует с новым компонентом — изолированным процессом, который отвечает за хранение и защиту LSA Secrets. Данные, хранящиеся в изолированном процессе защищены с помощью виртуализации и недоступны для остальной части операционной системы. LSA взаимодействует с изолированным процессом с помощью удаленных вызовов процедур (RPC). Credential Guard не настроен по умолчанию и имеет требования к аппаратному и программному обеспечению. Однако, он также не является абсолютной защитой от всех форм дампинга учетных данных.

Управляйте доступом Replicating Directory Changes и другими разрешениями, связанными с репликацией контроллера домена. Рассмотрите возможность отключения или ограничения NTLM-траффика. Рассмотрите необходимость мониторинга процессов и аргументов команд запуска программ, которые могут выступать индикаторами дампинга учетных данных. Например, инструменты удаленного доступа могут содержать такие средства как Mimikatz или PowerShell-сценарии типа Invoke-Mimikatz PowerSploit.

Контролируйте журналы репликации контроллеров домена на предмет незапланированных репликаций или запросов на репликацию. Также отслеживайте трафик, содержащий запросы на репликацию от сторонних IP-адресов.

Linux
Для получения паролей и хэшей из памяти, процесс должен открыть в системе файл */proc/PID/maps*, где *PID* — уникальный pid процесса. Инструмент мониторинга AuditD может использоваться для выявления враждебных процессов, открывающих этот файл и предупреждая о pid, имени процесса и других аргументах контролируемой программы.

Учетные данные в файлах (Credentials in Files)

Система: Windows, Linux, macOS
Права: Администратор, System, root

Описание: Злоумышленники могут искать в локальных файловых системах и удаленных общих папках файлы, содержащих пароли. Это могут быть файлы, созданные пользователями для хранения собственных учетных данных, общие хранилища учетных данных группы людей, файлы конфигурации, содержащие пароли для систем или служб, файлы исходного кода и двоичные файлы, содержащие пароли.
Используя инструменты дампинга учетных данных пароли также можно извлекать из резервных копий, образов и снапшотов виртуальных машин. Кроме того пароли могут содержаться в файлах настроек групповых политик (GPP), хранящихся на контроллере домена.

Рекомендации по защите: Применяйте организационные меры, запрещающие хранение паролей в файлах. Убедитесь, что разработчики и системные администраторы знают о рисках, связанных с хранением паролей в открытом виде в файлах конфигураций ПО. Проводите периодический мониторинг наличия в вашей системе файлов, содержащих пароли с их последующим удалением.
Ограничивайте общий доступ к файлам в определенных каталогах выдавая разрешения только нужным пользователям. Удалите файлы GPP, содержащие уязвимые настройки групповых политик.

Учетные данные в Реестре (Credentials in Registry)

Система: Windows
Права: Пользователь, администратор
Описание: Злоумышленники могут искать в реестре Windows учетные данные и пароли, которые хранятся там для использования программами или службами, иногда учетные данные хранятся для автоматического входа. Примеры команд для поиска парольной информации:

```
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s
```

Рекомендации про защите: Не храните учетные данные в реестре. Проводите мониторинг реестра на предмет наличия учетных данных. При необходимости хранения учетных данных ПО должно обеспечивать ограничение их разрешений в целях предотвращения возможности злоупотребления этими данными.

Эксплойты для получения учетных данных (Exploitation for Credential Access)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Ошибки, допущенные разработчиками механизмов аутентификации и авторизации, могут быть причиной наличия в ПО уязвимостей с помощью которых злоумышленник может получить несанкционированный доступ к учетным данным.

Например, в бюллетене MS14-068 описана уязвимость в протоколе Kerberos, с помощью которой злоумышленник может подделать билеты Kerberos используя права доменного пользователя. Эксплуатация уязвимостей для получения учетных данных может также применяться для повышения привилегий.

Рекомендации по защите: Регулярно обновляйте ПО используя централизованное управление установкой обновлений для рабочих станций и серверов предприятия. Разработайте и внедрите процесс выявления и анализа киберугроз в рамках которого будут определяться актуальные для вашего предприятия угрозы. Применяйте песочницы, средства виртуализации и микросегментации чтобы затруднить возможность продвижения злоумышленника с помощью эксплуатации уязвимостей. В ОС Windows доступны средства выявления активности, связанной с эксплуатацией уязвимостей, речь идёт о Windows Defender Exploit Guard (WDEG) и Enchanced Mitigation Experience Toolkit (EMET). Ещё один из способов предотвращения эксплуатации уязвимостей — это применение средств Control-flow integrity (CFI). CFI — это общее название методов, направленные на ограничение возможных путей исполнения программы в пределах заранее предсказанного графа потока управления. Однако, многие методы защиты могут не сработать, если вредоносное ПО разработано для уколенения от защитных мер, это также зависит от архитектуры анализируемой программы и её двоичных файлов.

Форсированная аутентификация (Forced Authentication)

Система: Windows
Права: Пользователь
Описание: Для аутентификации и коммуникации между windows-системами в рамках совместного использования ресурсов и сетевых файловых папок обычно используется протокол Server Message Block (SMB). Когда Windows пытается подключиться к удаленной системе по SMB, она автоматически пытается аутентифицировать пользователя и отправляет учетные данные текущего пользователя в удаленную систему, поэтому пользователю не нужно вводить учетные данные для получения доступа к сетевым ресурсам, что характерно для корпоративной среды. В качестве резервного протокола совместного использования ресурсов, в случае отказа инфраструктуры SMB, может использоваться протокол Web Distributed Authoring and Versioning (WebDAV), который является расширением протокола HTTP и обычно работает через TCP-порты 80 и 443.

Вызывая принудительную аутентификацию по SMB, злоумышленники могут злоупотреблять поведением атакуемой системы во время её подключения к удаленной системе и получать хэши учетных записей. С помощью техник фишинга противник может отправить жертве ссылку на контролируемый внешний ресурс или разместить специальный файл на рабочем столе или на общедоступном ресурсе. Когда пользовательская система обратится к ненадежному ресурсу она попытается выполнить аутентификацию и отправить по по протоколу SMB на удаленный сервер

хешированные учетные данные текущего пользователя. Получив хэш злоумышленник может выполнить офлайн-брутфорс и получить учетные данные в открытом виде или использовать их для атак Pass-the-Hash.

Рассмотрим наиболее популярные способы вызова принудительной SMB-аутентификации:
• Фишинговое вложение, содержащее документ с активным содержимым, которое автоматически загружается при открытии документа. Документ может включать запрос типа file[:]//[remote address]/Normal.dotm/, который инициирует аутентификацию по SMB.

• Модифицированный файл .lnk или .SCF (Windows Explorer Command File), содержащий в свойствах вместо пути к значку файла, внешнюю ссылку \[remote address]\pic.png. Таким образом, система будет пытаться загрузить значок файла и откроет ссылку.

Рекомендации по защите: Блокируйте исходящий SMB-трафик, направленный за пределы корпоративной сети, путем фильтрации и блокирования TCP-портов 139, 445 и UDP-порта 137. Фильтруйте и блокируйте выход WebDAV-трафика за пределы корпоративной сети. Если доступ к внешним ресурсам через SMB и WebDAV необходим, то ограничивайте внешние подключения с помощью белых списков.

Hooking (Зацепление)

Система: Windows
Права: Администратор, System
Описание: API функции Windows обычно хранятся в DLL-библиотеках. Техника перехвата заключается в перенаправлении вызовов API-функций посредством:

• Hook-процедуры — это встроенные в ОС процедуры, которые выполняют код при вызове различных событий, например, нажатие клавиш или перемещение мыши;

• Модификации адресной таблицы (IAT), в которой хранятся указатели на API-функции. Это позволит «обмануть» атакуемое приложение, заставив его запустить вредоносную функцию;

• Непосредственного изменения функции (сплайсинг), в ходе которого меняются первые 5 байт функции, вместо которых вставляется переход на вредоносную или иную функцию, определенную злоумышленником.

Подобно инъекциям, злоумышленники могут использовать hooking для исполнения вредоносного кода, маскировки его выполнения, доступа к памяти атакуемого процесса и повышения привилегий. Злоумышленники могут захватывать вызовы API, включающие параметры, содержащие аутентификационные данные.
Hooking обычно применяется руткитами для скрытия вредоносной активности в системе.

Рекомендации по защите: Перехват событий в ОС является частью нормальной работы системы, поэтому какое либо ограничение данной функциональности может негативно влиять на стабильность работы законных приложений, например антивирусного ПО. Усилия по предотвращению применения техник перехвата необходимо сосредоточить на более ранних этапах цепочки killchain. Обнаружить вредоносную hooking-активность можно с помощью мониторинга вызовов функций SetWindowsHookEx и SetWinEventHook, использования детекторов руткитов, анализа аномального поведения процессов, например, открытия сетевых подключений, чтение файлов и т.п.

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 коды 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 (https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#a-nameesaebmaesae-administrative-forest-design-approach).

Кейлогеры 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`.

Запрос ввода (Input Prompt)

Система: macOS
Права: Пользователь
Описание: При выполнении программ, требующих повышения привилегий, операционная система обычно запрашивает у пользователя соответствующие учетные данные. Злоумышленники могут имитировать эту функцию, чтобы запрашивать ввод учетных данных с помощью стандартной формы запроса. Эта форма запроса учетных данных может быть вызвана с помощью AppleScript:

```
set thePassword to the text returned of (display dialog "AdobeUpdater needs permission to check for updates. Please authenticate." default answer "")
```

Злоумышленник будет вызывать запрос на ввод учетных данных имитируя нормальное поведение ОС, например, поддельный установщик или пакет удаления вредоносных программ требует подтверждения соотвествующих полномочий.

Рекомендации по защите: Проводите обучение пользователей, чтобы они знали какие программы могут запрашивать разрешение и почему. Настройте обязательную проверку запускаемых сценариев AppleScript на наличие в них подписи доверенного разработчика.

Kerberoasting

Система: Windows
Права: Пользователь
Описание: Каждый экземпляр службы имеет уникальный идентификатор — Service Principal Name (SPN), который используется для проверки подлинности в Kerberos. SPN должен быть связан только с одной учетной записью, установщик службы записывает SPN в свойства учетной записи в AD.

Злоумышленники, имеющие действующий билет Kerberos ticket-granting ticket (TGT) могут запросить у службы Kerberos ticket-granting service (TGS) один или несколько сервисных билетов (service ticket) для взаимодействия с любым SPN, зарегистрированным на контроллере домена. Элементы сервисных билетов могут быть зашифрованы алгоритмом RC4, таким образом Kerberos 5 TGS-REP etype 23, который содержит хэш пароля учетной записи, связанной с целевой SPN и используемый в качестве приватного ключа (см. описание Kerberos) является

уязвимым и подвержен взлому посредством брутфорса. Эта же атака может быть выполнена с использованием сервисных билетов, полученных из сетевого трафика. Взломав полученный хэш противник может использовать действующую учетную запись для закрепления в системе, эскалации привилегий или дальнейшего продвижения по сети.

Рекомендации по защите: Применяйте сложные и длинные пароли (идеальный вариант 25+ знаков) для учетных записей служб и обеспечьте периодичность их смены. В ОС начиная с Windows Server 2012 доступна технология Group Managed Service Accounts (gMSA), которая предназначена для автоматической смены пароля служебных (технологических) учетных записей с возможностью их одновременного использования на нескольких серверах. В качестве альтернативы рассмотрите возможность использования хранилищ паролей сторонних производителей.

Ограничивайте права учетных записей предоставляя минимальные требуемые привилегии, исключайте членство учетных записей в привилегированных группах типа Domain Admins.
По возможности включите шифрование AES Kerboros или другой более сильный алгоритм шифрования, исключив использование RC4.

Включите аудит Kerberos Service Ticket Operations для журналирования запросов билетов службы Kerberos TGS. Исследуйте аномальные шаблоны активности, например, события Event ID 4769 — учетные записи, выполняющие многочисленные запросы в течение небольшого периода времени, особенно, если они запрашивали шифрование RC4 (Ticket Encryption Type: 0x17).

Keychain

Система: macOS
Права: root
Описание: Keychain (англ. «связка ключей») — это встроенное в macOS хранилище учетных записей и паролей для множества сервисов и фичей, таких как WiFi, веб-сайты, защищенные заметки, сертификаты и Kerberos. Файлы Keychain расположены в:
• *~/Library/Keychains;*
• */Library/Keychains;*
• */Network/Linrary/Keychains/.*

Встроенная по умолчанию в macOS консольная утилита *Security* предоставляет удобный способ управления учетными данными.
Для управления своими учетными данными пользователи должны использовать дополнительную учетную запись, предоставляющую доступ к их связке ключей. Если злоумышленник знает учетные данные от связки ключей пользователя, то он

может получить доступ ко всем остальным учетным данным, хранящимся в keychains этого пользователя. По умолчанию, для входа в Keychains применяется текущая учетная запись пользователя для входа в систему.

Рекомендации по защите: Разблокировка Keychains пользователя и использование из неё паролей — распространенный процесс, который не останется без внимания средств обнаружения вредоносной активности.

Отравление LLMNR/NBT-NS (LLMNR/NBT-NS Poisoning)

Система: Windows
Права: Пользователь
Описание: Link-Local Multicast Name Resolution (LLMNR) и NetBIOS Name Service (NBT-NS) — это протоколы, включенные во все версии Windows, которые служат альтернативным способом идентификации хоста. LLMNR базируется на формате DNS и разрешает сетевые имена соседних компьютеров без использования DNS. NBT-NS идентифицирует систему в локальной сети по её NetBIOS-имени.

Злоумышленник может подделать доверенный источник разрешения имен, который будет отвечать на трафик LLMNR (UDP5355)/NBT-NS(UDP137), чтобы жертва коммуницировала с контролируемой противником системой. Если запрашиваемый хост потребует идентификации/аутентификации, то имя пользователя и хеш NTLMv2 текущего пользователя хоста-жертвы будут отправлены в контролируемую противником систему. Таким образом, злоумышленник с помощью сетевого сниффера может собирать передаваемые хэши и затем в автономном режиме пытаться получить из них пароли с помощью средств перебора.
Существует несколько инструментов, которые могут использоваться для атак на службы имен в локальных сетях: NBNSpoof, Metasploit и Responder.

Рекомендации по защите: Рассмотрите возможно отключения LLMNR и NBT-NS в локальных настройках безопасности хоста или с помощью групповой политики. Используйте локальные средства безопасности, блокирующие LLMNR/NBT-NS-траффик.
Проверьте, что LLMNR отключен в реестре: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\EnableMulticast=dword:00000000`.
Если LLMNR/NBT-NS отключены политикой безопасности, то мониторинг трафика портов UDP5355 и UDP137 поможет обнаружить атаку.

Прослушивание сети (Network Sniffing)

Система: Windows, Linux, macOS
Описание: Злоумышленник может использовать сетевой интерфейс в режиме promiscuos mode («неразборчивый» режим), в котором сетевая плата будет принимать все пакеты независимо от того кому они адресованы или использовать

span-порты (порты зеркалирования) для захвата большого объема данных, передаваемых по проводным или беспроводным сетям.
Захваченные в ходе сниффинга данные могут содержать учетные данные отправленные через незащищенные соединения без использования протоколов шифрования. Различные атаки на сетевые службы имен типа отравления LLMNR/NBT-NS путем перенаправления трафика также могут использоваться для сбора учетных данных на веб-сайтах, прокси-серверах и внутренних системах.

В ходе прослушивание сети противник так же может выявить различные сведения о конфигурации (запущенные службы, номера версий, IP-адреса, имена хостов, VLAN ID и т.п.) необходимые для дальнейшего продвижения по сети и/или обхода средств защиты.

Рекомендации по защите: Убедитесь, что беспроводной трафик соответствующим образом зашифрован. По возможности, используйте Kerberos, SSL и многофакторную аутентификацию. Проводите мониторинг сетевых коммутаторов на предмет использования span-портов, отравления ARP/DNS и несанкционированных изменений конфигурации маршрутизатора.
Применяйте средства выявления и блокировки потенциально-опасного ПО, которое может быть использовано для перехвата и анализа сетевого трафика.

DLL-библиотеки фильтров паролей (Password Filter DLL)

Система: Windows
Права: Администратор, System
Описание: Фильтры паролей Windows — механизмы применения парольной политики для доменных и локальных учетных записей. Фильтры реализованы в виде DLL-библиотек, содержащих методы проверки соответствия потенциальных паролей требованиям политики безопасности. DLL фильтров паролей размещаются на хостах для локальных учетных записей и контроллерах домена для доменных аккаунтов.

Перед регистрацией новых паролей в Security Accounts Manager (SAM), служба Local Security Authority (LSA) запрашивает проверку паролей каждым зарегистрированным в системе фильтром паролей. Любые потенциальные изменения не вступят в силу прока каждый фильтр не подтвердит успешность проверки.

Злоумышленник может зарегистрировать в атакуемой системе вредоносные фильтры паролей с целью сбора учетных данных. Для проведения проверки сложности фильтры получают от LSA пароли открытым текстом. Вредоносные фильтры будут получать учетные данные открытым текстом при каждом запросе пароля.

Рекомендации по защите: Убедитесь, что в вашей системе зарегистрированы только валидные фильтры паролей. DLL фильтров по умолчанию хранятся в *C:\Windows\System32* и должны иметь соответствующую запись в реестре: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\[Notification Packages]`.
Вновь установленные фильтры паролей вступают в силу после перезагрузки системы, появляются в автозапуске и загружены в lsass.exe

Секретные ключи (Private Keys)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Закрытые ключи и сертификаты используются для аутентификации, шифрования/дешифрования и цифровых подписей.
Злоумышленник может собирать секретные ключи на компрометированных системах для дальнейшего использования при аутентификации в сервисах удаленных подключений типа SSH или расшифровки других собранных файлов, например, файлов данных электронной почты.

Файлы ключей и сертификатов имеют такие расширения как *.key, .pgp, .gpg, .ppk, .P12, .pem, .pfx, .cer, p7b, .asc*. Противник может искать файлы в каталогах ключей, например *~/.ssh* в *nix-системах или *C:\Users (username.ssh)* в Windows.

В процессе использования закрытые ключи должны запрашивать пароль или парольную фразу, поэтому противник параллельно может использовать технику захвата ввода для кейлоггинга или пытаться подобрать парольную фразу в автономном режиме.

Рекомендации по защите: Используйте сложные парольные фразы, чтобы затруднить взлом секретных ключей. Храните ключи на внешних криптографических носителях когда это возможно. Убедитесь, что доступ к критичным ресурсам открыт только для авторизованных ключей и регулярно проверяйте списки доступа.

Убедитесь в правильности разрешений в папках, содержащих секретные ключи. Используйте изолированную инфраструктуру для управления критическими системами, чтобы предотвратить коллизии учетных записей и разрешений, которые могут использоваться для перемещения по сети. Следуйте рекомендациям по защите от техник злоупотребления действующими учетными записями.

Организуйте мониторинг доступа к файлам и каталогам, связанным с криптографическими ключами и сертификатами, а также проводите аудит журналов проверки подлинности, выявляя аномальные действия, указывающие на неправильное использование ключей или сертификатов для удаленной проверки подлинности.

Взлом цепочки паролей в OS X (Securityd Memory)

Система: macOS
Права: root
Описание: В OS X до версии EL Capitan пользователи с правами root могут читать из Keychain пароли вошедших в систему пользователей в виде открытого текста. Это связано с тем, что для удобства пользователей Apple позволяет системе кэшировать учетные данные, чтобы не запрашивать у пользователей их повторный ввод при каждой необходимости.

Пароли, хранящиеся в связке Keychain многократно зашифрованы с помощью набора ключей. Ключи в свою очередь зашифрованы с помощью других ключей, хранящихся в том же файле, наподобие русской матрёшки. Мастер-ключ, который может открыть внешнюю матрешку и каскадно запустить расшифровку следующей матрешки представляет собой нечто иное, как зашифрованный с помощью PBKDF2 пароль, с которым пользователь вошёл в систему. Таким образом, для чтения первого пароля в пользовательской цепочке паролей необходим его пароль для входа или мастер-ключ. Обработка операций с keychain осуществляется процессом securityd, для этого в его памяти хранится мастер-ключ.

Имя права root, злоумышленник может сканировать память с целью поиска ключей шифрования цепочки keychain поэтапно расшифровав всю последовательность паролей пользователя, WiFi, почты, браузеров, сертификатов и т.п.

Перехват двух-факторной аутентификации (Two-Factor Authentication Interception)

Система: Windows, Linux, macOS
Права: Администратор, System, root
Описание: Использование двухфакторной и многофакторной аутентификации обеспечивает более высокий уровень безопасности, чем одна связка логин/пароль, однако организации должны знать о методах перехвата и обхода этих механизмов безопасности.

Злоумышленники могут целенаправленно использовать такие механизмы аутентификации как смарт-карты, для получения доступа в систему, сервисам и сетевым ресурсам.
Если для двухфакторной аутентификации (2FA) используется смарт-карта, то для получения пароля, связанного со смарт-картой при обычном использовании потребуется кейлоггер. Как со вставленной смарт-картой так и с паролем доступа к смарт-карте противник может подключиться к сетевому ресурсу, используя зараженную систему для проксирования аутентификации с использованием вставленного аппаратного токена.

Злоумышленники могут также нацелить кейлоггер для аналогичной атаки на другие аппаратные токены, такие как RSA SecurID. Захват ввода токена (включая личный идентификационный код пользователя) может обеспечить противнику временный доступ на период действия полученного одноразового пароля, а возможно позволит ему вычислить будущие значения одноразовых паролей (зная алгоритм и начальное значение для генерации последующих временных паролей).

Другие методы 2FA также могут быть перехвачены и использованы противником для несанкционированной аутентификации. Обычно однократные коды отправляются по внеполосным каналам связи (смс, электронная почта и т.п.). Если устройство и\или служба не защищены, то они могут быть уязвимы для перехвата.

Рекомендации по защите: Обеспечьте удаление смарт-карт, когда они не используются. Защищайте устройства и службы, используемые для передачи и получения внеполосных кодов. Выявляйте и блокируйте потенциально-опасное и вредоносное ПО, которое может использоваться для перехвата учетных данных в 2FA.