Инженерный вестник Дона, №3 (2026)
ivdon.ru/ru/magazine/archive/n3y2026/10810

О подходе к выбору инструмента для исследования Active Directory

А.А. Обласов, Д.В. Воропаев

Комсомольский-на-Амуре государственный университет

Аннотация: В работе рассмотрен подход к выбору инструмента для исследования уязвимостей службы каталогов Active Directory, в которой содержится информация, представляющая ценность для злоумышленников, дающая возможность определить лучшую точку для проникновения в систему и разработать оптимальную стратегию и тактику для реализации эффективной и быстрой атаки. В рамках данной работы проведен анализ возможных угроз службы каталогов и приведена классификация атак на Active Directory. Приведена классификация инструментов используемых для получения полезной информации из Active Directory. Рассмотрены возможности Cobalt Strike как инструмента эмуляции угроз и проведения постэксплуатационных задач на основе скрытого агента и обновляемой базы атакующих скриптов. Проведен анализ практической реализации кибератак с применением инструмента Cobalt Strike за последние несколько лет. Изучена и пошагово детализирована методика таких кибератак.
Ключевые слова: информационная безопасность, кибератака, сценарии атак, анализ угроз, служба каталогов, Active Directory, Cobalt Strike.

Введение

Взрывной рост информационных систем является необходимым условием для реализации стратегии цифровой трансформации. Переход бизнес-процессов на «цифру» генерирует колоссальные объемы данных [1], для обработки и хранения которых требуются мощные новые масштабируемые, информационные системы. Автоматизация процессов и внедрение искусственного интеллекта требуют интеграции сложных аналитических платформ в существующие ИТ-архитектуры компаний. Экосистемный подход подразумевает объединение разрозненных сервисов в единые многоуровневые информационные экосистемы [2]. Облачные технологии, интернет вещей, цифровые двойники, цифровые финансы и многие другие цифровые технологии – являются основными катализаторами развития информационных систем и роста их числа.

В 2026 году защита информации и информационных систем является критическим элементом выживания бизнеса и национальной безопасности,

требующим постоянного роста инвестиций. Все эти факты и обстоятельства создают условия, в которых наблюдение за информационными системами становится все более глубоким, разбор единичных конкретных событий – всё более кропотливым, а контроль информационных системам – критически важным аспектом для эффективного обеспечения информационной безопасности и стабильной работы организаций и предприятий в целом [3].

Одним из ключевых элементов корпоративной информационной системы является служба каталогов Active Directory (далее AD), которая играет центральную роль в управлении идентификацией и доступом пользователей к ресурсам системы [4].

В процессе проведения внутренней разведки злоумышленники используют широкий спектр методов для сбора исчерпывающих данных об AD.

Первоначальной целью является компрометация учетных записей пользователей и групп, что позволяет определить вектор и идентифицировать потенциальные объекты для дальнейших атак.

Получив несанкционированный доступ, злоумышленники анализируют существующие связи между пользователями [5], группами и компьютерами, выявляя уязвимости, способствующие эскалации привилегий, и определяя оптимальные маршруты для продвижения вглубь инфраструктуры.

Тщательный анализ структуры каталога позволяет злоумышленникам стратегически планировать свои действия и существенно снижать вероятность обнаружения. Активно используются специализированные программы и различные скрипты, автоматизирующие процессы сбора информации и генерации отчетов о конфигурации AD, что значительно упрощает задачу всестороннего исследования сетевой среды.

Служба каталогов AD, представляя повышенный интерес для злоумышленников, является источником повышенных рисков для безопасности информационных систем. Чтобы эффективно управлять рисками информационной безопасности, необходимо их идентифицировать, выявить возможные угрозы, оценить вероятность реализации, степень их воздействия на информационную систему и в дальнейшем выработать эффективную методику минимизации выявленных рисков [6].

Типология атак на AD

Типология распространённых видов атак на AD:

1. Атаки «Pass-the-Hash» (передай хэш).

Злоумышленники получают хэш пароля администратора и используют его для доступа к ресурсам без знания реального пароля [7].

2. Атаки «DNS» (Domain Name System – система доменных имён).

Вид атак, направленный на компрометацию сетевой инфраструктуры, позволяющий злоумышленнику через подмену DNS-записей перенаправлять пользователей на поддельные сайты [4].

3. Атаки «DHCP» (Dynamic Host Configuration Protocol – протокол динамической конфигурации хоста).

Вид атак, направленный на компрометацию сетевой инфраструктуры, через подмену DHCP-сервера, позволяющий злоумышленнику раздавать вредоносные сетевые настройки [4].

4. Атаки «Kerberoasting» (атака на сетевой протокол аутентификации Kerberos).

Атаки направляются против сервисных учётных записей, атакуя их билеты Kerberos [7]. Получив билет, злоумышленник может расшифровать пароль сервиса.

5. Атаки «DCSync» (Domain Controller Sync - синхронизация контроллер домена).

Вид атак, позволяющий злоумышленнику выдавать себя за контроллер домена с целью получения учетных данных.

6. Атаки «Golden Ticket» (золотой билет) [7].

Используется злоумышленником для подделки билетов Kerberos, предоставляющих полный контроль над системой [7]. Обычно осуществляется после захвата KDC (Key Distribution Center – центр выдачи ключей).

7. Атаки «Silver Ticket» (серебряный билет).

Атаки, похожие на Golden Ticket, но фокусирующиеся на поддельных билетах Kerberos для отдельных сервисов, позволяющих злоумышленнику обойти стандартные процедуры авторизации.

8. Атаки «Brute force» (перебор паролей).

Переборные атаки позволяют злоумышленникам подбирать учётные записи с простыми паролями, многократно пробуя разные комбинации [4].

9. Атаки «Side-channel» (побочный канал).

Атаки, нацеленные на сбор побочных каналов передачи данных, таких как временные метрики запросов, потребление энергии процессора и другое поведение аппаратных устройств [4].

Успешные атаки на AD дают возможность для реализации рисков вирусных заражений, распространения вредоносного ПО [4], утечки конфиденциальной информации, социального инжиниринга или блокировки работы всей информационной системы.

AD – не просто инструмент управления информационными системами, а стратегическое решение, формирующее основу для эффективной работы организаций в цифровую эпоху и представляющее интерес для злоумышленников, что соответственно требует повышенного внимания со стороны служб информационной безопасности.

Для реализации эффективной защиты информационной системы необходимо чёткое понимание возможностей, методов и средств, которые могут использовать злоумышленники [8]. Несмотря на использование гетерогенных сред, мультиплатформенного ПО [9], многие принципы защиты и процессы администрирования схожи.

С уверенностью можно утверждать, что киберпреступники способны создавать собственные уникальные инструменты для проникновения и исследования Active Directory, но такая деятельность требует много времени и усилий. В большинстве случаев, хакеры предпочитают использовать уже имеющиеся инструменты как более практичное готовое решение.

Классификация инструментов для атаки на AD

Приведем классификацию инструментов, используемых для получения полезной информации из AD на три основные группы:

1) встроенные инструменты;

2) сторонние утилиты и инструменты с открытым кодом;

3) коммерческие продукты для аудита и управления информационной безопасностью.

К первой группе относятся следующие встроенные инструменты:

1. Repadmin: Мощный инструмент командной строки для диагностики проблем репликации в Active Directory.

2. DCDiag: позволяет проверить работоспособность контроллеров домена, включая проверку DNS, связанную с проблемами репликации.

3. Active Directory Administrative Center: Центр администрирования AD с графическим интерфейсом.

4. PowerShell: Предназначен для управления объектами и выполнения различных операций с помощью скриптов.

Существуют сторонние утилиты и инструменты с открытым исходным кодом, предназначенные для работы с AD и выделенные во вторую группу:

1. AdFind: представляет консольную программу, предназначенную для получения разнообразной информации из AD.

2. Enum4linux: Средство для сбора данных из Windows и Samba систем, позволяющее выявлять пользователей, группы, общие папки и другие ресурсы.

3. CrackMapExec (CME): Комплексный фреймворк для проведения аудита безопасности сетей с функциями разведки, перечисления учетных данных и анализа параметров настройки AD.

4. Impacket: Библиотека Python классов для взаимодействия с сетевыми протоколами, включающая большое количество инструментов для работы с AD, выполнения запросов и использования найденных уязвимостей.

5. Mimikatz: Известный инструмент для извлечения паролей в открытом виде, хешей, PIN-кодов и Kerberos-билетов из памяти [7], что критически важно для постэксплуатации.

6. Recon-AD: Инструмент, который собирает информацию об AD и генерирует подробный HTML-отчет, дающий полное представление о текущем состоянии среды AD.

В третью группу мы выделим коммерческие продукты для аудита и управления информационной безопасностью, ориентированные на системных администраторов и специалистов в области защиты информации. В качестве примера приведем следующие программные продукты:

1. ADManager Plus: Комплексное веб-решение, предназначенное для упрощения и автоматизации управления AD и создания детализированной отчётности.

2. ADAudit Plus: Мощное веб-решение для аудита изменений в AD и создания отчётов об этих изменениях. В связке с ADManager Plus, ADAudit Plus обеспечивает комплексный контроль над Active Directory, от управления до мониторинга и аудита.

3. Netwrix Auditor: Инструмент, выявляющий потенциальные утечки данных и причины внесения изменений в настройки ИТ-систем, поскольку собирает данные аудита комплексно.

4. Cobalt Strike: представляет собой инструмент для специалистов по безопасности, способную имитировать реалистичные кибератаки, предоставляя возможность выявления уязвимостей и выполнения тестов на проникновение [11].

Сегодня рынок коммерческих инструментов очень разнообразен, и приведённый список можно значительно расширить, постоянно появляются новые программы, совершенствуется встроенная защита, но в целом данная классификация и примеры отражают основной функционал и специфические особенности каждой группы [4]. Выбор конкретного инструмента зависит от поставленной задачи: от ручного поиска данных администратором до автоматизированного сканирования сети в рамках аудита безопасности или теста на проникновение. В некоторых случаях предполагается использование нескольких инструментов [5] для получения развёрнутого анализа и более полной картины [4].

Анализ практической реализации атак с применением инструмента Cobalt Strike

Так, в ноябре 2022 года компания Google заявила об обнаружении 34 скомпрометированных вариантов Cobalt Strike, которые использовались злоумышленниками [10]. По данным Google Cloud Threat Intelligence (облачная разведка угроз), эксперты выявили модифицированные версии Cobalt Strike, начиная с версии 1.44 и заканчивая 4.7, представленные 275 уникальными JAR-файлами [10].

В августе 2023 года аналитики кибербразведки российской компании BI.ZONE, занимающейся управлением цифровыми рисками и обеспечением кибербезопасности, зафиксировали масштабную кампанию атак хакерской

группы Lone Wolf, нацеленную на российские предприятия логистики, производства, финансов и розничной торговли [11]. В этих атаках использовалось программное обеспечение (далее ПО) Cobalt Strike [11].

«Лаборатория Касперского» представила информацию о новой серии кибернападений с применением Cobalt Strike Beacon – законного инструмента для удаленного администрирования. При этом его активно используют для несанкционированного доступа к информационным системам с целью хищения конфиденциальной информации [12]. Зловредное ПО распространяется через зашифрованный код, который размещают в профилях на популярных цифровых платформах, таких как GitHub, Microsoft Learn Challenge, Quora и различных в том числе и российских социальных сетях [12].

Такие атаки впервые были зарегистрированы во второй половине 2024 года. Их жертвами были организации в России, Китае, Японии, Малайзии и Перу [12]. В 2025 году активность снизилась, но эксперты продолжают наблюдать всплески.

Анализ атак выявил типичную схему: киберпреступники начинают с отправки обманных писем, маскирующихся под корреспонденцию от известных госкорпораций (зачастую из нефтегазовой сферы) [12], выражающих заинтересованность в продукции или услугах потенциальных жертв. К письмам прикреплен вредоносный архив с файлами, встроенными в PDF-документы, которые имитируют содержание служебных данных. В действительности, внутри находятся исполняемые файлы (EXE и DLL) [12], содержащие вредоносное ПО.

В качестве инструментария для активации зараженного ПО злоумышленники применяют технику подмены DLL (Dynamic Link Library – динамическая библиотека ссылок) [12], а также используют легитимную утилиту, предназначенную для отправки отчетов об ошибках –

первоначально разработанную для оперативного информирования разработчиков о проблемах в работе приложений [12].

Возможности Cobalt Strike как инструмента для проведения постэксплуатационных задач

Злоумышленники, применяя мошеннические схемы, заменяют настоящие файлы инфицированными, заставляя пользователей открыть последние вместо подлинных [11,12]. Успешный запуск вредоносного кода влечет за собой внедрение Cobalt Strike Beacon в скомпрометированные системы, давая злоумышленникам возможность управления [12].

Нарушается безопасность сети и создаются устойчивые каналы между атакующими и их целями. Такой функционал реализуется через Beacon – специальный модуль (агент), входящий в состав инструмента Cobalt Strike [12].

Размещенный на скомпрометированной системе, Beacon функционирует как агент для злоумышленников, обеспечивая плацдарм для развертывания последующих этапов атаки. Критически важно для проведения комплексных операций то, что после запуска Beacon обеспечивает незаметный обмен данными и получение инструкций. Cobalt Strike применяет протокол управления, базирующийся на DNS, который значительно усложняет его выявление по сравнению с обычным веб-трафиком. Данный подход позволяет скрывать вредоносные команды в DNS-записях, используя алгоритм запутывания, интегрированный в Beacon.

С использованием Beacon становятся реализуемыми разнообразные вредоносные активности, включая сетевой мониторинг, похищение конфиденциальных данных, распространение вредоносного ПО в пределах сети и проведение атак с использованием программ-шифровальщиков [11,12].

Заключение

В рамках данной работы проведён анализ возможных угроз службы каталогов, систематизирована информация о возможных атаках на Active Directory, выделены три класса инструментов, используемых для получения полезной информации из Active Directory. Рассмотрены возможности Cobalt Strike как инструмента эмуляции угроз и проведения постэксплуатационных задач. Проведен анализ практической реализации кибератак с применением инструмента Cobalt Strike за последние несколько лет. Изучена и пошагово детализирована методика таких кибератак. Сделан вывод, что несмотря на разнообразие операционных систем, использование гетерогенных сред, мультиплатформенного ПО, многие принципы защиты и процессы администрирования схожи. Соответственно, схожи угрозы, риски, методики и инструменты для их реализации. Проведённый анализ демонстрирует возможности применения ПО Cobalt Strike как инструмента для проведения дальнейшего исследования Active Directory.

Литература

1. Усанов И. Г. Трансформационные императивы современного менеджмента // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2022. № 4(60). С. 121-126. DOI: 10.17084/20764359-2022-60-121. EDN FGTPJF.

2. Sharkov G. A System-of-Systems Approach to Cyber Security and Resilience // Information & Security An International Journal. 2017. Vol. 37. pp. 69-94. DOI: 10.11610/isij.3706.

3. Васильев А. Экономика кибербезопасности в мире // Cifra. Информационные технологии и телекоммуникации. 2024. № 1(1). С. 23-34. DOI: 10.18454/itech.2024.1.1. EDN OVMVOZ.

4. Dishan F. Mastering Active Directory: Design, deploy, and protect Active Directory Domain Services for Windows Server 2022, Third Edition // Grosvenor

House, 11 St Paul's Square, Birmingham, B3 1RB, UK. Packt Publishing Ltd. 2021. 780 p. ISBN 978-1-80107-039-3.

5. Трещев, И. А., Монастырная Е. И. Событийная формальная модель поведения злоумышленника // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2024. № 1(73). С. 42-46. EDN IZQRGT.

6. Минзов А. С., Немчанинова С. В., Бирулева М. А. Анализ методов управления рисками информационной безопасности в системах управления // Государственный университет «Дубна». 30 лет в науке. 2024. С. 328-337. DOI: 10.17084/20764359-2022-60-121. EDN BGMDAL.

7. Фролов А. Е., Нагаев Д. М. Исследование элементов безопасности Active Directory: возможные атаки // Проблемы правовой и технической защиты информации. 2024. №12. С. 88-93. EDN LWIUZS.

8. Кацупеев А. А., Щербакова Е. А, Воробьёв С.П. Постановка и формализация задачи формирования информационной защиты распределённых систем // Инженерный вестник Дона. 2015. №1(2). URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2868.

9. Верещагина Е.А., Колесникова Д.С., Рудниченко А.К. Особенности разработки информационной системы для предприятия // Инженерный вестник Дона. 2019. №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5533.

10. Sinclair G. Making Cobalt Strike harder for threat actors to abuse // Security & Identity. 2022. URL: cloud.google.com/blog/products/identity-security/making-cobalt-strike-harder-for-threat-actors-to-abuse.

11. Скулин О. В. Атаки с применением Cobalt Strike снова обрушились на российские компании // BI.ZONE. 2023. URL: bi.zone/news/ataki-s-primeneniem-cobalt-strike-snova-obrushilis-na-rossiyskie-kompanii/.

12. Стародубов М. И., Семенов Д. М., Акуленко В. И. Cobalt Strike Beacon с доставкой через GitHub и соцсети // Securelist by Kaspersky. 2025. URL: securelist.ru/cobalt-strike-attacks-using-quora-github-social-media/113139/.

References

1. Usanov I. G. Ucheny`e zapiski Komsomol`skogo-na-Amure gosudarstvennogo texnicheskogo universiteta. 2022. № 4(60). pp. 121-126. DOI: 10.17084/20764359-2022-60-121. EDN FGTPJF.

2. Sharkov G. A. Information & Security An International Journal. 2017. Vol. 37. pp. 69-94. DOI: 10.11610/isij.3706.

3. Vasil`ev A. Cifra. Informacionny`e texnologii i telekommunikacii. 2024. № 1(1). pp. 23-34. DOI: 10.18454/itech.2024.1.1. EDN OVMVOZ.

4. Dishan F. Mastering Active Directory: Design, deploy, and protect Active Directory Domain Services for Windows Server 2022, Third Edition Grosvenor House, 11 St Pauls Square, Birmingham, B3 1RB, UK. Packt Publishing Ltd. 2021. 780 p.

5. Treshhev, I. A., Monasty`rnaya E. I. Ucheny`e zapiski Komsomol`skogo-na-Amure gosudarstvennogo texnicheskogo universiteta. 2024. № 1(73). pp. 42-46. EDN IZQRGT.

6. Minzov A. S., Nemchaninova S. V., Biruleva M. A. Gosudarstvenny`j universitet «Dubna». 30 let v nauke. 2024. pp. 328-337. DOI: 10.17084/20764359-2022-60-121. EDN BGMDAL.

7. Frolov A. E., Nagaev D. M. Problemy` pravovoj i texnicheskoj zashhity` informacii. 2024. №12. pp. 88-93. EDN LWIUZS.

8. Kaczupeev A. A., Shherbakova E. A, Vorob`yov S.P. Inzhenernyj vestnik Dona. 2015. №1(2). URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2868.

9. Vereshhagina E.A., Kolesnikova D.S., Rudnichenko A.K. Inzhenernyj vestnik Dona. 2019. №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5533.

10. Sinclair G. Security & Identity. 2022. URL: cloud.google.com/blog/products/identity-security/making-cobalt-strike-harder-for-threat-actors-to-abuse.

11. Skulin O. V. Ataki s primeneniem Cobalt Strike snova obrushilis` na rossijskie kompanii [Cobalt Strike attacks have once again targeted russian companies] BI.ZONE. 2023. URL: bi.zone/news/ataki-s-primeneniem-cobalt-strike-snova-obrushilis-na-rossiyskie-kompanii/.

12. Starodubov M. I., Semenov D. M., Akulenko V. I. Cobalt Strike Beacon s dostavkoj cherez GitHub i soczseti [Cobalt Strike Beacon with delivery via GitHub and social media]. Securelist by Kaspersky. 2025. URL: securelist.ru/cobalt-strike-attacks-using-quora-github-social-media/113139/.

Дата поступления: 13.01.2025

Дата публикации: 25.02.2026