УДК 004.056.53

ПОДХОД К ОБНАРУЖЕНИЮ ПОДДЕЛЬНЫХ БИЛЕТОВ ДЛЯ ЗАЩИТЫ ОТ АТАК НА ПРОТОКОЛ АУТЕНТИФИКАЦИИ КЕРБЕРОС

Трушин М.М., Лукьянчиков О.И.

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет»,119454, Российская Федерация, г.Москва, проспект Вернадского, 78, maxmtrushin@gmail.com, lukyanchikov@mirea.ru

Цели. Протокол Керберос является фундаментальным механизмом аутентификации в корпоративных сетях, поэтому он регулярно подвергается атакам со стороны злоумышленников. Одними из самых опасных являются атаки типа «золотой» и «серебряный» билет. При их реализации атакующий использует поддельные билеты, полученные в обход стандартного процесса аутентификации, предусмотренного протоколом. Учитывая, что современные методы противодействия подобным угрозам не обеспечивают должной защиты, поскольку они основаны на анализе уже произошедших событий, необходима возможность своевременно обнаружить их и нейтрализовать. Цель работы – детектирование атак типа «золотой» и «серебряный» билет путем анализа содержимого поддельных билетов, генерируемых злоумышленниками, на этапе их первичного использования. Для выявления аномалий в билетах, позволяющих сделать вывод об их нелегитимности, необходимо построить автоматическую систему. Методы. Для достижения поставленной цели выполнен анализ функционала программных средств, предназначенных для генерации поддельных билетов, таких как, Mimikatz, с целью понимания принципов их работы. Также осуществлен анализ содержимого различных нелегитимных билетов для выявления аномальных закономерностей. На основе выявленных особенностей определены достаточные критерии, по которым выполняется анализ дли обнаружения подозрительных аутентификаций в системе с использованием детерминированного метода. Результаты. Выявлены несколько аномалий, наличие которых в билете однозначно свидетельствует о его нелегитимности, а также одна аномалия, требующая дополнительный анализ для вынесения вердикта. Описана абстрактная система, использующая детерминированный метод для обнаружения поддельных билетов, включая некоторые детали реализации. Выводы. Все выявленные логические несоответствия, характерные для поддельных билетов, возникают вследствие неспособности атакующих точно воспроизвести оригинальную структуру целевого домена. Причиной этому является то, что каждый домен формируется на основе уникальных характеристик, присущих конкретной инфраструктуре, таких как, иерархия пользователей и групп, настройки служб или политики безопасности. Несмотря на очевидность и простоту ошибок в поддельных билетах, они позволят наверняка обнаружить подозрительную аутентификацию и предотвратить негативные последствия, вызванные атакой на протокол.

Ключевые слова: аутентификация, протокол Керберос, обнаружение кибератак, золотой билет, серебряный билет

AN APPROACH TO DETECTING COUNTERFEIT TICKETS TO PROTECT AGAINST ATTACKS ON THE KERBEROS AUTHENTICATION PROTOCOL

Trushin M.M., Lukyanchikov O.I.

Federal State Budgetary Educational Institution of Higher Education «MIREA – Russian Technological University», 119454, Russian Federation, Moscow, Vernadskogo Ave., 78, e-mail: maxmtrushin@gmail.com*, lukyanchikov@mirea.ru*

Objectives. The Kerberos protocol serves as a fundamental authentication mechanism within corporate networks, making it a frequent target of attacks by malicious actors. Among the most dangerous are the so-called Golden Ticket and Silver Tickee attacks. In these scenarios, the attacker utilizes forged tickets that bypass the standard authentication process defined by the protocol. Given that current mitigation techniques fail to provide adequate protection – largely because they rely on post-event analysis – there is a critical need for the capability to detect and neutralize such threats at an early stage. The objective of this study is to detect Golden Ticket and Silver Ticket attacks by analyzing the contents of forged tickets generated by attackers during their initial use. To identify anomalies within these tickets that indicate illegitimacy, an automated detection system must be developed. Methods. To achieve the stated objective, the functionality of software tools designed to generate forged tickets, such as Mimikatz, was analyzed to gain an understanding of their operating principles. An analysis of the contents of various illegitimate tickets was also carried out to identify anomalous patterns. Based on the revealed characteristics, sufficient criteria were defined to perform the analysis for detecting suspicious authentications in the system using a deterministic method. Results. Several anomalies have been identified, the presence of which in a ticket clearly indicates its illegitimacy, as well as one anomaly that requires additional analysis to reach a verdict. An abstract system is described that uses a deterministic method to detect forged tickets, including certain implementation details. Coclusions. All identified logical inconsistencies typical of forged tickets stem from the attacker's inability to accurately replicate the original structure of the target domain. This occurs because each domain is formed

based on unique characteristics inherent to a specific infrastructure, such as user and group hierarchy, service configurations, or security policies. Despite the obvious and simple nature of the errors in forged tickets, they will reliably detect suspicious authentication and prevent the negative consequences of an attack on the protocol.

Key words: authentication, Kerberos protocol, cyberattacks detection, Golden Ticket, Silver Ticket

Введение

Существование современных информационных систем – от облачных сервисов до корпоративных сетей – немыслимо без надежных методов аутентификации, способных обеспечить защиту внутренних ресурсов. Ежедневно в мире совершаются миллионы запросов на подтверждение личности пользователей и устройств – будь то вход в электронную почту, доступ к базе данных или подключение к облачным сервисам. Безопасность подобных операций является критическим фундаментом цифровой инфраструктуры, а их компрометация способна привести к катастрофическим последствиям, включая утечки конфиденциальных данных или остановку бизнес-процессов. По этой причине организации вынуждены внедрять и поддерживать надежные методы проверки подлинности пользователей.

Одним из наиболее распространенных и востребованных механизмов аутентификации, используемых в современных информационных системах, является протокол Керберос [1]. Несмотря на более чем 30-летнюю историю, данный протокол остается ключевым элементом в обеспечении контроля доступа как в коммерческих, так и в государственных организациях. По данным исследований, порядка 90-95 процентов компаний из списка Fortune 1000 так или иначе используют его в своей инфраструктуре. Одной из главных причин столь широкого распространения протокола является его интеграция со службой каталогов Active Directory [2], являющейся стандартом для организаций, использующих экосистему Windows.

В то же время высокая популярность делает Керберос одной из приоритетных целей для злоумышленников. Его глубокая интеграция в корпоративной среде создает условия, при которых успешно совершенная атака может привести к серьезным последствиям. Несмотря на надежность криптографической составляющей и многоуровневую систему защиты, протокол имеет слабые места, а их эксплуатация имеет весьма высокую результативность [3] (рис. 1).

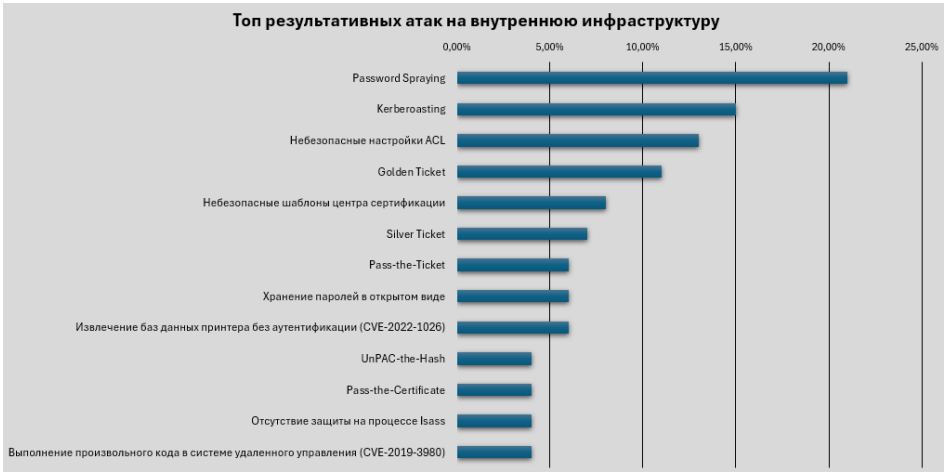

Рисунок 1 – Результативность атак на внутреннюю инфраструктуру

Атаки «золотой» и «серебряный» билет впервые были обнаружены и представлены Бенджамином Дельпи, разработчиком инструмента Mimikatz [4], в 2014 году. Учитывая высокую степень угроз, связанных с подобными атаками, исследования, направленные на их обнаружение и смягчение, по-прежнему остаются актуальными и востребованными [5-7]. Основная проблема атак заключается в том, что их очень трудно обнаружить и вовремя предотвратить [8], поскольку в их основе лежат не ошибки реализации, а функционал самого протокола [9]. Именно поэтому для своевременного реагирования на угрозу необходимо иметь возможность определить ее на ранних этапах.

Протокол Керберос

Керберос [1] – сетевой протокол аутентификации, разработанный для безопасного подтверждения личности пользователей и сервисов в распределенных вычислительных системах. Основной задачей протокола является предотвращение несанкционированного доступа за счет применения криптографических методов защиты, исключающих возможность перехвата или подделки учетных данных в процессе аутентификации. Протокол поддерживает механизм взаимной аутентификации, при котором не только клиент, но и сервер подтверждает подлинность, а также обеспечивает механизм единого входа [10] (SSO – Single Sign On), позволяя пользователям получать доступ к различным ресурсам в рамках домена после однократного подтверждения личности, что значительно упрощает процесс аутентификации.

Основу работы протокола формируют три ключевые сущности:

1. Клиент – участник системы, который инициирует запросы на получение доступа к ресурсам. В роли клиента может выступать пользователь или некоторое приложение.
2. Сервис – приложение или устройство, к ресурсам которого клиент хочет получить доступ. В роли сервиса может выступать файловый сервер, база данных или другое приложение.
3. Контроллер домена – центральный элемент, который отвечает за проверку подлинности и предоставление доступов. В его роли выступает центр распределения ключей (KDC – Key Distribution Center), который состоит из двух частей: сервиса аутентификации (AS - Authentication Service) и сервиса выдачи билетов (TGS – Ticket Granting Service). Сервис аутентификации обеспечивает проверку подлинности клиентов и сервисов, в то время как сервис выдачи билетов выдает специальные пропуски, именуемые билетами, для доступа к конкретным сервисам. Иными словами, контроллер домена – доверенная третья сторона, которая обеспечивает безопасное взаимодействие между клиентом и сервисом.

Процесс аутентификации

Рассмотрим подробно, каким образом выполняется процесс аутентификации в Керберос [11] (рис. 2). Он включает в себя несколько последовательных этапов, каждый из которых выполняет важную функцию в обеспечении безопасности обмена данными между сторонами. Понимание всех аспектов работы механизма аутентификации необходимо для выявления потенциально уязвимых мест в системе, которые могут являться целью злоумышленников.

На первом этапе клиенту, желающему получить доступ к ресурсам определенного сервиса, необходимо выполнить аутентификацию на контроллере домена и получить TGT билет (Ticket Granting Ticket). Для этого клиент выполняет запрос к сервису аутентификации (AS REQ), передавая в нем имя пользователя и временную метку, зашифрованную его ключом, который также известен контроллеру домена. Таким способом личность клиента может быть проверена без использования пароля. Сервис аутентификации, в свою очередь, проверяет имя пользователя, а также расшифровывает временную метку, чтобы удостовериться, что полученный запрос в действительности исходит от нужного пользователя. В случае успеха сервис аутентификации передает в ответе (AS REP) TGT билет, зашифрованный ключом контроллера домена, который в дальнейшем позволяет клиенту в рамках той же сессии взаимодействовать с контроллером домена без повторного прохождения аутентификации.

Данный билет содержит временные метки, указывающие на его срок действия, а также различные привилегии, группы, в которых состоит клиент, и пр. Клиент также получает сессионный ключ, который дублируется в билете для подтверждения личности во время выполнения дальнейших запросов. Он формируется с использованием ключа клиента.

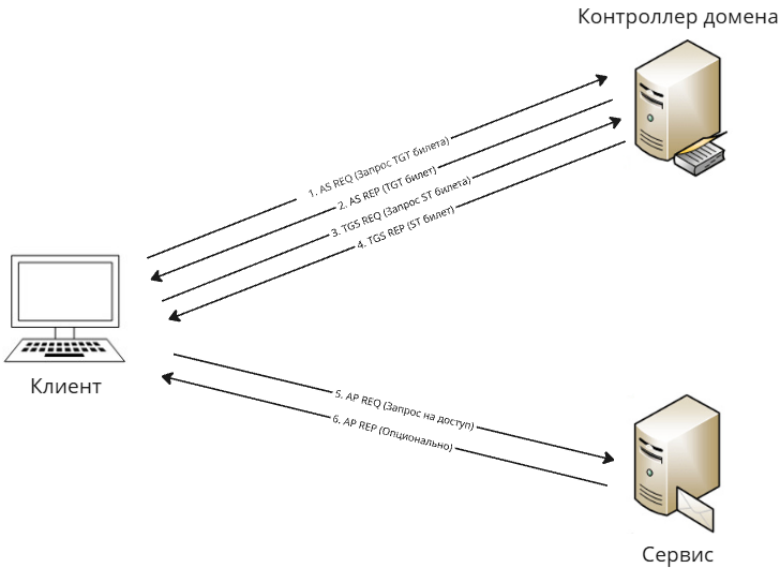

Рисунок 2 – Процесс аутентификации

Следующий этап включает в себя получение клиентом сервисного билета (ST - Service Ticket). Клиент инициирует запрос (TGS REQ) к сервису выдачи билетов, передавая в нем TGT, полученный ранее, идентификатор сервиса, а также зашифрованный при помощи сессионного ключа аутентификатор. В нем содержится идентификатор клиента и временная метка. Сервис выдачи билетов расшифровывает предназначенный для него TGT, извлекая оттуда сессионный ключ, после чего с его помощью расшифровывает аутентификатор, чтобы проверить личность клиента и актуальность билета при помощи временных меток. Если проверка была успешно выполнена, сервис выдачи билетов ответным сообщением (TGS REP) передает ST, предназначенный для целевого сервиса и зашифрованный его ключом. В сервисном билете аналогично содержатся временные метки, привилегии, группы, а также другой сессионный ключ, который в дальнейшем будет использован клиентом для подтверждения личности сервису. Иными словами, ST – тот же самый TGT, только зашифрованный ключом сервиса и содержащий другой сессионный ключ. Важно обратить внимание, что при выдаче ST сервис выдачи билетов не проверяет наличие прав у клиента для доступа к сервису, которому предназначен билет, поскольку Керберос является исключительно протоколом аутентификации. Ответственность за авторизацию клиента возложена на сами сервисы.

На финальном этапе клиент подтверждает свою личность сервису, получая доступ к необходимым ресурсам, а также проверяет личность сервиса при необходимости. Для этого посылается запрос (AP REQ), в котором клиент отправляет сервисный билет и аутентификатор. Сервис же, в свою очередь, их расшифровывает и проверяет подлинность. После успешной аутентификации налаженный канал связи используется для взаимодействия сторон. Клиент также может дополнительно попросить сервис подтвердить свою личность. В этом случае сервис направит ответ (AP REP), в котором будет содержаться его аутентификатор, зашифрованный сессионным ключом клиента, а также при необходимости еще один сессионный ключ, при помощи которого будет обеспечиваться шифрование в рамках общения.

Векторы атак на протокол

Предложенная в рамках данной статьи система предполагает защиту от двух типов атак: «золотой» билет [12] (Golden Ticket) и «серебряный» билет [13] (Silver Ticket), поэтому в данном разделе будут рассмотрены именно они. Golden Ticket – тип атаки на протокол Керберос, при котором злоумышленник создает поддельный TGT билет, содержащий всевозможные привилегии. С его помощью может быть получен доступ к любому сервису в рамках домена. Атака возможна в случае компрометации пароля учетной записи «krbtgt» контроллера домена, на основе которого рассчитываются ключи для шифрования TGT билетов. Наиболее распространенный способ получения данного пароля – DCSync атака [14], которая эксплуатирует механизм репликации данных. Злоумышленник, притворяясь контроллером домена, отправляет запрос на синхронизацию данных другому контроллеру домена, который в ответ присылает актуальные ключи. Рассмотрим типичный сценарий атаки с использованием «золотого» билета:

1. В первую очередь, завладев ключом, злоумышленник формирует собственный TGT билет, содержащий любого привилегированного пользователя с широким набором прав в системе. В результате атакующий

полностью пропускает первый шаг, который предполагает запрос TGT у сервиса аутентификации, избегая обнаружения (рис. 3).

2. Далее сгенерированный TGT используется в запросе на получение сервисного билета. Поскольку TGT зашифрован с использованием действительного ключа, сервис выдачи билетов считает его полностью легитимным и выдает необходимый ST.

3. Наконец, полученный ST билет используется для установления сессии с целевым сервисом. Отправленный билет с точки зрения сервиса является корректным, поскольку он был, как и положено, получен через сервис выдачи билетов, поэтому аутентификация выполняется успешно, и злоумышленник получает привилегированный доступ, после чего может отдавать любые команды сервису, полностью компрометируя его.

Данная атака ставит под угрозу всю инфраструктуру домена, предоставляя атакующему неограниченный доступ к любым ресурсам. Поскольку подобная атака практически не оставляет за собой следов, не считая событий в журналах, она может оставаться незамеченной в течение очень длительного времени. Существовать угроза будет до тех пор, пока не будет изменен пароль учетной записи «krbtgt».

4. Silver Ticket – атака, в ходе которой злоумышленник создает поддельный ST с повышенными привилегиями, чтобы получить неограниченный доступ к конкретному сервису. Поскольку ключи, при помощи которых шифруются сервисные билеты, формируются на основе хэша пароля целевой машины, для совершения атаки должен быть известен данный секрет.

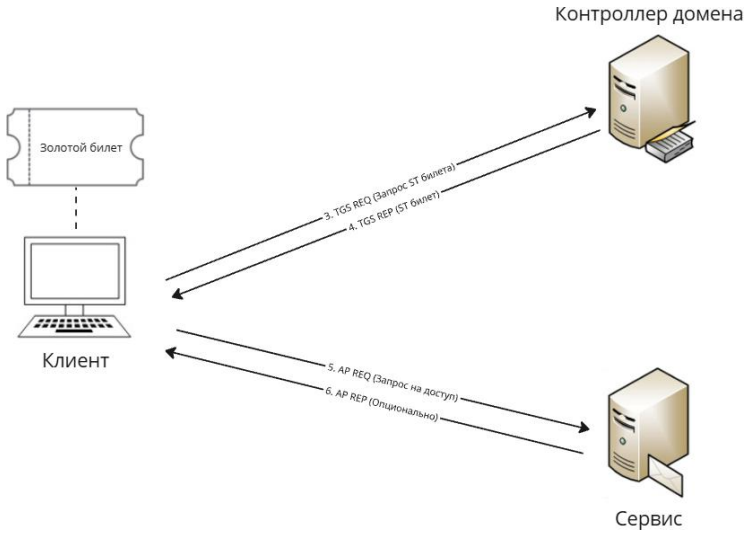

Рисунок 3 – Использование «золотого» билета

Процесс атаки с использованием «серебряного» билета выглядит следующим образом:

1. Сперва атакующий формирует поддельный сервисный билет, содержащий учетную запись пользователя с повышенными привилегиями. В отличие от «золотого» билета, в данной атаке пропускаются сразу два этапа, поэтому взаимодействие с контроллером домена не осуществляется вовсе (рис. 4).

2. Сформированный билет помещается в кэш сервисных билетов на локальной машине, после чего с использованием него инициируется запрос к сервису для выполнения аутентификации.

3. Сервис успешно расшифровывает билет, подтверждая личность и предоставляя злоумышленнику перечисленные в билете привилегии. В результате атакующий может выполнять любые действия на данном сервисе.

Несмотря на то что данная атака приводит к компрометации только одного сервиса, она может иметь серьезные последствия, особенно если сервис играет важную роль в инфраструктуре организации. Как и в случае с «золотым» билетом, данная атака практически не оставляет после себя следов, из-за чего ее весьма трудно обнаружить. Действовать «серебряный» билет будет до тех пор, пока не будет изменен пароль атакуемой машины.

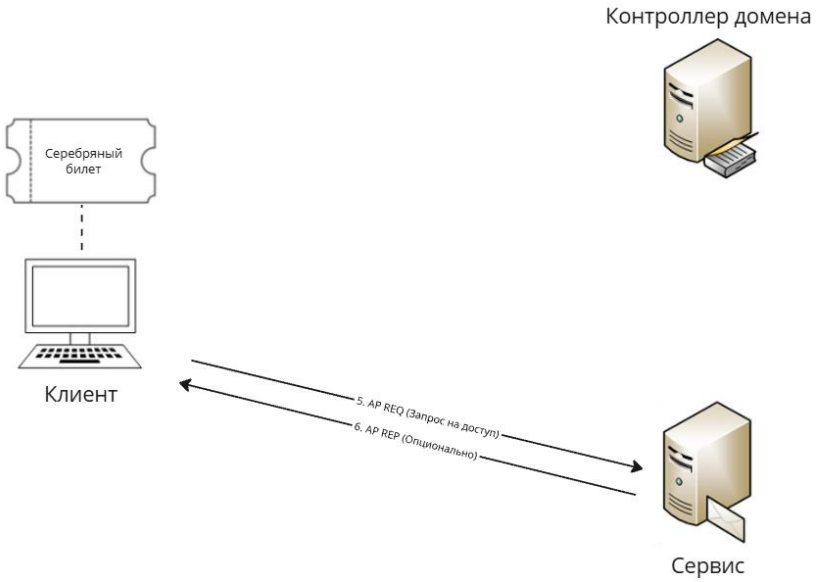

Рисунок 4 – Использование «серебряного» билета

Признаки поддельных билетов

Существующие методы противодействия подобным атакам в большинстве своем сводятся к различным рекомендациям для минимизации рисков, а также анализу журналов событий на предмет наличия подозрительной активности. Хотя данные способы и помогают снизить вероятность успешного выполнения атаки, они не устраняют полностью возможность ее возникновения. Более того, данные методы не обеспечивают оперативного выявления компрометации системы, поскольку основаны на анализе уже случившихся событий. Таким образом, необходимо научиться обнаруживать атаку в момент попытки использования поддельного билета, чтобы полностью исключить негативные последствия.

Обнаружение поддельных билетов основано на эвристическом анализе. Иными словами, существуют различные логические ошибки и особенности, содержащиеся в сгенерированных билетах, благодаря которым можно сделать вывод о том, что билет не является легитимным.

Поскольку злоумышленнику необходимо получить максимально возможные права доступа к системе, при генерации билета используются известные идентификаторы привилегированных групп (рис. 5), к примеру, администратор домена. Однако в реальных рабочих окружениях, где необходимо множественное разграничение доступа, полное совпадение групп, указанных в билете, с реальными практически невозможно. Таким образом, мы можем сопоставить членство в группах пользователя, указанного в нем, и записанного в системе, после чего сделать вывод о легитимности данного билета.

gam\Domain Admins	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-512	ActiveDirectory	Group
gam\Domain Users	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-513	ActiveDirectory	Group
gam\Schema Admins	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-518	ActiveDirectory	Group
gam\Enterprise Admins	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-519	ActiveDirectory	Group
gam\Group Policy Creator Owners	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-520	ActiveDirectory	Group

Рисунок 5 – Пример известных привилегированных групп, используемых в поддельных билетах

Другой признак поддельного билета – несоответствие пары имя пользователя и идентификатор. Легитимный процесс аутентификации гарантирует, что два данных значения будут взаимосвязаны между собой. Однако злоумышленники, не имея представления о реальном соответствии, часто допускают эту логическую ошибку. Такой билет будет исправно работать, поскольку система опирается лишь на идентификатор, игнорируя имя пользователя. В нашем случае подобное несоответствие может быть использовано при обнаружении поддельных билетов.

Еще одним фактором нелегитимного билета могут выступать активные сессии для несуществующих пользователей. Такая ситуация возникает в том случае, если атакующий использует имя или идентификатор пользователя, которые отсутствуют в домене. В случае честной аутентификации активная сессия может быть связана только с действительной учетной записью, поэтому такое несоответствие является серьезной аномалией.

Также нелегитимный билет может быть вычислен по наличию идентификаторов пользователей в списке идентификаторов групп. Подобное поведение может встречаться и в обычных случаях, к примеру, такое

происходит при миграции домена. Однако данная ситуация является не столь частой, поэтому подобное событие необходимо считать аномалией, требующей более детального анализа.

Как правило, в крупных организациях используется множество доменов, и пользователь может относится сразу к нескольким из них. Однако сгенерировать такой билет, где будут учтены группы сразу нескольких доменов, практически невозможно, благодаря чему он может быть элементарно обнаружен в подобной среде.

Система обнаружения поддельных билетов

Чтобы своевременно обнаруживать поддельные билеты, необходима автоматическая система, которая обеспечивала бы проверку перечисленных ранее признаков на этапе первичного использования билета злоумышленником (рис. 6).

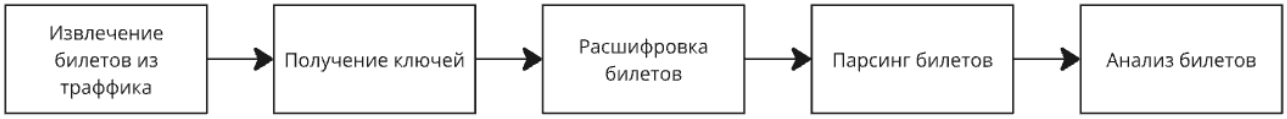

Рисунок 6 – Система обнаружения поддельных билетов

В первую очередь требуется заполучить билет, чтобы была возможность его проверить. Для этого может быть организован анализ сетевого траффика на соответствующих портах транспортного уровня. В случае «золотого» билета оптимальной точкой для анализа является контроллер домена, поскольку поддельные билеты могут приходить только в TGS REQ запросе к сервису выдачи билетов (рис. 7). Подобные запросы выполняются непосредственно с использованием протокола Керберос.

Для «серебряного» билета ситуация несколько отличается. В первую очередь, подобные билеты используются в AP REQ запросах, поэтому обнаруживаться и анализироваться они должны на целевых сервисах, к которым выполняется доступ (рис. 7).

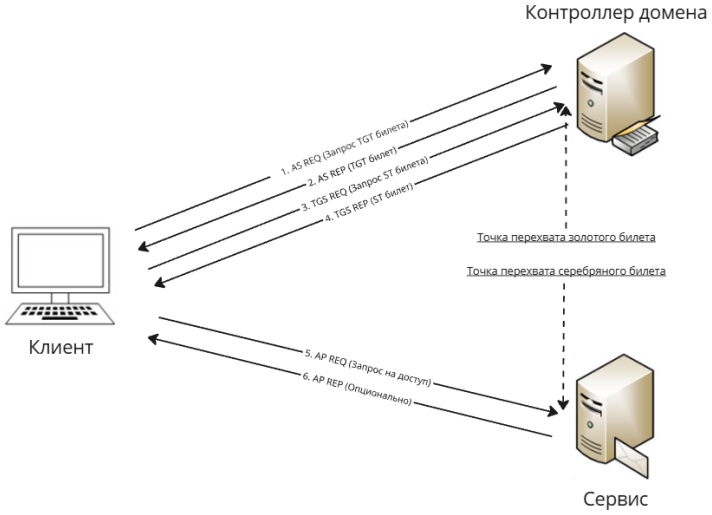

Рисунок 7 – Точки перехвата билетов

Кроме того, существует множество различных протоколов, поддерживающих внешние механизмы аутентификации, такие как GSS-API (Generic Security Services Application Program Interface). Внешний механизм аутентификации позволяет сторонам при использовании какого-либо протокола подтвердить личности друг друга и наладить защищенный канал связи. Керберос в том числе может служить для достижения данной цели, поэтому AP REQ запросы, потенциально содержащие «серебряные» билеты, могут встречаться в таких протоколах как RPC, LDAP и других. Таким образом, необходимо уметь извлекать сервисные билеты из максимально большого количества протоколов, поддерживающих Керберос в качестве механизма аутентификации. В противном случае поддельный билет может быть пропущен.

Наиболее значимая информация для анализа находится в засекреченной части запроса, поэтому ее извлечение требует предварительной расшифровки билета. Для этого необходимо обладать соответствующими секретными ключами. Пароль, используемый для формирования ключей, при помощи которых шифруются сервисные билеты (Machine Account Password), хранится в защищенной части реестра каждого участника домена. При наличии прав системного пользователя он может быть прочитан, после чего преобразован в необходимый ключ.

Пароль от учетной записи «krbtgt», на основе которого формируются ключи для шифрования TGT билетов, расположен на контроллере домена в локальной базе данных Active Directory. Поскольку данный файл постоянно используется и защищается системой, извлечь из него необходимую информацию весьма проблематично. Вместо этого может быть использован в легитимных целях механизм синхронизации данных между контроллерами домена, описанный ранее.

При наличии билета и подходящих секретных ключей необходимые данные могут быть извлечены для последующего анализа. Подробные алгоритмы расчета ключей [15], а также расшифровки и парсинга билетов рассматриваться в рамках данной статьи не будут.

Финальный этап включает в себя детальный анализ полученных из билета данных на предмет наличия несоответствий и логических ошибок, описанных ранее. В случае обнаружения каких-либо признаков поддельного билета могут быть использованы различные стратегии для противодействия атаке в зависимости от требований. К примеру, блокировка данного соединения или информирование специалистов по информационной безопасности.

Заключение

Рассмотренный метод обнаружения поддельных билетов основан на анализе их содержимого на предмет наличия логических ошибок. Несмотря на то что многие логические ошибки являются довольно очевидными и примитивными, они практически гарантированно будут встречаться, поскольку отследить многочисленные особенности, политики и настройки реальной среды для злоумышленников в настоящий момент очень проблематично.

Подобная система может показаться избыточной для большинства организаций, где уровень рисков не так высок и достаточно базовых методов защиты. Однако в инфраструктурах с повышенными требованиями к безопасности – к примеру, в государственных, финансовых или промышленных системах – использование системы становится весьма актуальным. В таких организациях описанные векторы атак представляют более серьезную угрозу, поэтому предложенная система защиты должна рассматриваться как обязательный элемент архитектуры безопасности.

Список литературы

1. Neuman B. C., Ts'o T. Kerberos: An authentication service for computer networks //IEEE Communications magazine. – 1994. – Т. 32. – №. 9. – С. 33-38.
2. Desmond B. et al. Active Directory: Designing, Deploying, and Running Active Directory. – " O'Reilly Media, Inc.", 2008.
3. 13 уязвимостей на компанию: свежая ИБ-статистика от пентестеров [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/bastion/articles/876946/, свободный
4. Revazova A., Korkin I. RASP for LSASS: Preventing Mimikatz-Related Attacks //arXiv preprint arXiv:2401.00316. – 2023.
5. Matsuda W. et al. Detection of the Silver Ticket for Seamless Single Sign-On Focusing on a Ticket Lifetime //Journal of Information Processing. – 2025. – Т. 33. – С. 156-167.
6. Liu Q. et al. HADES: Detecting Active Directory Attacks via Whole Network Provenance Analytics //arXiv preprint arXiv:2407.18858. – 2024.
7. Senturk Z., Irmak E. Persistence Techniques in Microsoft Active Directory: Detection and Mitigation Strategies //2024 12th International Symposium on Digital Forensics and Security (ISDFS). – IEEE, 2024. – С. 01-06.
8. Crandall C., Cole T. How to stop attackers from owning your Active Directory //Cyber Security: A Peer-Reviewed Journal. – 2022. – Т. 5. – №. 4. – С. 294-302.
9. Qatinah S. H., Al-Baltah I. A. Kerberos Protocol: Security Attacks and Solution //2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI). – IEEE, 2024. – С. 1-7.
10. De Clercq J. Single sign-on architectures //International Conference on Infrastructure Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2002. – С. 40-58.
11. Motero C. D. et al. On attacking Kerberos authentication protocol in windows active directory services: A practical survey //IEEE Access. – 2021. – Т. 9. – С. 109289-109319.
12. Pocarovsky S. et al. Kerberos Golden Ticket Attack //Proceedings of the Computational Methods in Systems and Software. – Cham : Springer International Publishing, 2022. – С. 677-688.
13. Grippo T., Kholidy H. A. Detecting Forged Kerberos Tickets in an Active Directory Environment //arXiv preprint arXiv:2301.00044. – 2022.

14. Badhwar R. Advanced active directory attacks and prevention //The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. – Cham : Springer International Publishing, 2021. – С. 131-144.
15. Garman J. Kerberos: The Definitive Guide: The Definitive Guide. – " O'Reilly Media, Inc.", 2003.

References

1. Neuman B. C., Ts'o T. Kerberos: An authentication service for computer networks //IEEE Communications magazine. – 1994. – Т. 32. – №. 9. – С. 33-38.
2. Desmond B. et al. Active Directory: Designing, Deploying, and Running Active Directory. – " O'Reilly Media, Inc.", 2008.
3. 13 vulnerabilities per company: fresh pentesting security stats [Electronic resource]. – Access mode: https://habr.com/ru/companies/bastion/articles/876946/, open
4. Revazova A., Korkin I. RASP for LSASS: Preventing Mimikatz-Related Attacks //arXiv preprint arXiv:2401.00316. – 2023.
5. Matsuda W. et al. Detection of the Silver Ticket for Seamless Single Sign-On Focusing on a Ticket Lifetime //Journal of Information Processing. – 2025. – Т. 33. – С. 156-167.
6. Liu Q. et al. HADES: Detecting Active Directory Attacks via Whole Network Provenance Analytics //arXiv preprint arXiv:2407.18858. – 2024.
7. Senturk Z., Irmak E. Persistence Techniques in Microsoft Active Directory: Detection and Mitigation Strategies //2024 12th International Symposium on Digital Forensics and Security (ISDFS). – IEEE, 2024. – С. 01-06.
8. Crandall C., Cole T. How to stop attackers from owning your Active Directory //Cyber Security: A Peer-Reviewed Journal. – 2022. – Т. 5. – №. 4. – С. 294-302.
9. Qatinah S. H., Al-Baltah I. A. Kerberos Protocol: Security Attacks and Solution //2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI). – IEEE, 2024. – С. 1-7.
10. De Clercq J. Single sign-on architectures //International Conference on Infrastructure Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2002. – С. 40-58.
11. Motero C. D. et al. On attacking Kerberos authentication protocol in windows active directory services: A practical survey //IEEE Access. – 2021. – Т. 9. – С. 109289-109319.
12. Pocarovsky S. et al. Kerberos Golden Ticket Attack //Proceedings of the Computational Methods in Systems and Software. – Cham : Springer International Publishing, 2022. – С. 677-688.
13. Grippo T., Kholidy H. A. Detecting Forged Kerberos Tickets in an Active Directory Environment //arXiv preprint arXiv:2301.00044. – 2022.
14. Badhwar R. Advanced active directory attacks and prevention //The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. – Cham : Springer International Publishing, 2021. – С. 131-144.
15. Garman J. Kerberos: The Definitive Guide: The Definitive Guide. – " O'Reilly Media, Inc.", 2003.