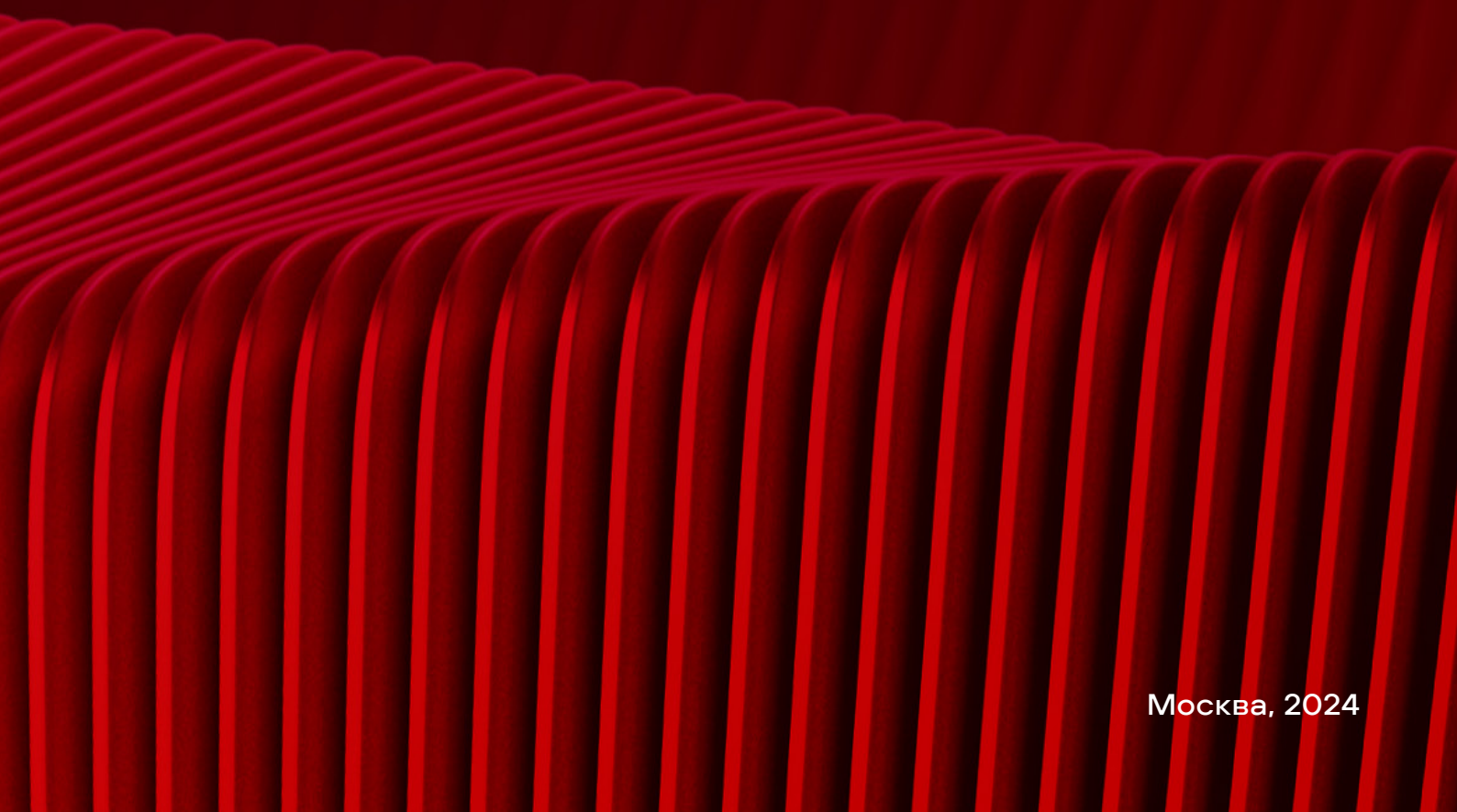
positive technologies

РУКОВОДСТВО ПО ЗАЩИТЕ
Veeam Backup & Replication 12



Москва, 2024

Содержание

1. Введение

Современные компании сталкиваются с беспрецедентным ростом киберугроз, включая атаки на критически важные ИТ-системы. Согласно исследованию Positive Technologies, в третьем квартале 2024 года доля успешных атак на компании через эксплуатацию уязвимостей составила 33%.

Основными проблемами информационной безопасности остаются низкий уровень защищенности программного обеспечения, некорректные конфигурации, а также недостаток практической информации по рекомендациям для защиты ИТ-систем.

Мы создали серию документов с практическими рекомендациями по защите ИТ-инфраструктуры, чтобы помочь организациям минимизировать уязвимости и повысить киберустойчивость.

Наши рекомендации основаны на методологии ХардкорИТ — структурированного подхода к анализу и укреплению защиты информационных систем. Одной из ключевых частей подхода является процесс харденинга.

Харденинг — методика повышения уровня безопасности представляет собой комплекс мероприятий, направленных на выявление и устранение уязвимостей в системах и приложениях. В рамках харденинга выполняются следующие шаги:

- Отключение неиспользуемых функций для снижения поверхности атаки.
- Изменение настроек по умолчанию с учетом принципов безопасности.
- Устранение известных уязвимостей через обновления и конфигурацию.

Данный документ разработан для решения практических задач по защите системы резервного копирования на базе продукта Veeam Backup & Replication 12 и включает:

1. Примеры недопустимых событий для системы резервного копирования;
2. Пример типовой архитектуры Veeam Backup & Replication 12 для малых и средних компаний;
3. Описание методов повышения защищенности ПО без использования наложенных средств защиты.
4. Расчет метрики Time to Attack для стандартных настроек и рекомендованного профиля защиты.
5. Анализ влияния параметров защиты на функциональность и производительность систем.

Этот документ ориентирован на широкий круг специалистов, включая руководителей, архитекторов и инженеров. Основной акцент в документе сделан на использовании встроенных защитных механизмов программного продукта.

2. Проблематика защиты Veeam Backup & Replication

2.1. Покрытие рынка

Системы резервного копирования играют важную роль в поддержании целостности данных и непрерывности функционирования ИТ-систем. Резервирование данных позволяет снизить риски потери информации.

Регулярное создание резервных копий становится особенно важным из-за роста объемов информации и увеличения рисков кибербезопасности. Правильно настроенная система резервного копирования защищает компанию от различных опасностей, включая технические неполадки, вредоносные действия и природные катастрофы.

По версии аналитического агентства Gartner, компания Veeam является лидером в отчете Magic Quadrant for Enterprise Backup and Recovery Software market

По данным самого производителя, более 550 000 компаний более чем в 150 странах используют продукты Veeam для обеспечения сохранности данных, в том числе 74% 2000 крупнейших публичных компаний мира по версии журнала Forbes (Forbes Global 2000).

Согласно мнению аналитиков, продукты Veeam в своей нише еще недавно занимали 50–65% российского рынка. Несмотря на то что компания Veeam прекратила свою деятельность в России, ограничив доступ российским клиентам к своим сервисам, коммерческие организации не спешат переходить на альтернативные решения для резервного копирования.

Этот документ описывает типичные проблемы безопасности системы резервного копирования на базе Veeam Backup & Replication (далее — VBR) и дает рекомендации по повышению защищенности.

2.2. Статистика по уязвимостям

Компания Veeam публикует информационные статьи по безопасности в своей базе знаний. Там же можно найти список уязвимостей, включенных в американскую национальную базу данных уязвимостей NVD. На момент написания документа эта база данных включала 15 записей, касающихся уязвимостей продукта Veeam Backup & Replication. Из них 11 имели оценку по шкале CVSS v3.1 более 7 баллов.

Архитектурные особенности

Система резервного копирования на базе Veeam Backup & Replication имеет следующие архитектурные особенности с точки зрения защищенности инфраструктуры:

1. Централизованная консоль управления. Может быть целью атак на систему резервного

копирования. Если злоумышленник получит доступ к консоли управления, он может изменить параметры и получить доступ к данным резервного копирования.

2. Использование сетевых хранилищ для резервных копий. Если резервное копирование выполняется в сетевое хранилище, расположенное в общедоступном сегменте, и резервные копии хранятся в незашифрованном виде, злоумышленник, получив доступ к сетевому хранилищу, может таким образом получить доступ к копии данных всей организации.

3. Злоумышленник может получить доступ через сервер резервного копирования к серверам, которые являются клиентами системы резервного копирования.

4. Интеграция с виртуализацией: если злоумышленник получит доступ к Veeam, он может получить доступ к виртуальным машинам.

5. Использование сетевых протоколов при выполнении задач резервного копирования может быть использовано для перехвата данных, если сетевая инфраструктура не защищена должным образом.

6. Зависимость от Active Directory. Аутентификация через Active Directory может позволить злоумышленнику повысить права и получить доступ к другим ресурсам.

Таким образом, Veeam Backup & Replication может являться как ключевой (промежуточной) системой в цепочке атаки злоумышленника, так и целевой системой, выступающей в качестве главной цели для злоумышленника.

Понимание этих особенностей поможет в создании более безопасной архитектуры.

3. Недопустимые события Veeam Backup & Replication

Взламывая системы резервного копирования, злоумышленники могут преследовать ряд целей:

1. Шантаж и вымогательство. Злоумышленники могут зашифровать данные и требовать выкуп за доступ к ним.

2. Кража данных. Чувствительная информация может быть украдена и использована для мошенничества или продажи.

3. Уничтожение данных. Злоумышленники могут уничтожить резервные копии (зачастую вместе с данными в работающей информационной системе) и таким образом нанести критический ущерб бизнесу.

4. Доступ к системам. Получив доступ к резервным копиям или к агентам резервного копирования, злоумышленники могут проникнуть в основную инфраструктуру.

Рассмотрим в качестве недопустимых событий наиболее часто встречающиеся атаки на системы резервного копирования:

- кража данных из резервных копий;
- уничтожение резервных копий.

Сценарии реализации недопустимых событий тогда могут быть следующими:

- доступ к дисковому или ленточному хранилищу резервных копий;
- получение административного доступа к серверу управления Veeam Backup & Replication;
- получение полномочий администратора или оператора резервного копирования;
- получение полномочий оператора по восстановлению данных или оператора ленточных накопителей.

4. Пример типовой инсталляции Veeam Backup & Replication 12

В этом разделе приведен пример типовой инсталляции системы резервного копирования на базе Veeam Backup & Replication в компании, где все компоненты системы резервного копирования Veeam Backup & Replication развернуты на одном виртуальном сервере.

4.1. Архитектурная схема типовой инсталляции

Архитектурная схема типовой инсталляции системы резервного Veeam Backup & Replication приведена на рисунке 1.

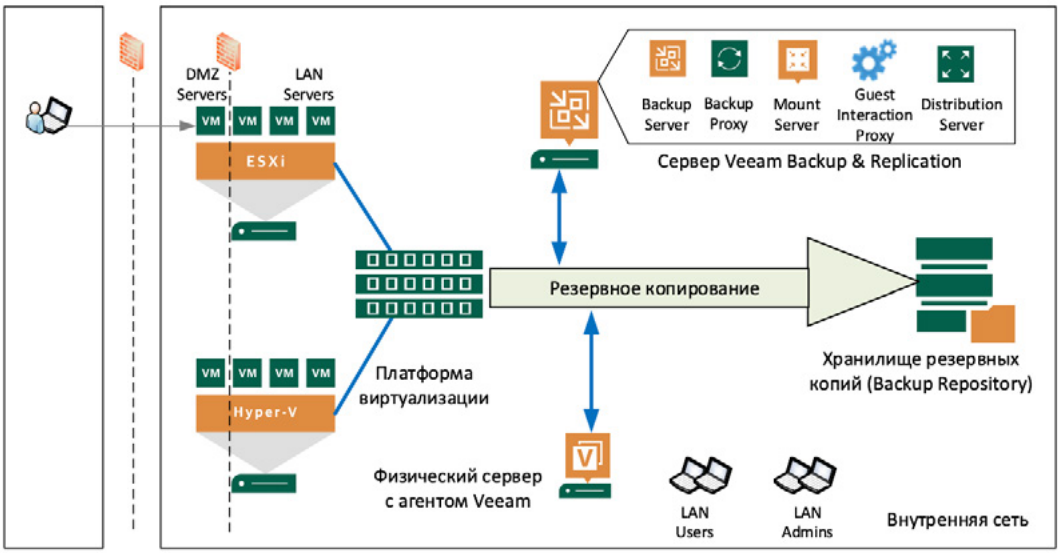


Рисунок 1. Архитектурная схема с примером типовой инсталляции Veeam Backup & Replication

4.2. Описание типовой инсталляции

В типовой инсталляции сервер резервного копирования и все его компоненты разворачиваются на одной виртуальной машине на продуктивной платформе виртуализации. В качестве операционной системы для сервера резервного копирования используется Microsoft Windows Server версии 2012 и выше.

В качестве хранилища резервных копий используется локально подключенное или подключенное по сети хранилище данных.

Для крупных организаций и организаций с большим количеством одновременных задач копирования компоненты системы резервного копирования могут быть вынесены на отдельные виртуальные или физические серверы.

Система резервного копирования на базе Veeam Backup & Replication состоит из следующих компонентов:

1. Сервер резервного копирования (Backup Server) — центр настройки и управления системой резервного копирования.

2. Прокси-серверы резервного копирования (Backup Proxy) — компонент, ответственный за перемещение данных. Используется для извлечения данных виртуальной машины из исходного хранилища данных, их обработки и доставки в целевое хранилище.

3. Выделенные серверы монтирования (Mount Server) — компонент, необходимый для восстановления файлов гостевой ОС виртуальной машины и элементов приложений в исходном местоположении.

4. Репозиторий резервных копий (Backup Repository) — место, используемое для хранения резервных файлов, копий виртуальных машин и вспомогательных файлов-реплик.

5. Guest Interaction Proxy — компонент, необходимый для организации взаимодействия сервера резервного копирования с гостевыми ОС на базе Microsoft.

6. Сервер распространения (Distribution Server) — компонент инфраструктуры управления агентом Veeam, используемый для автоматического развертывания установочных файлов агента Veeam на защищаемых компьютерах.

Если в организации имеются физические серверы, то резервное копирование с них осуществляется с помощью установленных на этих серверах агентов Veeam.

В организациях с географически распределенной инфраструктурой может быть развернуто несколько серверов резервного копирования на разных площадках. Для единого управления распределенной системой резервного копирования может быть установлен компонент Veeam Backup Enterprise Manager.

В зависимости от задач резервного копирования и сложности инфраструктуры компании могут быть также установлены дополнительные компоненты системы резервного копирования.

Для управления системой резервного копирования используется консоль администрирования Veeam Backup & Replication console. По умолчанию консоль администрирования устанавливается на сервер резервного копирования при его установке. Для удаленного управления консоль администрирования может быть установлена на отдельный сервер или рабочую станцию администратора.

Конфигурационные данные системы резервного копирования хранятся в базе данных. В качестве СУБД Veeam Backup & Replication может использовать PostgreSQL (по умолчанию начиная с Veeam версии 12) или Microsoft SQL Server.

Учетные записи и пароли пользователей системы резервного копирования хранятся в базе данных и шифруются с помощью механизма Data Protection API (DPAPI).

5. Проблемы безопасности типовой инсталляции

Типовая инсталляция системы резервного копирования на базе Veeam Backup & Replication 12 с параметрами по умолчанию зачастую обладает следующими проблемами с точки зрения безопасности:

- Устаревшие версии. Использование неактуальных версий ПО системы резервного копирования и операционных систем для нее может приводить к уязвимостям. Важно проводить регулярное обновление.

- Копируемые данные и резервные копии хранятся в одном и том же хранилище, что может привести к потере всех данных одномоментно, в том числе в результате действия злоумышленника.
- Не используется офлайн-хранение резервных копий (копий, отделенных «воздушным зазором» от защищаемой инфраструктуры, или копий, хранящихся на выключенном оборудовании).
- Отсутствует шифрование резервных копий.
- Сетевой трафик резервного копирования не шифруется.
- Использование неперсонифицированных учетных записей или учетных записей с избыточными правами для доступа к консоли управления.
- Отсутствие двухфакторной аутентификации (2FA). Она помогает защитить доступ к интерфейсу управления Veeam.
- Сессия пользователя в консоли управления не завершается при бездействии.
- Не настроен параметр создания неизменяемых резервных копий, в том числе для хранения резервных копий конфигурации самой системы резервного копирования. При активации опции создания неизменяемых резервных копий указывается период времени, в течение которого файлы резервных копий должны быть неизменяемыми. В течение этого периода файлы резервных копий нельзя перемещать, изменять или удалять, но можно копировать. Функция неизменяемости резервных копий (даже со стороны администратора) позволяет избежать шифрования бэкапов со стороны вредоносного ПО. Такие резервные копии защищаются в течение всего своего жизненного цикла хранения.

Для системы резервного копирования на базе Veeam Backup & Replication могут быть применены 14 тактик и более 140 техник из матрицы MITRE ATT&CK (приведены в приложении 1). Для их применения достаточно низкой квалификации атакующего (условно ее можно обозначить как «киберхулиган» или «энтузиаст-одиночка»).

6. Расчет времени проникновения для инсталляции с параметрами по умолчанию

При параметрах по умолчанию только 3 из 44 превентивных контролей были реализованы, что значительно облегчает злоумышленнику реализацию недопустимых событий. Это может занять у него всего 2 шага и около 8,5 часов (см. рисунки 2 и 3).

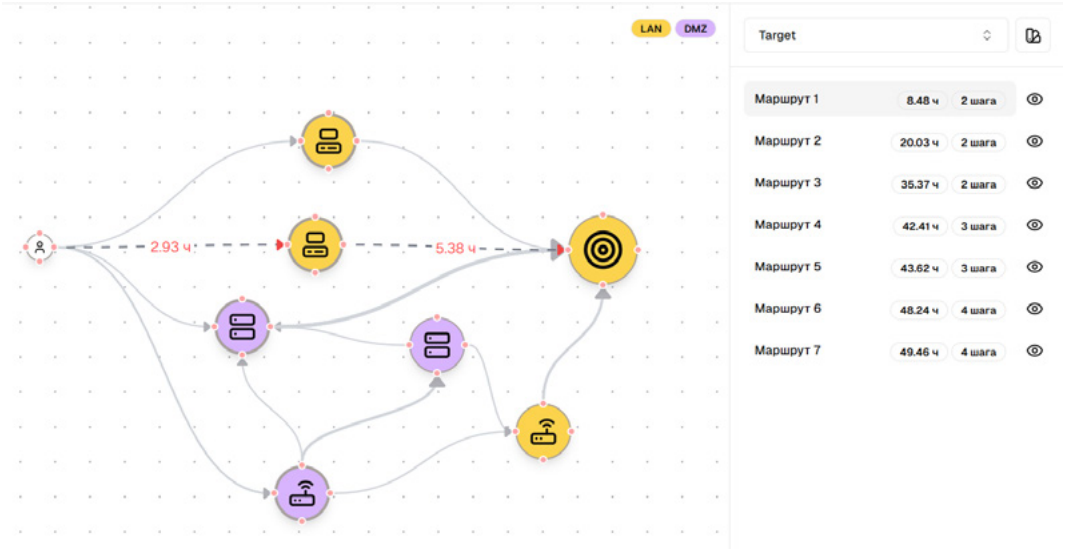


Рисунок 2. Путь атакующего до применения рекомендаций по защищенности

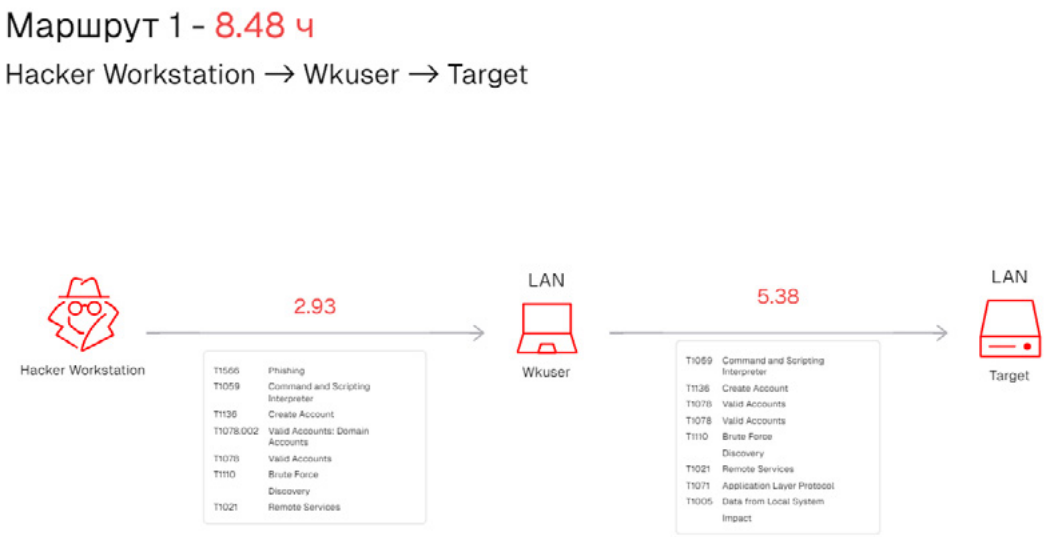


Рисунок 3. Путь атакующего до применения рекомендаций по защищенности с детализацией по техникам

7. Рекомендации по повышению защищенности

При развертывании Veeam Backup & Replication 12 автоматически применяются параметры безопасности по умолчанию. В этом разделе приведены рекомендации по повышению защищенности типовой установки Veeam Backup & Replication 12.

Соответствие рекомендаций защитным мерам из матрицы MITRE ATT&CK указано в таблице. Подробное описание рекомендаций приведено в подразделах ниже.

Таблица 1. Соответствие рекомендаций защитным мерам из матрицы MITRE ATT&CK

Рекомендация	**Защитные меры из матрицы MITRE ATT&CK**
Установка обновлений для Veeam Backup & Replication 12	M1051 — Update Software
Сегментация сети	M1030 — Network Segmentation
Использование выделенного хранилища под резервные копии	M1053 — Data Backup
Хранение не менее трех копий данных	M1053 — Data Backup
Использование не менее двух разных типов носителей для хранения резервных копий	M1053 — Data Backup
Наличие хотя бы одной резервной копии на удаленной площадке	M1029 — Remote Data Storage
Существование хотя бы одной резервной копии офлайн	M1057 — Data Loss Prevention
Шифрование резервных копий при их хранении	M1041 — Encrypt Sensitive Information
Использование шифрования на каналах связи при передаче резервных копий	M1041 — Encrypt Sensitive Information
Создание неизменяемых резервных копий	M1057 — Data Loss Prevention
Ограничение доступа к серверам репозитория с помощью IPMI-интерфейса	M1057 — Data Loss Prevention
Разработка и реализация ролевой модели доступа к системе резервного копирования	M1018 — User Account Management
Использование многофакторной аутентификации для доступа к системе резервного копирования	M1032 — Multi-factor Authentication
Применение средств обнаружения вредоносного ПО	M1049 — Antivirus/Antimalware
Регулярный анализ защищенности	M1016 — Vulnerability Scanning
Ограничение длительности сессии при бездействии пользователя	M1036 — Account Use Policies

Применение политики регулярной смены паролей	M1027 — Password Policies
Применение политики сложности паролей	M1027 — Password Policies
Изменение конфигурации протоколов SSL и TLS	M1041 — Encrypt Sensitive Information
Отключение протокола SMBv1	M1042 — Disable or Remove Feature or Program

7.1. Установка обновлений для Veeam Backup & Replication

Используйте только поддерживаемые производителем версии ПО, а также следите за выпуском новых версий, обновлений и рекомендаций по безопасности. Такие обновления содержат исправления программных ошибок и закрывают уязвимости, которые были обнаружены в ходе эксплуатации. Подпишитесь на еженедельную сводку рекомендаций по безопасности на сайте производителя. Подробнее о построении процесса управления уязвимостями можно узнать на курсе-практикуме.

Известные проблемы: нет.
Снижение производительности: нет.

7.2. Сегментация сети

Для инфраструктуры системы резервного копирования желательно использовать выделенное сетевое оборудование. Это позволит архитектурно изолировать потоки трафика резервного копирования. В случае если нет возможности использовать выделенное сетевое оборудование, рекомендуется выделить инфраструктуру системы резервного копирования в отдельный логический сетевой сегмент.

Известные проблемы: нет.
Снижение производительности: нет.

7.3. Использование выделенного хранилища под резервные копии

Для хранения резервных копий необходимо использовать выделенные хранилища (отличные от тех, которые используются для хранения продуктивных данных). Вывод из строя или взлом хранилища, где хранятся и продуктивные данные, и резервные копии, приведет к безвозвратной потере данных компании.

Известные проблемы: нет.
Снижение производительности: нет.

7.4. Хранение не менее трех копий данных

Для уменьшения рисков потери информации необходимо иметь как минимум три копии данных: продуктивные данные, основная резервная копия, копия бэкапа.

Для создания копии бэкапа настройте функцию Backup Copy для Veeam Backup & Replication согласно инструкции.

Известные проблемы: нет.
Снижение производительности: нет.

7.5. Использование не менее двух разных типов носителей для хранения резервных копий

Резервную копию данных и копию бэкапа рекомендуется хранить на двух различных типах носителей. Veeam Backup & Replication поддерживает ленты, диски, облачные хранилища и многое другое. Подробно о типах репозиториев для хранения резервных копий можно узнать в руководстве пользователя.

Известные проблемы: нет.
Снижение производительности: нет.

7.6. Наличие хотя бы одной резервной копии на удаленной площадке

Наличие хотя бы одной резервной копии на площадке, отличной от тех, на которых размещается продуктивный контур информационной системы, позволит защитить данные в случае полной потери инфраструктуры площадки. Отдельной площадкой может выступать резервный ЦОД компании, либо это может быть облачное хранилище.

Для копирования данных на удаленную площадку настройте функцию Backup Copy (см. п. 7.5). Для ускорения копирования по WAN-каналам можно использовать встроенную функцию WAN acceleration. Подробнее с функцией WAN acceleration можно ознакомиться в руководстве пользователя.

При использовании в качестве репозитория для хранения копий бэкапов объектного хранилища можно использовать функцию Scale-Out-Repositories с хранением копий бэкапов на уровне capacity tier.

Подробнее с функцией Scale-Out-Repositories можно ознакомиться в руководстве пользователя.

Известные проблемы: нет.
Снижение производительности: нет.

7.7. Существование хотя бы одной резервной копии офлайн

Существование хотя бы одной резервной офлайн-копии, отделенной «воздушным зазором» от защищаемой инфраструктуры, или копии, хранящейся на выключенном оборудовании, поможет сохранить критически важные данные даже в случае, если злоумышленник удалит как данные в продуктивной системе, так и доступные по сети резервные копии.

В качестве офлайн-носителей могут выступать отчуждаемые ленточные носители или ротируемые отчуждаемые USB- или eSATA-диски.

Рекомендуется хранить офлайн-носители на площадке, отличной от той, где хранятся продуктивные данные и основные резервные копии. Для хранения офлайн-носителей необходимо выделить физически защищенное место с контролем доступа к носителям.

Подробнее о настройке резервного копирования на ленточные носители можно узнать в руководстве пользователя.

При использовании ротируемых USB- или eSATA-носителей необходимо включить параметр «This repository is backed by rotated hard drives» в дополнительных параметрах репозитория резервных копий. Когда этот параметр включен, Veeam Backup & Replication распознает цель резервного копирования как хранилище резервных копий с ротируемыми дисками и использует специальный алгоритм, чтобы убедиться, что цепочка резервных копий, созданная на этих дисках, не нарушена.

Подробнее об использовании ротируемых носителей для резервного копирования можно узнать в руководстве пользователя.

Известные проблемы: нет.
Снижение производительности: нет.

7.8. Шифрование резервных копий при их хранении

Чтобы злоумышленник не смог изучить ваши данные в случае их кражи, рекомендуется активировать функцию шифрования резервных копий. Шифрование резервных копий преобразует данные в нечитаемый зашифрованный формат с помощью криптографического алгоритма и секретного ключа.

Для защиты данных в резервных копиях рекомендуется использовать встроенное шифрование Veeam Backup & Replication.

Следует использовать шифрование для всех резервных копий, включая копии бэкапов и резервные офлайн-копии.

Шифрование для задания на резервное копирование настраивается в окне «advanced job settings.». При настройке необходимо включить шифрование и указать пароль для защиты данных в файлах резервных копий, созданных в ходе резервного копирования.

При создании пароля для шифрования следуйте рекомендациям:

- Рекомендуемая минимальная длина пароля — 12 символов.
- Пароль должен содержать символы в верхнем и нижнем регистре.
- Пароль должен включать буквы, цифры и знаки препинания.
- Пароль должен существенно отличаться от использованных ранее.
- Пароль не должен содержать никакой реальной информации, связанной с вами, например, дату рождения, имя вашего питомца, ваше имя для входа и так далее.
- Добавьте подсказку, которая поможет вам вспомнить пароль. Подсказка для пароля отображается, когда вы импортируете зашифрованный файл или ленту на сервер резервного копирования и пытаетесь его разблокировать.
- Храните пароли в надежном месте. Если вы потеряете или забудете свой пароль, вы не сможете восстановить данные из резервных копий или лент, зашифрованных этим паролем, если только вы не используете ключи Enterprise Manager в процессе шифрования.
- Регулярно меняйте пароли для шифрования. Использование разных паролей помогает повысить уровень безопасности шифрования.

Подробнее о настройке шифрования резервных копий при их хранении можно узнать в руководстве пользователя.

Известные проблемы:

1. Шифрование данных отрицательно влияет на коэффициент дедупликации, если для резервных копий используется хранилище с функцией дедупликации.
2. При утрате пароля, установленного для заданий, данные из файла резервной копии можно будет восстановить только при определенных условиях. Подробнее про восстановление данных без пароля можно узнать в руководстве пользователя.

Снижение производительности: да.

7.9. Использование шифрования на каналах связи при передаче резервных копий

Для защиты данных при передаче по сети во время резервного копирования рекомендуется шифровать сетевой трафик. Шифрование трафика можно настроить для сетей IPv4 и IPv6. По умолчанию Veeam Backup & Replication шифрует трафик только при передаче по публичным каналам связи. Для шифрования трафика резервного копирования в локальной сети передачи данных необходимо создать сетевые правила. Шифрование сетевого трафика обеспечивается TLS-соединением.

Veeam Backup & Replication 12 поддерживает версии TLS 1.3 (частично) и 1.2.

Версии TLS 1.0 и 1.1 являются небезопасными, их рекомендуется отключить (см. раздел 7.19).

Чтобы создать сетевое правило с шифрованием трафика, выполните следующие шаги:

1. В главном меню консоли управления Veeam Backup & Replication выберите «Network Traffic Rules».

2. В поле «Name» укажите имя правила.

3. В окне «Global Network Traffic Rules» нажмите «Add» и выберите правило IPv4 или IPv6. Обратите внимание, что правило IPv6 можно добавить, только если установлен флажок «Enable IPv6 communication». Дополнительные сведения см. в разделе «IPv6 Support» руководства пользователя Veeam Backup & Replication.

4. В разделе «Source IP address range» укажите диапазон IP-адресов для компонентов инфраструктуры резервного копирования на исходном сайте.

5. В разделе «Target IP address range» укажите диапазон IP-адресов для компонентов инфраструктуры резервного копирования на целевом сайте.

6. Установите флажок «Encrypt network traffic».

Известные проблемы: нет.
Снижение производительности: да.

7.10. Создание неизменяемых резервных копий

Создание неизменяемых резервных копий, в том числе для хранения резервных копий конфигурации самой системы резервного копирования, поможет защитить данные от удаления или изменения в результате атаки злоумышленника, действия вредоносных программ или любых других вредоносных действий.

При активации функции создания неизменяемых резервных копий указывается период времени, в течение которого файлы резервных копий должны быть неизменяемыми. В течение этого периода файлы резервных копий нельзя перемещать, изменять или удалять, но можно копировать.

Функцию создания неизменяемых резервных копий можно активировать для следующих типов хранилищ:

- Dell Data Domain;
- защищенный репозиторий;
- HPE StoreOnce;
- репозиторий на базе объектного хранилища;

- масштабируемый репозиторий резервных копий.

Защищенный репозиторий представляет собой репозиторий на базе Linux-сервера, поддерживающий функции неизменяемых резервных копий и одноразовых учетных данных.

Одноразовые учетные данные используются только один раз для развертывания компонента Veeam Data Mover или транспортного сервиса при добавлении сервера Linux в инфраструктуру резервного копирования. Эти учетные данные не хранятся в инфраструктуре резервного копирования. Даже если сервер Veeam Backup & Replication будет взломан, злоумышленник не сможет получить учетные данные и подключиться к защищенному репозиторию.

Чтобы уменьшить поверхность атаки, защищенный репозиторий должен размещаться на физическом компьютере с локальным хранилищем.

Подробнее о функции создания неизменяемых резервных копий можно узнать в руководстве пользователя.

Известные проблемы: нет.
Снижение производительности: нет.

7.11. Ограничение доступа к серверам репозитория с помощью IPMI-интерфейса

При настройке создания неизменяемых резервных копий у серверов репозитория должен быть отключен или значительно ограничен доступ с использованием интерфейсов IPMI, таких как iLO, iDrack, IPMI, и иных средств, позволяющих дистанционно удалить информацию с дисков в обход средств ОС. Информацию по настройке интерфейса IPMI для конкретного типа оборудования см. в документации производителя оборудования.

Известные проблемы: нет.
Снижение производительности: нет.

7.12. Разработка и реализация ролевой модели доступа к системе резервного копирования

При выдаче прав пользователям системы резервного копирования соблюдайте принцип минимальных привилегий. Убедитесь, что всем учетным записям назначена определенная роль и что они добавлены в конкретную группу с этой ролью.

В Veeam Backup & Replication есть семь ролей пользователей с предопределенными правами. При назначении пользователю роли ознакомьтесь с функцией роли и назначайте пользователю минимально необходимую роль.

Перечень ролей и разрешенные для них действия указаны в руководстве пользователя.

При разработке ролевой модели применяйте следующие правила:

- Предоставьте каждому администратору Veeam собственную учетную запись администратора и добавьте его учетную запись администратора в соответствующую группу безопасности в Veeam, чтобы обеспечить отслеживаемость действий.
- Предоставляйте доступ только к тем задачам, которые необходимы для работы.
- Строго ограничьте количество пользователей, которые могут войти в систему с помощью Veeam Console.
- Во время эксплуатации системы мониторьте действия учетных записей на предмет подозрительной активности.

Известные проблемы: нет.
Снижение производительности: нет.

7.13. Использование многофакторной аутентификации для доступа к системе резервного копирования

Для защиты учетных записей пользователей с помощью дополнительной проверки рекомендуется включить многофакторную аутентификацию (MFA) для консоли Veeam Backup & Replication. В качестве второго метода проверки используется одноразовый пароль (OTP), сгенерированный в мобильном приложении-аутентификаторе.

Для включения многофакторной аутентификации для всех пользователей выполните следующие шаги:

1. Войдите в консоль Veeam Backup & Replication как администратор.
2. Откройте «Users and Roles» → « Security».
3. Удалите группы пользователей из списка, если они есть. Оставьте только конкретных пользователей.
4. Установите флажок «Enable multi-factor authentication (MFA)».
5. Нажмите «OK».

Подробнее об использовании функции многофакторной аутентификации и ее ограничениях можно узнать в руководстве пользователя.

Известные проблемы: нет.
Снижение производительности: нет.

7.14. Применение средств обнаружения вредоносного ПО

Применение средств антивирусной защиты на узлах, входящих в инфраструктуру системы резервного копирования, позволит защитить данные от вирусов, в том числе от вирусов-шифровальщиков.

Veeam Backup & Replication имеет встроенные методы обнаружения вредоносного ПО. Подробнее о методах обнаружения вредоносного ПО, встроенных в Veeam Backup & Replication, можно узнать в руководстве пользователя.

Известные проблемы: нет.
Снижение производительности: да.

7.15. Регулярный анализ защищенности

Veeam Backup & Replication имеет встроенный инструмент Security Analyzer, позволяющий проверить, что конфигурация серверов резервного копирования соответствует рекомендуемым производителем практикам безопасности для компонентов инфраструктуры резервного копирования на базе Microsoft Windows Server и Linux.

Рекомендуется регулярно выполнять проверку на соответствие защищенности компонентов инфраструктуры резервного копирования рекомендациям производителя.

Чтобы выполнить проверку безопасности, откройте вкладку Home консоли управления Veeam и нажмите кнопку Security & Compliance. После этого откроется окно Security & Compliance Analyzer и автоматически запустится проверка безопасности.

Известные проблемы: нет.
Снижение производительности: нет.

7.16. Ограничение длительности сессии при бездействии пользователя

Ограничение длительности сессии при бездействии пользователя исключит возможность входа другого лица от имени пользователя в случае, если тот отлучился или забыл закрыть сессию.

Установить тайм-аут для автоматического выхода из системы можно в консоли управления Veeam.

Для настройки тайм-аута выполните следующие шаги:

1. В разделе «Users and Roles» выберите «Enable auto log off after <number> min of inactivity».

2. Установите флажок и укажите количество минут.

Рекомендуемый тайм-аут для автоматического выхода из системы: 60–120 минут.

Известные проблемы: нет.
Снижение производительности: нет.

7.17. Применение политики регулярной смены паролей

О том, каким должен быть максимальный срок действия пароля, нет однозначного мнения. При слишком коротком сроке действия повышается нагрузка на подразделение, занимающееся поддержкой ИТ-инфраструктуры, так как очень часто смена пароля приводит к блокировке учетной записи пользователя.

Типичные причины блокировки при смене пароля:

- пользователь забыл сменить пароль на одном из своих устройств или в одном из приложений;
- ошибки используемого ПО, которое некорректно обрабатывают ситуацию смены пароля.

При слишком большом сроке увеличивается вероятность использования скомпрометированных паролей. Чаще всего срок действия пароля устанавливается в диапазоне от 40 до 180 дней. Решение о максимальном сроке действия пароля предлагается принимать исходя из условий и особенностей деятельности конкретной организации.

Пороговое значение блокировки рекомендуется подбирать экспериментально с диапазоном от пяти до десяти попыток аутентификации, ориентируясь на количество запросов пользователей в техническую поддержку по поводу блокировки учетной записи.

Известные проблемы: нет.
Снижение производительности: нет.

7.18. Применение политики сложности паролей

При использовании политики сложных паролей злоумышленникам труднее подобрать пароли и взломать хеши, чтобы получить несанкционированный доступ к критически важным системам.

Рекомендуемая минимальная длина пароля — 12 символов. В пароле должны быть как минимум три из четырех групп символов.

Известные проблемы: нет.
Снижение производительности: нет.

7.19. Изменение конфигурации протоколов SSL и TLS

Протоколы SSL 2.0 и 3.0 имеют хорошо известные уязвимости безопасности, и их рекомендуется отключить. Протоколы TLS 1.0 и 1.1 являются устаревшими, их также рекомендуется отключить.

Для отключения протоколов SSL 2.0 и 3.0 установите следующие значения для следующих ключей реестра:

Значение 1:

- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client\DisabledByDefault
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\DisabledByDefault
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client\DisabledByDefault
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\DisabledByDefault

Значение 0:

- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client\Enabled
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client\Enabled
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled

При отключении TLS установите следующие значения для следующих ключей реестра:

Значение 1:

- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client\DisabledByDefault
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\DisabledByDefault
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client\DisabledByDefault
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\DisabledByDefault

Значение 0:

- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client\Enabled
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client\Enabled
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled

Известные проблемы: нет.
Снижение производительности: нет.

7.20. Отключение протокола SMBv1

С помощью команд PowerShell проверьте, отключен ли на серверах протокол SMBv1. Для Windows 2012 R2 и выше используйте следующие команды:

- Get-WindowsFeature FS-SMB1).Installed

- Get-SmbServerConfiguration \| Select EnableSMB1Protocol

Значение True в полученном результате выполнения команды означает, что протокол SMBv1 включен.

Отключить протокол SMBv1 можно двумя способами:

1. С помощью команд (для Windows 2012 R2 и выше):

- Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
- Set-SmbServerConfiguration -EnableSMB1Protocol $false

2. С использованием групповых политик по инструкции Microsoft.

Известные проблемы: при использовании Windows XP или Windows Server 2003, при использовании устаревшей функциональности «Просмотр сетевого окружения», а также при использовании устаревших моделей МФУ могут возникнуть проблемы при использовании протокола SMB версии выше 1.

Снижение производительности: нет.

8. Расчет времени проникновения (TTA) после применения рекомендаций

После применения рекомендаций количество реализованных превентивных контролей выросло до 15 из 43. Благодаря этому расчетное TTA увеличилось до 13 часов (см. рисунки 4 и 5).

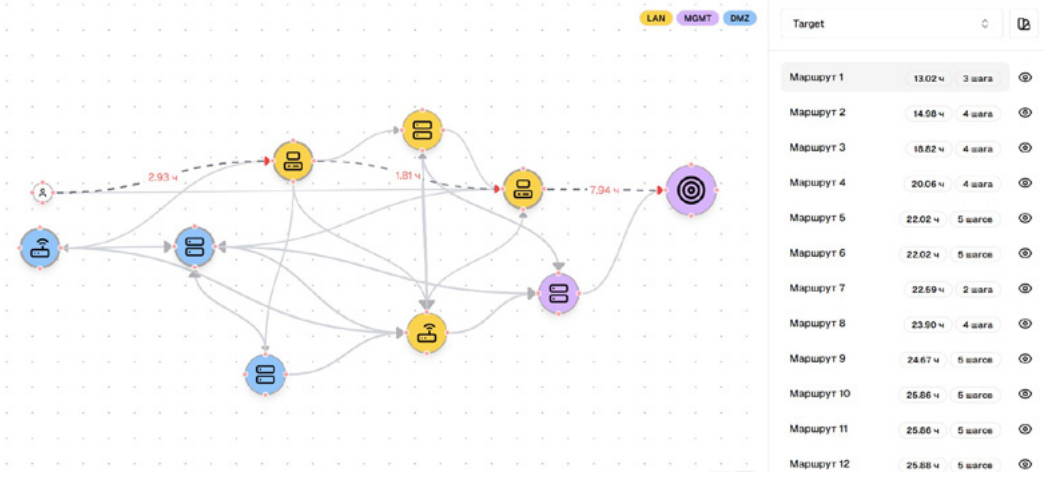


Рисунок 4. Путь атакующего после применения рекомендаций

Рисунок 5. Путь атакующего после применения рекомендаций с детализацией по техникам

9. Заключение

После примененного харденинга благодаря размещению системы резервного копирования в отдельном сетевом сегменте с ограничением доступа к сегменту увеличилось количество точек на пути злоумышленника в цепочке атаки. Кроме того, увеличилось время выполнения атаки на сервер резервного копирования. Общее время атаки увеличилось почти на 60%. Таким образом, у команды мониторинга и реагирования будет больше времени на детектирование и локализацию действий злоумышленника. При этом нужно отметить, что для значительного увеличения времени атаки и ее усложнения необходимо провести мероприятия по защите не только целевой системы, но и всех ключевых систем в ИТ-инфраструктуре, через которые может развиваться цепочка атаки.

В результате харденинга увеличилось время выполнения атаки, к тому же, злоумышленнику потребуется применять более сложные техники, чтобы попытаться украсть резервные копии. Более того, вследствие применения рекомендации по шифрованию резервных копий при их хранении, даже в случае успешной атаки злоумышленнику нужно будет расшифровать данные.

После применения рекомендаций по созданию неизменяемых и резервных копий уничтожение резервных копий становится для злоумышленника трудноосуществимой задачей и может быть достигнуто только за очень продолжительное время (не менее срока жизни неизменяемых копий) и с применением комбинированных методов атаки, включая физический доступ к носителям и уничтожение или кражу копий.

Приложение 1

Применимые тактики и техники из матрицы MITRE ATT&CK

В рамках тактики «Разведка» могут быть применены следующие техники:

- T1589 — сбор информации об атакуемых пользователях;
- T1590 — сбор информации об атакуемой сетевой инфраструктуре;
- T1591 — сбор бизнес-информации об атакуемой организации;
- T1592 — сбор информации об атакуемых узлах;
- T1593 — поиск на общедоступных сайтах;
- T1594 — поиск на сайтах атакуемой организации;
- T1595 — активное сканирование;
- T1596 — поиск технической информации в общедоступных источниках;
- T1597 — поиск в закрытых источниках;
- T1598 — фишинг с целью сбора сведений.

В рамках тактики «Подготовка ресурсов» могут быть применены следующие техники:

- T1583 — приобретение инфраструктуры;
- T1584 — компрометация сторонней инфраструктуры;
- T1585 — создание учетных записей;
- T1586 — компрометация учетных записей;
- T1587 — разработка собственных средств;
- T1588 — подготовка необходимых средств;
- T1608 — размещение средств;
- T1650 — приобретение доступа.

В рамках тактики «Первоначальный доступ» могут быть применены следующие техники:

- T1078 — существующие учетные записи;
- T1091 — распространение через съемные носители;
- T1190 — недостатки в общедоступном приложении;
- T1195 — компрометация цепочки поставок;
- T1199 — доверительные отношения;
- T1566 — фишинг.

В рамках тактики «Выполнение» могут быть применены следующие техники:

- T1047 Инструментарий управления Windows;
- T1053 — запланированная задача (задание);

- T1059 — интерпретаторы командной строки и сценариев;
- T1072 — средства развертывания ПО;
- T1106 — нативный API;
- T1129 — общие модули;
- T1203 — эксплуатация уязвимостей в клиентском ПО;
- T1204 — выполнение с участием пользователя;
- T1569 — системные службы.

В рамках тактики «Закрепление» могут быть применены следующие техники:

- T1037 — сценарии инициализации при загрузке или входе в систему;
- T1053 — запланированная задача (задание);
- T1078 — существующие учетные записи;
- T1098 — манипуляции с учетной записью;
- T1136 — создание учетной записи;
- T1197 Задания BITS
- T1205 — передача управляющих сигналов в трафике;
- T1505 — компонент серверного ПО;
- T1547 — автозапуск при загрузке или входе в систему;
- T1556 — изменение процесса аутентификации;
- T1574 — перехват потока исполнения.

В рамках тактики «Повышение привилегий» могут быть применены следующие техники:

- T1037 — сценарии инициализации при загрузке или входе в систему;
- T1053 — запланированная задача (задание);
- T1055 — внедрение кода в процессы;
- T1068 — эксплуатация уязвимостей для повышения привилегий;
- T1078 — существующие учетные записи;
- T1134 Манипуляции с токенами доступа;
- T1484 Изменение доменной политики;
- T1547 — автозапуск при загрузке или входе в систему;
- T1548 Обход механизмов контроля привилегий;
- T1574 — перехват потока исполнения.

В рамках тактики «Предотвращение обнаружения» могут быть применены следующие техники:

- T1006 Прямой доступ к тому;
- T1014 Руткит;

- T1027 Обфусцированные файлы или данные;
- T1036 Маскировка;
- T1055 Внедрение кода в процессы;
- T1070 Устранение индикаторов;
- T1078 Существующие учетные записи;
- T1112 Изменение реестра;
- T1127 Выполнение через доверенные утилиты разработчика;
- T1134 Манипуляции с токенами доступа;
- T1140 Деобфускация/декодирование файлов или данных;
- T1197 Задания BITS;
- T1202 Непрямое выполнение команд;
- T1205 Передача управляющих сигналов в трафике;
- T1207 Поддельный контроллер домена;
- T1211 Эксплуатация уязвимостей для предотвращения обнаружения;
- T1216 Выполнение через системный сценарий;
- T1218 Выполнение с помощью системных бинарных файлов;
- T1222 Изменение разрешений для файлов и каталогов;
- T1480 Ограничения на исполнение;
- T1484 Изменение доменной политики;
- T1548 Обход механизмов контроля привилегий;
- T1550 Использование альтернативных сущностей для аутентификации;
- T1553 Нарушение работы средств контроля доверия;
- T1556 Изменение процесса аутентификации;
- T1562 Ослабление защиты;
- T1564 Сокрытие артефактов;
- T1574 Перехват потока исполнения;
- T1599 Преодоление границ сети;
- T1600 Понижение надежности шифрования;
- T1622 Предотвращение отладки.

В рамках тактики «Получение учетных данных» могут быть применены следующие техники:

- T1003 Получение дампа учетных данных;
- T1040 Прослушивание сетевого трафика;
- T1056 Перехват вводимых данных;
- T1110 Метод перебора;
- T1187 Принудительная аутентификация;
- T1212 Эксплуатация уязвимостей для получения учетных данных;

- T1528 Кража токена доступа к приложению;
- T1539 Кража сессионных куки;
- T1552 Незащищенные учетные данные;
- T1555 Учетные данные из хранилищ паролей;
- T1556 Изменение процесса аутентификации;
- T1557 «Злоумышленник посередине»;
- T1558 Кража или подделка билетов Kerberos;
- T1606 Подделка учетных данных для веб-ресурсов.

В рамках тактики «Изучение» могут быть применены следующие техники:

- T1007 Изучение системных служб;
- T1010 Изучение открытых приложений;
- T1012 Запросы к реестру;
- T1016 Изучение конфигурации сети;
- T1018 Изучение удаленных систем;
- T1033 Изучение владельца или пользователей системы;
- T1040 Прослушивание сетевого трафика;
- T1046 Изучение сетевых служб;
- T1049 Изучение сетевых подключений;
- T1057 Изучение процессов;
- T1069 Изучение групп разрешений;
- T1082 Изучение системы;
- T1083 Изучение файлов и каталогов;
- T1087 Изучение учетных записей;
- T1124 Изучение системного времени;
- T1135 Изучение общих сетевых ресурсов;
- T1201 Изучение парольной политики;
- T1482 Изучение доверительных отношений между доменами;
- T1518 Изучение установленного ПО;
- T1615 Изучение групповой политики;
- T1622 Предотвращение отладки;
- T1652 Изучение драйверов устройств.

В рамках тактики «Перемещение внутри периметра» могут быть применены следующие техники:

- T1080 — заражение общего содержимого;
- T1210 — эксплуатация уязвимостей в удаленных службах;
- T1534 — внутренний целевой фишинг;

- T1570 — передача инструментов внутри периметра.

В рамках тактики «Сбор данных» могут быть применены следующие техники:

- T1005 — данные из локальной системы;
- T1039 — данные с общих сетевых дисков;
- T1056 — перехват вводимых данных;
- T1074 — промежуточное хранение данных;
- T1119 — автоматизированный сбор данных;
- T1557 — «злоумышленник посередине»;
- T1560 — архивация собранных данных.

В рамках тактики «Организация управления» могут быть применены следующие техники:

- T1001 Обфускация данных;
- T1008 Резервные каналы;
- T1071 Протокол прикладного уровня;
- T1090 Прокси-сервер;
- T1095 Протоколы (кроме прикладного уровня);
- T1102 Веб-служба;
- T1104 Отдельный канал для каждого этапа;
- T1105 Передача инструментов из внешней сети;
- T1132 Кодирование данных;
- T1205 Передача управляющих сигналов в трафике;
- T1219 ПО для удаленного доступа;
- T1568 Динамическое разрешение;
- T1571 Нестандартный порт;
- T1572 Туннелирование протокола;
- T1573 Зашифрованный канал.

В рамках тактики «Эксфильтрация данных» могут быть применены следующие техники:

- T1011 Эксфильтрация через альтернативную сетевую среду;
- T1020 Автоматизированная эксфильтрация;
- T1029 Передача по расписанию;
- T1030 Ограничение размера передаваемых блоков данных;
- T1041 Эксфильтрация по каналу управления;
- T1048 Эксфильтрация по альтернативному протоколу;
- T1567 Эксфильтрация через веб-службу.

В рамках тактики «Деструктивное воздействие» могут быть применены следующие техники:

- T1485 Уничтожение данных;
- T1486 Шифрование данных;
- T1489 Остановка службы;
- T1490 Препятствование восстановлению системы;
- T1496 Несанкционированное использование ресурсов;
- T1498 Сетевой отказ в обслуживании;
- T1499 Точечный отказ в обслуживании;
- T1529 Завершение работы или перезагрузка системы;
- T1531 Прекращение доступа к учетной записи;
- T1561 Уничтожение диска;
- T1565 Манипуляции с данными.