Бютнер С.И. Методы противодействия атаке типа «ПОДМЕНА МАРШРУТА» (BGP HIJACKING) // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 1(51) с. 77–80

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.736

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ АТАКЕ ТИПА «ПОДМЕНА МАРШРУТА» (BGP HIJACKING)

Бютнер С.И.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: serafimkavasaki@gmail.com

BGP hijacking, или подмена маршрута, — это атака на протокол маршрутизации Border Gateway Protocol (BGP), которая позволяет злоумышленникам перенаправлять или перехватывать интернет-трафик. Такие атаки могут использоваться для шпионажа, кражи данных или саботажа. В статье обсуждаются методы противодействия BGP hijacking, включая использование RPKI, мониторинг аномалий и внедрение криптографической защиты в BGP. Эти меры способны повысить устойчивость сети и снизить вероятность компрометации маршрутов.

Ключевые слова: BGP hijacking, подмена маршрута, маршрутизация, RPKI, кибербезопасность, защита сети, аномалии трафика.

METHODS OF COUNTERING A "ROUTE SUBSTITUTION" TYPE ATTACK (BGP HIJACKING)

Buetner S.I.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com

BGP hijacking, or route hijacking, is an attack on the Border Gateway Protocol (BGP) that allows attackers to redirect or intercept internet traffic. These attacks can be used for espionage, data theft, or sabotage. The article explores methods to counter BGP hijacking, including the use of RPKI, anomaly monitoring, and cryptographic protection in BGP. These measures can enhance network resilience and reduce the likelihood of route compromise.

Keywords: BGP hijacking, route hijacking, routing, RPKI, cybersecurity, network protection, traffic anomalies.

Введение

Протокол BGP (Border Gateway Protocol) является основой современной маршрутизации в Интернете, связывая автономные системы (AS) между собой для обеспечения глобальной передачи данных. Однако из-за отсутствия встроенных механизмов аутентификации и проверки маршрутов, BGP уязвим к атакам, известным как BGP hijacking или подмена маршрута. В рамках этой атаки злоумышленники могут объявлять неверные маршруты, перенаправляя трафик через подконтрольные им сети, что может привести к утечке данных, отказу в обслуживании и даже созданию условий для массовых атак.

BGP hijacking остаётся серьёзной угрозой как для крупных провайдеров, так и для малых сетей. Известные случаи, такие как перенаправление трафика финансовых организаций или шпионаж через ложные маршруты, показывают, насколько разрушительными могут быть

такие атаки. Учитывая ключевую роль протокола BGP в функционировании Интернета, разработка эффективных методов противодействия этим атакам становится приоритетной задачей для операторов сетей и специалистов по кибербезопасности.

Методы противодействия атаке типа «подмена маршрута»

Атака типа BGP hijacking начинается с того, что злоумышленник отправляет неверные анонсы маршрутов в BGP. Эти ложные маршруты могут быть направлены на перенаправление трафика через вредоносную автономную систему, создание "чёрной дыры" (blackhole) для блокировки доступа к ресурсам или проведение атаки "человек посередине" (MITM), чтобы перехватывать данные. Главная причина уязвимости BGP заключается в его архитектуре, где маршруты принимаются на веру, без проверки их достоверности[1].

Для противодействия таким атакам разрабатываются различные методы защиты, которые можно условно разделить на три категории: криптографические решения, мониторинг аномалий и организационные меры.

Одним из наиболее перспективных методов защиты от BGP hijacking является использование RPKI. Эта технология позволяет провайдерам удостоверять подлинность объявляемых маршрутов с помощью цифровых подписей. С помощью RPKI маршруты проверяются на соответствие авторитетным записям, что исключает возможность анонсирования несанкционированных маршрутов. Однако RPKI сталкивается с рядом проблем, включая сложность внедрения и необходимость участия большого количества автономных систем для достижения глобального эффекта[2].

Ещё одним важным аспектом защиты является мониторинг аномалий в BGP-объявлениях. Сервисы, такие как BGPmon и RIPE Atlas, позволяют отслеживать подозрительные изменения маршрутов, например, внезапное увеличение количества объявляемых префиксов или изменение маршрутов крупных сетей. Операторы могут настроить автоматическое уведомление о таких событиях, что позволяет быстро реагировать на возможные атаки[3].

Фильтрация маршрутов предполагает настройку списков доступа и политик BGP для ограничения приёма маршрутов только от доверенных источников. Например, крупные провайдеры могут заранее договариваться о фильтрации неверных маршрутов на основе договорённостей с соседними автономными системами (AS). Эта мера снижает вероятность успешной атаки, но требует значительных ресурсов для поддержания актуальных списков[4].

Хотя BGP изначально не был разработан с учётом безопасности, современные инициативы, такие как BGPsec, направлены на интеграцию механизмов шифрования и аутентификации. BGPsec использует цифровые подписи для проверки аутентичности маршрутов, передаваемых через сети. Несмотря на преимущества, внедрение BGPsec сопряжено с высокими затратами и сложностями, связанными с необходимостью обновления оборудования и программного обеспечения[4].

Организационные меры включают в себя повышение осведомлённости о рисках BGP hijacking среди сетевых администраторов и внедрение стандартов, таких как MANRS (Mutually Agreed Norms for Routing Security). MANRS предлагает набор рекомендаций для операторов сетей, включая улучшение фильтрации маршрутов, предотвращение спуфинга (подделки источников IP-адресов) и обмен информацией о возможных угрозах[5].

В реальном мире даже небольшие автономные системы могут стать участниками крупных атак из-за отсутствия должной настройки маршрутов. Например, в 2018 году ложный маршрут, объявленный одной из азиатских телекоммуникационных компаний, привёл к перенаправлению трафика Google через Россию и Китай. Этот случай продемонстрировал, насколько критично глобальное сотрудничество и согласованность в сфере маршрутизации.

Заключение

BGP hijacking остаётся одной из наиболее серьёзных угроз для глобальной маршрутизации в Интернете. Учитывая отсутствие встроенных механизмов безопасности в протоколе BGP, атаки на маршруты могут использоваться как для кражи данных, так и для масштабного саботажа.

Методы противодействия, такие как внедрение RPKI, использование инструментов мониторинга и фильтрации маршрутов, а также криптографическая защита, являются ключевыми инструментами в борьбе с этой угрозой. Однако их эффективность напрямую зависит от готовности операторов сетей инвестировать в новые технологии и сотрудничать на глобальном уровне.

Для обеспечения надёжной защиты необходимо не только внедрять технические меры, но и следовать стандартам безопасности, таким как MANRS, которые способствуют повышению устойчивости всей маршрутизационной экосистемы. В эпоху растущих угроз BGP hijacking играет всё более важную роль в дискуссиях о будущем Интернета, подчёркивая необходимость совместных усилий в области сетевой безопасности.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
3. Лаврова Д. С. и др. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 3. – С. 70-77.
4. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
5. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры / А. М. Гельфанд, В. В. Сигачева, А. В. Архипов, Л. К. Сиротина // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2023. – № 3. – С. 21-27. – DOI 10.46418/2079-8199_2023_3_3. – EDN BKGRAY.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
2. Lesnova E. M., Pestov I. E. Development of a method error detection and correction for a distributed information network based on big data //Regional Informatics and Information Security. - 2018. – pp. 236-240.
3. Lavrova D. S. et al. Preventing Dos attacks by predicting the values of correlation parameters of network traffic //Problems of information security. Computer systems. – 2018. – No. 3. – pp. 70-77.
4. Minyaev A. A. Method for evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
5. Analysis and risk management of information security of an object of critical information infrastructure / A.M. Gelfand, V. V. Sigacheva, A.V. Arkhipov, L. K. Sirotina // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2023. – No. 3. – pp. 21-27. – DOI 10.46418/2079-8199_2023_3_3. – EDN BKGRAY.