Бютнер С.И. Подмена DNS-запросов в микропрограммах маршрутизаторов для скрытой передачи данных // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 3(53) с. 103–106

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ПОДМЕНА DNS-ЗАПРОСОВ В МИКРОПРОГРАММАХ МАРШРУТИЗАТОРОВ ДЛЯ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ

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

Подмена DNS-запросов в прошивках маршрутизаторов представляет собой один из современных методов скрытой передачи данных, который может использоваться злоумышленниками для кражи информации, обхода сетевых фильтров или создания каналов для удалённого управления заражёнными устройствами. В данной статье рассматриваются принципы работы этой атаки, её последствия для пользователей и организаций, а также способы защиты, включая мониторинг сетевого трафика, использование безопасных DNS-серверов и регулярное обновление прошивок маршрутизаторов.

Ключевые слова: Подмена DNS, маршрутизаторы, скрытая передача данных, компрометация прошивки, безопасность сети, утечка данных.

SPOOFING DNS QUERIES IN ROUTER FIRMWARE FOR COVERT DATA TRANSFER

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

DNS query spoofing in router firmware is a modern method of covert data transmission that can be used by attackers to steal information, bypass network filters, or create channels for remote control of compromised devices. This article explores the principles behind this attack, its consequences for users and organizations, and protection methods, including network traffic monitoring, using secure DNS servers, and regularly updating router firmware.

Keywords: DNS spoofing, routers, covert data transmission, firmware compromise, network security, data leakage.

Введение

Современные маршрутизаторы являются не только ключевыми элементами сетевой инфраструктуры, но и потенциальными целями для атак, направленных на компрометацию их прошивок. Одной из таких атак является подмена DNS-запросов на уровне микропрограммного обеспечения маршрутизатора с целью скрытой передачи данных. Этот метод представляет собой серьёзную угрозу для безопасности как частных пользователей, так и корпоративных сетей, так как позволяет злоумышленникам манипулировать трафиком без непосредственного вмешательства на уровне конечных устройств.

DNS (Domain Name System) играет критическую роль в работе Интернета, переводя доменные имена в IP-адреса. Если злоумышленник получает контроль над DNS-запросами, он

может перенаправлять пользователей на вредоносные сайты, перехватывать передаваемую информацию или использовать DNS-запросы для создания скрытых каналов передачи данных. Особую опасность представляет подмена DNS-запросов, встроенная в прошивку маршрутизатора, так как этот метод позволяет атакам оставаться незаметными для стандартных антивирусных решений и систем мониторинга безопасности.

Подмена DNS-запросов в микропрограммах маршрутизаторов для скрытой передачи данных

Одним из наиболее изощрённых методов манипуляции сетевым трафиком является внедрение вредоносного кода в микропрограммы маршрутизаторов с целью подмены DNS-запросов. Эта техника позволяет злоумышленникам скрытно контролировать сетевые соединения пользователей, модифицировать маршрутизацию трафика и даже передавать данные в обход традиционных систем обнаружения[1].

Атака начинается с компрометации маршрутизатора, которая может происходить через использование уязвимостей в прошивке, слабых паролей администратора или поддельных обновлений программного обеспечения. После получения доступа злоумышленник внедряет вредоносный код в прошивку маршрутизатора, который изменяет обработку DNS-запросов. В результате при попытке пользователя обратиться к определённому домену маршрутизатор может подменять ответ DNS-сервера, направляя трафик на контролируемый злоумышленниками ресурс[2].

Однако возможности данной атаки не ограничиваются простым перенаправлением пользователей на фишинговые сайты. Более сложные схемы позволяют использовать DNS-запросы в качестве скрытого канала передачи данных. Вредоносное ПО на компрометированном устройстве может кодировать информацию в специфические DNS-запросы, которые маршрутизатор затем отправляет на сервер атакующего. Этот метод делает передачу данных практически незаметной для традиционных средств обнаружения, поскольку DNS-запросы считаются стандартной частью сетевого взаимодействия и редко подвергаются детальному анализу[3].

Одним из известных примеров использования подобных техник является применение DNS-туннелирования для обхода межсетевых экранов и фильтрации трафика. Вредоносные программы могут встраивать конфиденциальную информацию в поддельные DNS-запросы, а атакующий сервер, получая их, расшифровывает переданные данные. Такой подход позволяет злоумышленникам скрытно извлекать данные из корпоративных сетей, передавать команды заражённым устройствам или организовывать удалённое управление ботнетами[4].

Использование подмены DNS-запросов в прошивках маршрутизаторов также делает обнаружение атаки значительно сложнее. В отличие от вредоносного ПО на компьютере, которое можно выявить с помощью антивирусных решений, вредоносные изменения в микропрограмме маршрутизатора остаются незамеченными до тех пор, пока администратор сети не проведёт детальный анализ трафика или не заменит прошивку на официальную версию.

Защита от данной атаки требует комплексного подхода. В первую очередь пользователи должны регулярно обновлять прошивки маршрутизаторов, так как производители периодически выпускают патчи для устранения уязвимостей. Кроме того, рекомендуется

отключить удалённое управление маршрутизатором, если оно не используется, и сменить стандартные пароли администратора на более сложные[5].

Одним из эффективных методов защиты является использование безопасных DNS-серверов с поддержкой DNS over HTTPS (DoH) или DNS over TLS (DoT). Эти протоколы обеспечивают шифрование DNS-запросов, что затрудняет их перехват и подмену. Также следует использовать системы мониторинга трафика, которые могут выявлять аномальные DNS-запросы, указывающие на возможное наличие скрытого канала передачи данных.

Корпоративным пользователям рекомендуется применять сегментацию сети, ограничивая доступ маршрутизаторов к критически важным системам, а также использовать инструменты анализа трафика и детектирования аномалий. Внедрение правил брандмауэра для фильтрации подозрительных DNS-запросов и запрет использования нестандартных DNS-серверов также может помочь в предотвращении атак.

Современные маршрутизаторы играют важную роль в обеспечении безопасности сети, и их компрометация может привести к серьёзным последствиям, включая утечку конфиденциальной информации и потерю контроля над устройствами. Подмена DNS-запросов в прошивках маршрутизаторов остаётся одной из наиболее сложных для обнаружения угроз, требующей как технических мер защиты, так и осведомлённости пользователей о рисках, связанных с использованием устаревшего и неподдерживаемого сетевого оборудования.

Заключение

Подмена DNS-запросов в микропрограммах маршрутизаторов представляет собой опасный вектор атаки, который позволяет злоумышленникам скрыто управлять трафиком, организовывать скрытые каналы передачи данных и компрометировать сетевую инфраструктуру. Данная угроза особенно опасна тем, что остаётся незамеченной при стандартных методах защиты, поскольку изменения в прошивке маршрутизатора трудно обнаружить без специализированного анализа трафика и оборудования.

Защита от подобных атак требует регулярного обновления прошивок, использования безопасных DNS-серверов и мониторинга сетевого трафика для выявления аномалий. В условиях растущей киберугрозы пользователи и компании должны уделять особое внимание безопасности маршрутизаторов, так как их компрометация может стать первым шагом к более масштабной атаке на всю сеть. Только комплексный подход к обеспечению безопасности сетевых устройств может минимизировать риски и защитить критически важные данные от несанкционированного доступа.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
2. 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.

3. 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.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

1. Kotenko I. V. and others. A touchscreen-based human-machine interaction model for monitoring the security of computer networks. – 2018.
2. Minyaev A. A. Method of evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
3. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on big data //Regional Informatics and information security. - 2018. pp. 236-240.
4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 345-348.
5. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelec communications in science and education. - 2021. – pp. 409-414.