Способ защиты информационных систем от атак с использованием DNS-кэша клиента

В.А. Копылов, e-mail: vladkop.ru@mail.ru

Краснодарское высшее военное училища имени генерала армии С.М.Штеменко

Ключевые слова: *По мере того, как усилия систем защиты направляются на повышение безопасности сервера, злоумышленники развивают атаки с использованием DNS-кэша клиента, в которых пользователи имеют ограниченные ресурсы и возможности. DNS-атаки позволяют незаметно разрушить кэш пользователя путем фальсификации ответов DNS. В отличие от существующих статичных методов, в этой статье предлагается освободить пользователя от тяжёлой работы по предотвращению неуловимых атак DNS клиента с помощью метода защиты движущихся целей (MTD). Способ защиты информационных систем от атак DNS-кэша относится к области обеспечения безопасности информационных систем и может быть использован в системах предотвращения компьютерных атак.*

Ключевые слова: *DNS, защита движущейся цели, информационная система, компьютерная атака.*

Введение

По мере того как повсеместное использование мобильной связи перерастает традиционные модели сетевых услуг, провайдеры стараются удовлетворять потребности в повсеместном доступе. Большинство крупных провайдеров, предлагающих услугу доменных имен (DNS) [1-3] для пользователей, уменьшают задержки и повышают эффективность, что приводит к созданию уязвимостей. Злоумышленники используют множество способов, чтобы вторгнуться или повредить DNS-серверы и побуждают разрабатывать технологии защиты на стороне сервера, чтобы повысить живучесть системы при атаках [4,5]. Тем не менее, по сравнению с защитой сервера, безопасность клиента неравномерна и крайне несущественна. Существующие комплексные средства противодействия обнаружению или блокировке [6-8] практически невозможно применить на стороне клиента из-за их высокой стоимости. Поскольку пассивная защита обречена быть недостаточной против постоянно совершенствующихся кибератак, разработка подходов к защите с использованием защиты движущихся целей (MTD) [9, 10] является необходимой. Многие технологии уже были разработаны для защиты DNS [11, 12], но большая

часть предыдущих работ направлена на безопасность на стороне сервера. Несмотря на то, что разработанные методы обеспечивают достаточно высокий уровень безопасности [13], некоторые недостатки еще предстоит решить. Во-первых, почти все существующие технологии предъявляют чрезмерно высокие требования к ресурсам, что делает их нереалистичными для клиентских устройств с ограниченными ресурсами. Во-вторых, эффективность защитного механизма быстро ухудшается против динамической среды из-за отсутствия адаптируемости.

Основной целью данного исследования является разработка способа защиты информационных систем от атак DNS-кэша.

Исходя из поставленной цели, были сформулированы следующие задачи:

- рассмотреть механизм реализации DNS-атаки на стороне клиента;
- разработать способ защиты информационных систем от атак DNS-кэша на стороне клиента, засоряющих кэш поддельными ответами на основании технологий виртуализации и «защиты движущейся цели».

1. Материалы и результаты исследования

Ответы от DNS-серверов на запросы пользователей сохраняются в течение определенного периода времени в кэше DNS, что позволяет удовлетворять пользователей, отправляющих один и тот же запрос, меньшими задержками и получать лучшую эффективность использования ресурсов. Но данная схема содержит уязвимости, которые используют злоумышленники [14]. Например, атака с отравлением кэша DNS на стороне клиента может внедрить вредоносные программы и отправлять запросы на DNS сервер. Затем пользователю отправляется поддельный ответ от злоумышленника, благодаря чему злоумышленник постепенно манипулирует кэшем пользователя. Атаки на DNS-кэш выполняются путем замены элементов в таблице DNS-кэша фальшивыми, что открывает путь к дальнейшему повреждению системы, перехвату запросов или утечкам конфиденциальности [15, 16]. На рис. 1 показан пример DNS-атаки клиента.

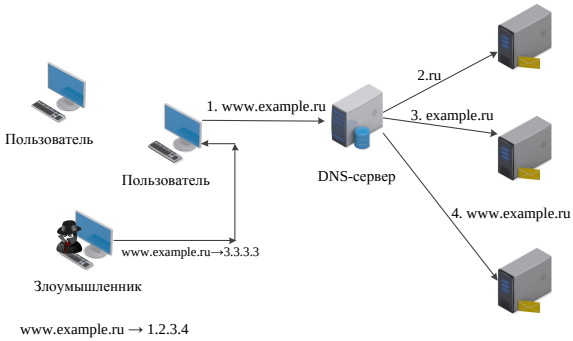

Рис. 1. Пример DNS-атаки на стороне клиента

Разработанный способ защиты информационных систем от атак DNS-кэша на стороне клиента позволяет повысить результативность защиты, за счет использования метода защиты движущихся целей (MTD), а также использования технологий виртуализации, что достигается имитацией поочередной работы большого числа пользователей сети с постоянно изменяющимися параметрами адресации.

Реализация предлагаемого способа защиты поясняется обобщенной структурно-логической последовательностью, представленной на рис. 2, где на начальном этапе задается количество виртуальных сетевых карт (блок 1), для каждой виртуальной сетевой карты задается MAC-адрес и доменное имя (блок 2). После чего задается время и порядок переключения между виртуальными сетевыми картами (блок 3).

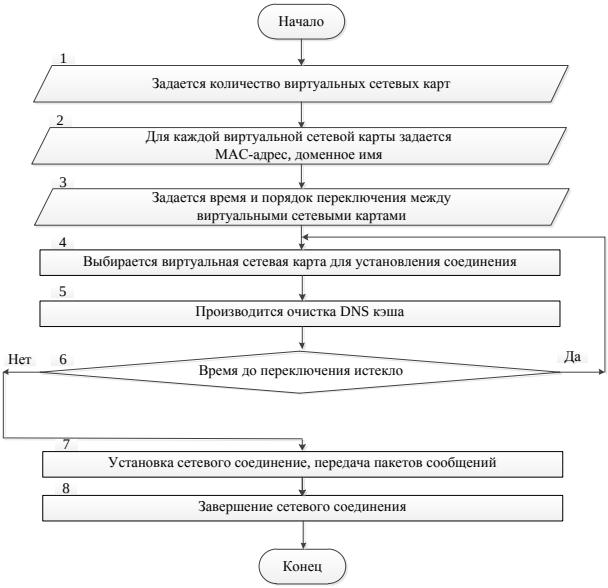

Рис. 2. Блок схема последовательности действий, реализующих способ защиты информационных систем от атак DNS-кэша на стороне клиента

На следующем этапе выбирается виртуальная сетевая карта для установления соединения (блок 4) и производится очистка DNS-кэша (блок 5) для удаления всей информации о ранее осуществляемых соединениях.

После установления соединения (блок 7) осуществляется передача пакетов сообщений. Если после передачи пакетов сообщений для обмена информацией не осталось, производится завершение соединения (блок 8). Если после передачи пакетов сообщения остались, но время до переключения истекло (блок 6), соединение разрывается и производится установка сетевого соединения с использованием следующей виртуальной сетевой карты (блоки 4, 5, 7).

Заключение

Таким образом, в разработанном способе защиты информационных систем от атак DNS-кэша на стороне клиента обеспечивается повышение результативности защиты, за счет использования метода защиты движущихся целей (MTD), а также использования технологий виртуализации, что достигается имитацией поочередной работы

большого числа пользователей сети с постоянно изменяющимися параметрами адресации.

Предлагаемый способ защиты информационных систем от атак DNS-кэша на стороне клиента позволяет вносить изменения на клиентских устройствах только на программном уровне, что уменьшает стоимость и затраты на реализацию системы защиты.

Литература

1. RFC 1034. Domain Names Concepts and Facilities (DNS). 1987. [Электронный ресурс]: база данных. – URL: https://tools.ietf.org/html/rfc1034 (дата обращения: 29.11.2021).
2. RFC 1035. Domain names implementation and specification (DNS). 1987. [Электронный ресурс]: база данных. – URL: https://tools.ietf.org/html/rfc1035 (дата обращения: 29.11.2021).
3. Олифер, В. Компьютерные Сети. Принципы, технологии, протоколы: / В. Олифер, Н. Олифер : учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.
4. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 166-173.
5. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2009. – № 1(72). – С. 181-187.
6. Соколовский, С. П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н.Е. Жуковского: Сборник научных статей VIII Международной научно-практической конференции «Научные чтения имени профессора Н.Е. Жуковского», Краснодар, 20–21 декабря 2017 года / КВВАУЛ им. Героя Советского Союза А.К. Серова. – Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг", 2018. – С. 47-52.
7. Соколовский, С. П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения : Материалы XXIII Международной научно-практической конференции,

посвященной памяти генерального конструктора ракетно-космических систем академика М.Ф. Решетнева. В 2-х частях, Красноярск, 11–15 ноября 2019 года / Под общей редакцией Ю.Ю. Логинова. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева", 2019. – С. 447-448.

8. Патент № 2355024 C2 Российская Федерация, МПК G06F 15/00, G06F 17/00. Способ мониторинга безопасности автоматизированных систем : № 2007105319/09 : заявл. 12.02.2007 : опубл. 10.05.2009 / А. С. Евстигнеев, К. М. Зорин, М. А. Карпов [и др.] ; заявитель ВОЕННАЯ АКАДЕМИЯ СВЯЗИ имени С.М. Буденного.

9. Патент № 2696330 C1 Российская Федерация, МПК G06F 21/50, G06F 21/60, H04L 9/00. Способ защиты вычислительных сетей : № 2018128075 : заявл. 31.07.2018 : опубл. 01.08.2019 / В. В. Барабанов, А. А. Ефремов, Р. В. Максимов [и др.] ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище имени генерала армии С.М. Штеменко" Министерство обороны Российской Федерации.

10. Патент № 2649789 C1 Российская Федерация, МПК H04L 12/801, H04L 29/06, H04L 9/32. Способ защиты вычислительных сетей : № 2017125677 : заявл. 17.07.2017 : опубл. 04.04.2018 / Р. В. Максимов, Д. Н. Орехов, И. С. Проскуряков, С. П. Соколовский ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище имени генерала армии С.М. Штеменко" Министерства обороны Российской Федерации.

11. Результаты анализа способов компрометации средств защиты информации / А. Л. Гаврилов, С. Л. Катунцев, Д. Н. Орехов, С. П. Соколовский // Технические и технологические системы: Материалы девятой Международной научной конференции «ТТС-17», Краснодар, 22–24 ноября 2017 года / Кубанский государственный технологический университет, Краснодарское высшее военное авиационное училище летчиков имени А.К. Серова; под общей редакцией Б.Х. Гайтова. – Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг", 2017. – С. 117-121.

12. Соколовский, С. П. Применение адаптивных нечетких систем в вопросах разработки средств выявления несанкционированных воздействий на информацию / С. П. Соколовский, Н. А. Усов // Информатика: проблемы, методология, технологии : материалы XVI Международной научно-методической конференции, Воронеж, 11–12

февраля 2016 года / Под редакцией Тюкачева Н.А.. – Воронеж: Научно-исследовательские публикации, 2016. – С. 259-264.

13. Катунцев, С. Л. Моделирование способа обфускации идентификаторов сетевых устройств в интересах минимизации компрометирующих признаков средств проактивной защиты вычислительных сетей / С. Л. Катунцев, Д. Н. Орехов, С. П. Соколовский // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2018. – № 3. – С. 239-248.

14. Иванов, И. И. Этюды технологии маскирования функционально-логической структуры информационных систем / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 11–12 октября 2017 года. – Санкт-Петербург: федеральное государственное казенное военное образовательное учреждение высшего образования "военная академия связи имени маршала советского союза с. м. Буденного" министерства обороны Российской Федерации, 2017. – С. 147-154.

15. Душкин, А. В. Особенности оценки времени противодействия несанкционированным воздействиям на информационные телекоммуникационные системы / А. В. Душкин, М. Ю. Петшауэр, С. П. Соколовский // Информация и безопасность. – 2009. – Т. 12. – № 2. – С. 305-308.

16. Иванов, И. И. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 11–12 октября 2017 года. – Санкт-Петербург: федеральное государственное казенное военное образовательное учреждение высшего образования "военная академия связи имени маршала советского союза с. м. Буденного" министерства обороны Российской Федерации, 2017. – С. 138-147.