Система обнаружения несанкционированных воздействий на систему доменных имен

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

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

Аннотация. *В то время как доменные имена используются авторизованными пользователями, несанкционированные DNS-серверы осуществляют вредоносную деятельность, используя вредоносные программы и вирусы, получают доступ к конфиденциальным данным пользователей. Разработана система, которая помогает операторам выявлять использование несанкционированных DNS-серверов в своих сетях. Она работает путем пассивного анализа DNS-трафика и не требует активного зондирования сторонних серверов. С помощью данной системы обнаруживаются серверы, управляющие ответами, которые влияют на непопулярные домены. Среди них выделяются как законные сервисы, которые предлагают дополнительную защиту клиентам, так и сервисы под контролем вредоносных программ, которые управляют трафиком с вероятными вредоносными целями.*

Ключевые слова: *DNS, авторизованный пользователь, несанкционированный DNS-сервер, система доменных имен.*

Введение

DNS имеет основополагающее значение для интернета, поскольку он преобразует доменные имена в IP-адреса. Операторы обычно развертывают рекурсивные DNS-серверы для обработки запросов, близких к их пользователям [1]. Однако часто встречаются пользователи, которые намеренно выбирают открытые рекурсивные серверы или непреднамеренно полагаются на произвольные серверы. Последнее может произойти, например, когда программное обеспечение, установленное на компьютерах пользователей, автоматически изменяет конфигурацию DNS [2]. Рекурсивные DNS-серверы будут отвечать на запросы пользователей, обращаясь к авторизованному серверу для доменного имени. Другими словами, некоторые рекурсивные серверы иногда отвечают на запросы с ответами, которые отличаются от того, что возвращается от авторизованных пользователей [3-5]. Такие изменения могут

происходить как по законным причинам, так и из-за вредоносных программ и вирусов, изменяющих настройки DNS клиентов.

Соответственно, идентификация несанкционированных серверов на основе пассивного наблюдения за движением сопряжена со многими проблемами [6]. Во-первых, методы балансировки нагрузки DNS обычно используются сетями доставки контента, поэтому ответы могут сильно различаться, например, изменяться с течением времени и в зависимости от географического положения клиента и сервера.

Во-вторых, вредоносные серверы могут возвращать совершенно законные ответы на подавляющее большинство запросов, изменяя при этом лишь небольшое подмножество запросов, например, для очень специфических доменных имен. Система оценивает согласованность ответов всех серверов, извлекая функции непосредственно из DNS-трафика. Эти функции включают количество и тип записей в ответах DNS, типичные значения полей времени жизни (TTL) возвращаемых IP-адресов. Данная система способна выявлять вредоносные серверы, которые лишь эпизодически манипулируют ответами, чтобы заставить пользователей проходить через поддельные серверы, вероятно, находящиеся под контролем злоумышленников.

Основной целью данного исследования является определение основных проблем преобразования доменных имен в IP-адреса в области несанкционированного воздействия на их преобразования и разработка алгоритма защиты, обеспечивающего минимизацию рисков случайных и преднамеренных изменений.

Исходя из поставленной цели, были сформулированы следующие задачи исследования:

- определить сущность понятия протокола DNS и алгоритма преобразования его в IP-адрес;
- разработать алгоритм защиты процессов преобразования доменных имен в IP-адреса, доступный для технологической реализации и внедрения.

1. Разработка моделей

DNS - это крупномасштабная система, состоящая из миллионов серверов, которые взаимодействуют для разрешения запросов пользователей, реализуемая на основе соответствующего стандарта [7]. Несмотря на то, что существующая концепция реализации данной системы взаимодействия регламентирована и активно совершенствуется в области её защиты, на сегодняшний день существует ряд уязвимостей, которые становятся причиной развития кибер-мошенничества и нарушения конфиденциальности пользователя [8]. На рис. 1 показан случай, где зараженный клиент связывается с вредоносным DNS-

сервером и запрашивает конфиденциальное доменное имя (например, site.ru), но получает в качестве ответа IP-адрес поддельного веб-сервера.

Клиентам не предоставляются средства для проверки подлинности и целостности ответа и, таким образом, они подвергаются воздействию вредоносных мошеннических DNS-серверов. Именно поэтому исследование аномалий DNS является острым дискуссионным вопросом. В некоторых работах предлагаются общие методы выявления аномалий в DNS [9], например, отравление кэша DNS. Здесь возникает вопрос о том, могут ли изменения DNS быть обнаружены непосредственно из DNS-трафика [10, 11]. Это позволило бы сетевым операторам идентифицировать клиентов, подверженных изменениям, без необходимости периодически проверять внешние хосты на наличие подозрительных DNS.

Таким образом, средство защиты представляет собой систему, помогающую операторам идентифицировать использование несанкционированных DNS-серверов в своих сетях [12, 13].

Система защиты направлена на поиск измененных DNS-ответов, в том числе предоставленных мошенническими серверами, которые перенаправляют трафик на определенные вредоносные серверы. Она обрабатывает пакеты DNS-трафика из сети и выдает подробную информацию об аномалиях DNS [14, 15].

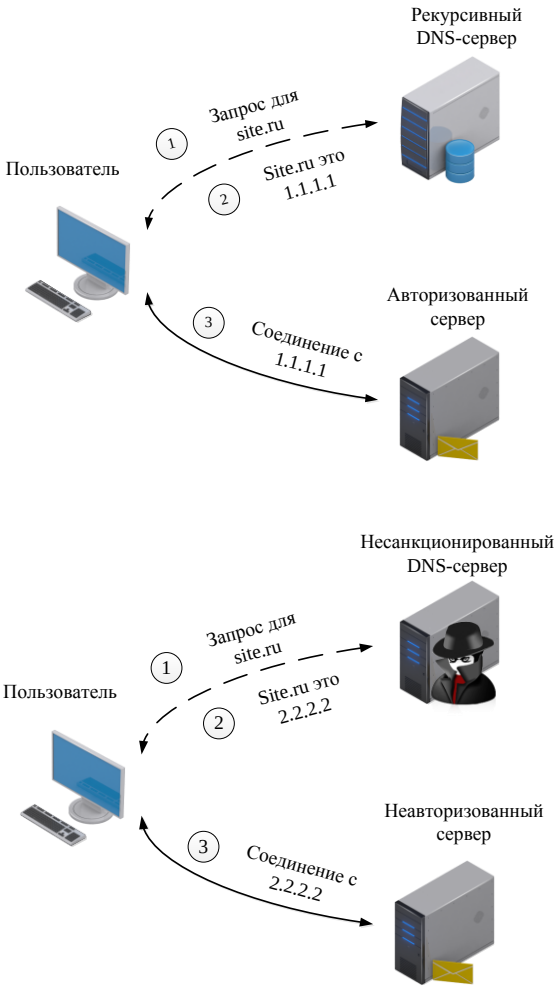

Рис. 1. Управление DNS с помощью поддельных ответов DNS

Учитывая все вышесказанное, на рис. 2 изображена предлагаемая блок-схема алгоритма функционирования системы защиты, которая включает в себя следующую последовательность действий.

Предварительно задаются исходные данные – имена DNS серверов (зона), которые будут подвергаться анализу (блок 1). Зона – часть дерева доменных имен, размещаемая как единое целое на некотором сервере доменных имен, а чаще одновременно на нескольких серверах. Целью

выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации.

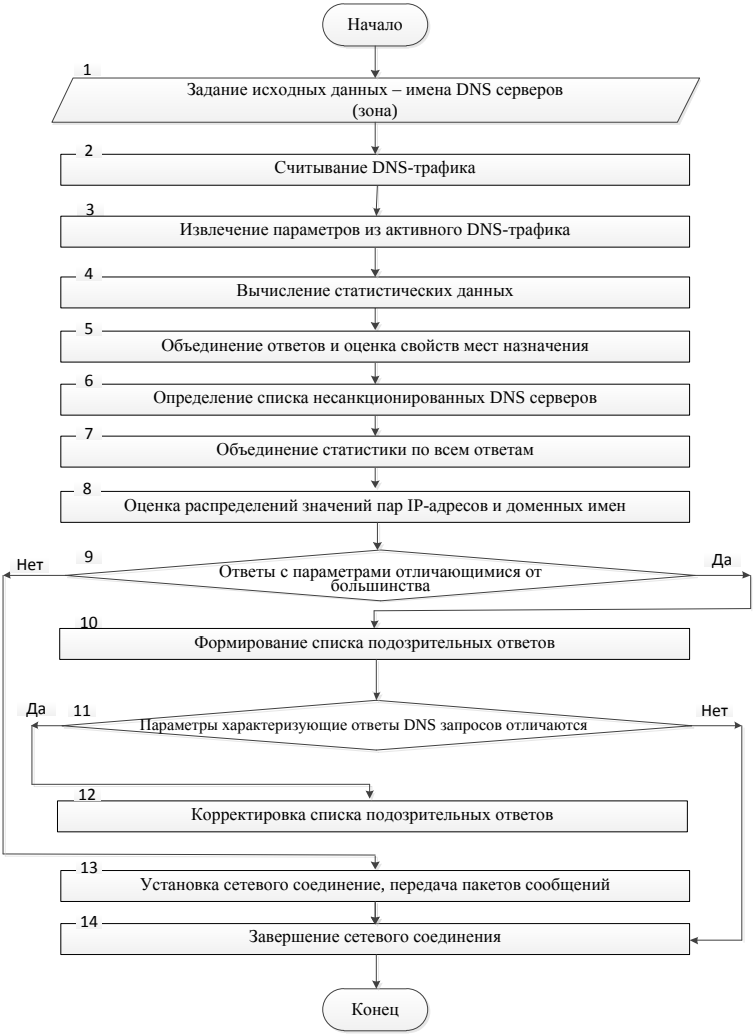

Рис. 2. Блок-схема алгоритма функционирования системы защиты

Далее осуществляется считывание параметров DNS-трафика (блок 2) и извлечение параметров из активного DNS-трафика, пассивно наблюдаемого в сети (блок 3).

На следующем этапе происходит агрегация ответов по каждому домену и вычисление статистических данных о разрешениях пар доменных имен и IP-адресов и обнаружение аномалий на основе статистики, а также выявление необычных разрешения DNS, которые помечены как подозрительные (блок 4).

Затем происходит отфильтровывание ложных срабатываний, объединение ответов, и, таким образом, происходит оценка адреса назначения, куда направляются пользователи при разрешении доменов (блок 5).

После чего, разрешения, помеченные как аномальные, используются для определения окончательного списка несанкционированных DNS-серверов, и результаты представляются вместе со статистикой, объясняющей источник аномалий (блок 6). Производится объединение статистики по всем ответам, относящимся к каждому домену (блок 7). Далее оцениваются распределения значений для каждой пары IP-адреса и доменного имени (блок 8).

На следующем этапе производится консолидация статистики для каждого запрашиваемого домена. Для этого объединение всех ответов, соответствующих каждому домену. Серверы, которые дадут ответы с параметрами, отличающимися от большинства заслуживают оценки на предмет возможных изменений (блок 9).

Затем формируется список подозрительных ответов (блок 10). К сожалению, прямое сравнение неэффективно, так как количество образцов может быть очень низким для непопулярных серверов. Таким образом, непопулярные серверы часто будут помечены как подозрительные.

IP-адреса и доменные имена, помеченные как подозрительные, включают в себя изменения, но также и ложные срабатывания. Это ожидается, поскольку на предыдущем этапе считаются подозрительными все резолюции, расходящиеся с большинством. Однако некоторые пользователи могут предпочесть использовать серверы, расположенные в сетях, которые физически удалены от места, где они подключены. Серверы в разных местах могут вести себя по-разному. Каждый сервер отвечает на запросы, связанные с различными веб-службами, размещенными в различных системах. Если система размещает несколько популярных доменов, ожидается, что параметры, характеризующие ответы, будут отличаться, например, TTL должен варьироваться от ответа к ответу (блок 11).

Несанкционированные DNS-серверы, изменяют это поведение. Например, вредоносное ПО возвращает IP-адреса, на которых размещены серверы злоумышленника для различных доменов. Следовательно, особенности таких реакций не следуют общим закономерностям, т. е. представляют небольшую вариабельность. Система защиты реализует простое правило, доказавшее свою достаточность для фильтрации ложных срабатываний из списка подозрительных пар IP-адресов и доменных имен. Таким образом производится очистка списка подозрительных ответов (блок 12).

После получения отчетов об активности DNS, помечаются несанкционированными DNS-серверами. Система защиты создает отчет для каждого сервера и представляет его аналитику. В отчете содержится краткое описание глобальной активности DNS (например, количество запросов) и подробная информация о функциях, приводящих к пометке определенных серверов. Последнее позволяет аналитику обнаруживать веб-сайты, которыми управляют несанкционированные DNS-серверы. Устанавливается сетевое соединение (блок 13).

После передачи пакетов сообщений сетевое соединение завершается (блок 14).

Заключение

Проведенное моделирование процессов ИС позволяет повысить эффективность функционирования информационной системы образовательного назначения за счет внедрения возможности формирования профессионально-ориентированного образовательного контента для различных направлений подготовки с учётом дифференцированных весовых коэффициентов.

Информационные модели отражают основные входные потоки, выходные данные, задействованные ресурсы и управляющие воздействия. Входными параметрами являются информация о целях и задачах изучения дисциплины, информация об учебно-методическом и материально-техническом обеспечении дисциплины, непосредственно сам образовательный контент и другие данные. Выходными данными являются, индивидуализированные для направления подготовки рабочая программа и УМК, процесс формирования которых выполняется под регламентацией управляющей информации из ФГОС, учебного плана, положения об УМК, и в соответствии с методологией подготовки и способами представления. Исполнителями процессов с использованием информационной системы являются преподаватель и студент.

Литература

1. RFC 1034. Domain Names Concepts and Facilities (DNS). 1987. [Электронный ресурс]: база данных. – URL: https://tools.ietf.org/html/rfc1034 (дата обращения: 19.11.2021).

2. Олифер, В. Компьютерные Сети. Принципы, технологии, протоколы: / В. Олифер, Н. Олифер : учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.

3. Гаврилов А.Л. 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.

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. RFC 1035. Domain names implementation and specification (DNS). 1987. [Электронный ресурс]: база данных. – URL: https://tools.ietf.org/html/rfc1035 (дата обращения: 19.11.2021).

8. 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.

9. Информационная безопасность [Электронный ресурс]: база данных. – URL: http/wiki.merionet.ru/servernye-resheniya. (дата обращения: 19.11.2021).

10. Душкин, А. В. Способ распознавания вредоносных воздействий на информационную систему / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Телекоммуникации. – 2011. – № 10. – С. 25-28.

11. Патент № 2408928 C1 Российская Федерация, МПК G06F 21/20, H04L 12/28. Способ сравнительной оценки структур информационно-вычислительной сети: № 2009129726/08 : заявл. 03.08.2009 : опубл. 10.01.2011 / П. А. Берест, К. Г. Богачев, Л. С. Выговский [и др.] ; заявитель Государственное образовательное учреждение высшего профессионального образования "Военная академия связи имени С.М. Буденного" Министерства обороны Российской Федерации.

12. Патент № 2408928 C1 Российская Федерация, МПК G06F 21/20, H04L 12/28. Способ сравнительной оценки структур информационно-вычислительной сети : № 2009129726/08 : заявл. 03.08.2009 : опубл. 10.01.2011 / П. А. Берест, К. Г. Богачев, Л. С. Выговский [и др.] ; заявитель Государственное образовательное учреждение высшего профессионального образования "Военная академия связи имени С.М. Буденного" Министерства обороны Российской Федерации.

13. Соколовский, С. П. Модель конфликта в информационной сфере / С. П. Соколовский, С. Р. Шарифуллин, Е. С. Маленков // VIII Международная научно-практическая конференция молодых ученых, посвященная 57-ой годовщине полета Ю.А. Гагарина в космос: Сборник научных статей, Краснодар, 12–13 апреля 2018 года / КВВАУЛ им. А.К. Серова. – Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг", 2018. – С. 299-304.

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. 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.