из расчетов ячейки о значением выше 14,4, значение сетки воды распределим из ячейки (x_1, y_0) к ячейкам, состояние которых будет ближайшим к среднему. Проведя повторный расчет, исключая ячейки, состояние которых в сетке дороги более 14,4, получим среднее значение, равное 12. Следовательно, ячейки с состоянием в сетке дороги, равным 14, также исключаются из расчетов. На ячейки с состоянием, близким к среднему, распределим воду из предыдущих ячеек. Проведя следующие расчеты, исключив ячейки, которые в сетке дороги имеют состояние более 12, получим среднее значение, равное 11, тем самым исключив ячейки с состоянием в сетке дороги, равным 12.

После повторных расчетов ячеек, состояние которых в сетке дороги не более 11, получим среднее значение, равное 10,3. Среднее значение не менее максимального состояния ячейки расчетной сетки дорог, следовательно, уровень воды в ячейках, состояние которых в сетке дорог меньше среднего значения, будет равен 10,3 и данный результат является конечным для представленной модели.

Для того чтобы определить лучшую ячейку расположения ливневого слива, необходимо уменьшить общее количество воды. Уменьшив общее количество воды до значения 1, получим, что вода будет находиться строго в ячейке (x_4 ,y_4), что и является лучшим расположением для данной сетки дороги.

Список цитированных источников

1. Петров, Д.О. Система расчета и визуализация зоны затопления на основе клеточного автомата / Д.О. Петров, А.А. Волчек, Д.А. Костюк, Н.Н. Шешко // Актуальные проблемы наук о Земле: использование природных ресурсов и сохранение окружающей среды: сб. материалов Междунар. науч.-практ. конф., посвящ. году науки в Респ. Беларусь: в 2 ч., Брест, 25 – 27 сент. 2017 г. – Брест: БрГУ, 2017. – Ч. 1. – С. 145–148.

2. Liu L. et al. Developing an effective 2-D urban flood inundation model for city emergency management based on cellular automata // Natural Hazards and Earth System Sciences. – 2014. – No, 2 (3). – P. 6173–6199.

3. Азизов, Н.Ю. Использование клеточного автомата в качестве метода прогнозирования развития динамических природных явлений по данным спутниковой съемки // Международный студенческий научный вестник. – 2016. – No 2. – С. 134–136.

УДК 004.056.57

ФИЛЬТРАЦИЯ DNS ЗАПРОСОВ С ПОМОЩЬЮ ДИНАМИЧЕСКИХ ЗОН С ПОЛИТИКОЙ ОТВЕТОВ В ОТКРЫТЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Бубнов Я. В.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь

Научный руководитель: Иванов Н. Н. канд. физ.-мат. наук, доцент

Узлы компьютерных сетей постоянно подвергаются атакам, направленным на завладение или компрометацию ресурсов атакуемого устройства. Частными примерами подобных угроз являются вредоносные программы BernardPOS и FrameworkPOS, предназначенные для кражи информации о кредитных картах с платежных систем. Обе эти программы объединяет аналогичный подход к передаче захваченной информации уда-

ленному управляющему узлу. Передача осуществляется путем ее инкапсуляции в пакеты протокола DNS так называемым DNS туннелированием. Пример доменного имени используемого при DNS туннелировании:

```
zhmyaA-Aaahhh-Drink-mal-ein-Jgermeister-.hidemyself.org.
```

Методы обнаружения DNS-туннелирования в компьютерных сетях предложены в нескольких работах [1, 2]. Однако остается открытым вопрос распространения политики принятого решения по распределенной системе DNS-серверов.

Основным способом противодействия угрозам, исходящим с вредоносных доменов, является использование зон с политикой ответов (RPZ). Данный подход предложен консорциумом ISC и подразумевает создание зоны со списком доменов, которые подлежат блокировке. Пример такой зоны:

```
$ORIGIN RPZ.EXAMPLE.ORG
*.hidemyself.org    CNAME    .    ; return NXDOMAIN
```

Основная проблема данного подхода в контексте блокирования DNS туннелирования заключается в принципиальной невозможности превентивного создания подобной зоны. Причина связана с динамическим характером доменных имен, используемых при DNS туннелировании. Другими словами, DNS-домены для туннелирования могут создаваться быстрее, чем файл зон будет успевать синхронизироваться с, например, открытой базой вредоносных доменов. Решение данной проблемы может быть осуществлено двумя способами.

Первый способ требует установку промежуточного кеширующего DNS-клиента, в который интегрирован один из известных детекторов DNS-туннелей. Каждый запрос клиента на разрешение DNS-имени должен быть проанализирован детектором на предмет присутствия DNS-туннеля и только потом может быть продолжен стандартный процесс разрешения доменного имени. Для уменьшения времени обработки запросов может быть использовано кеширование результатов детектирования в виде зон с политикой ответов — динамических RPZ. Преимущество данного подхода состоит в отсутствии необходимости модифицировать существующую DNS-инфраструктуру, а также синхронизировать динамические RPZ с остальными клиентами. Обобщенная схема данного подхода представлена на рисунке 1.

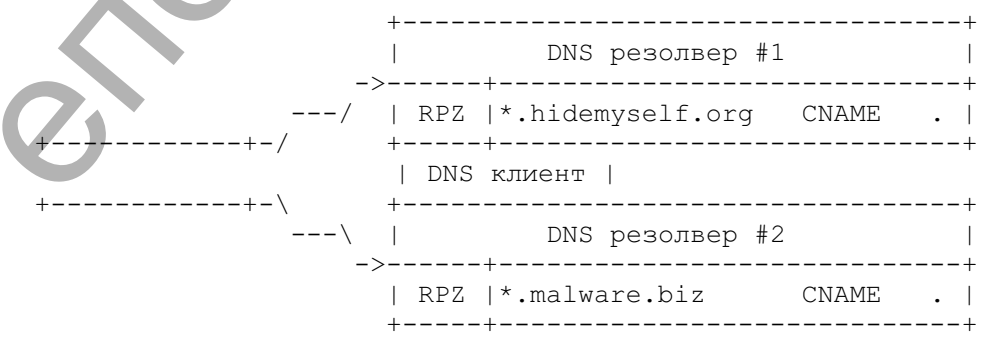

Рисунок 1 — Схема интеграции детектора в DNS-резолверы

По причине того, что ресурсные затраты на развертывание и оперирование детектора DNS-туннелей могут быть значительными, возможен иной способ интеграции. Второй

способ подразумевает интеграцию детектора DNS туннелей в первичный (авторитативный) DNS-сервер. Как и в случае с промежуточным DNS клиентом, сервер должен кэшировать вредоносные домены в динамической RPZ в течение некоторого периода времени. Однако, в отличие от первого подхода, данная динамическая RPZ-зона реплицируется на вторичные DNS-серверы с помощью стандартной схемы передачи зон AFXR. Таким образом, ресурсно-затратный детектор может быть развернут исключительно на авторитативном сервере. Схема данного подхода представлена на рисунке 2.

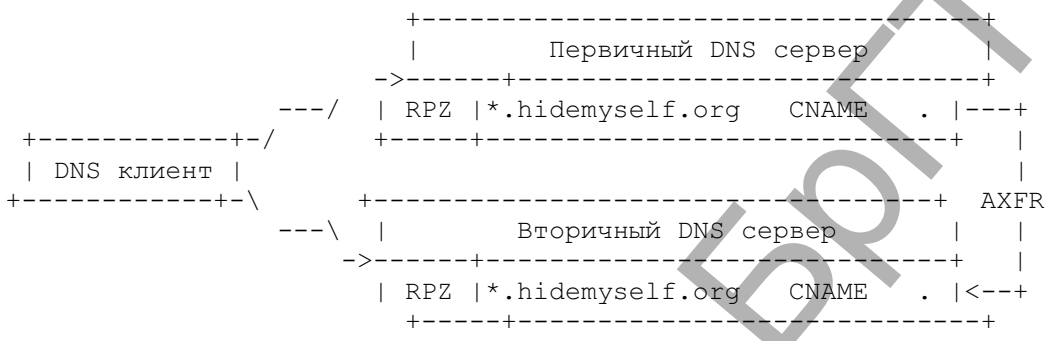

Рисунок 2 — Схема интеграции детектора в первичный DNS-сервер

В качестве дополнительной оптимизации размера зоны с политикой ответов вместо полного доменного имени предлагается сохранение подстановочной маски с доменом максимум второго уровня.

Два предложенных метода характеризуются широкими возможностями горизонтального масштабирования системы детектирования DNS-туннелирования в существующую инфраструктуру системы доменных имен. Благодаря дублированию DNS-резолверов в первом способе и наличию реплицированных вредоносных доменов на вторичных серверах во втором способе обеспечиваются гарантии высокой доступности системы в случае интеграции детекторов.

Список цитированных источников

1. Bubnov, Y. DNS Tunneling Detection Using Feedforward Neural Network / Y. Bubnov // European Journal of Engineering Research & Science. – 2018. – Vol. 3, № 11. – P. 16-19.

2. Nadler, A. Detection of Malicious and Low Throughput Data Exfiltration Over the DNS protocol / A. Nadler, A. Aminov, A. Shabtai – Negev : Ben Gurion University of the Negev, 2017.

УДК 004.65

ОТХОД ОТ РЕЛЯЦИОННОЙ МОДЕЛИ В СОВРЕМЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Дубицкий А. В., Матюшин Б. Н., Маркина А. А.
Брестский государственный технический университет, г. Брест, Беларусь
Научный руководитель: Костюк Д. А., канд. техн. наук, доцент

В последние годы наблюдается возвращение интереса к нереляционным системам управления базами данных. До нынешнего роста активное использование нереляционных хранилищ наблюдалось во времена мэйнфреймов, после чего в период доминиро-