Анализ блогов, форумов, социальных сетей

с целью выявления в режиме реального времени источников информационных атак*

Т.В. ИГНАТОВА, В.А. ИВИЧЕВ, Ф.Ф. ХУСНОЯРОВ, ООО «Медиалогия», Москва. E-mail: tignatova@mlg.ru, vivichev@mlg.ru, fh@mlg.ru

Современный Интернет невозможно представить без социальных медиа. Государственные деятели, коммерческие, государственные, общественные организации, оппозиция, граждане используют их как грандиозную трибуну. К сожалению, эта трибуна может быть использована для распространения дезинформации, а то и враждебной пропаганды в огромных масштабах. В этой статье мы показываем, насколько уязвимыми являются социальные медиа для проникновения в них ботнетов с целью проведения информационных атак.
Ключевые слова: социальные медиа, ботнет, информационная атака, информационная система

Социальные медиа[1], к числу которых относятся, например, Facebook и Twitter, значительно превосходят традиционные способы общения людей как по объему, так и качеству коммуникаций. Наряду с миллионами пользователей, активно использующих платформы социальных медиа для прямых коммуникаций, они также привлекают пользователей другого типа, которые эксплуатируют социальные медиа в качестве эффективных средств для достижения влияния на большую и разнообразную web-аудиторию. Например, в США в 2008 г. во время президентских выборов социальные медиа широко использовались командой Обамы[2]. Существует мнение, что социальные медиа в качестве коммуникационных платформ демократии явились ключевой особенностью весенних арабских революций на Ближнем Востоке[3]. Таким образом, глобальная интеграция социальных медиа в повседневную жизнь стала объективной реальностью.

---

* Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации. УДК 004.031.42.

[1] Web-платформы, обеспечивающие социальную деятельность пользователей. Пользователь социальной медиа владеет учетной записью, описывающий его социальные атрибуты, такие как имя, пол, интересы и контактную информацию.

[2] *Vargas J.A.* Obama raised half a billion online. URL: http://voices.washingtonpost.com/44/2008/11/obama-raised-half-a-billion-on.html, November 2008.

[3] *Salem F.* and *Mourtada R.* Civil movements: The impact of Facebook and Twitter // The Arab Social Media Report. – 2011. – 1(2).



Наряду с контентом, создаваемым в социальных медиа человеком, появилось новое поколение компьютерных программ, называемых ботнетами и используемых для широкомасштабного влияния на пользователей социальных медиа[4].

Ботнет – это программное обеспечение, которое управляет учетными записями в конкретной социальной сети и может выполнять основные виды деятельности пользователя. Главным отличием ботнета от других компьютерных программ в социальных медиа (например, Twitter-ботов, которые размещают прогноз погоды) является то, что он способен выдавать себя за человека.

Например, создание учетной записи пользователя в социальной медиа включает в себя три задачи: предоставление реального e-mail адреса, создание профиля пользователя, активация учетной записи. При этом один человек (или организация) может иметь несколько учетных записей пользователя с использованием различных e-mail адресов. Очевидно, что эти задачи можно полностью автоматизировать. Это позволяет ботнету проникнуть в конкретную социальную медиа для оказания влияния на аудиторию, в частности, распространять дезинформацию и пропаганду в целях формирования или изменения общественного мнения. Пример – использование Twitter-ботов для запуска клеветнических кампаний и формирования искусственного общественного мнения в США в 2010 г. на промежуточных выборах[5].

Актуальность проблемы выявления ботнетов и информационных атак, организованных посредством их использования

Поскольку ботнет похож на реального человека с учетной записью какой-либо социальной сети, он может отправлять сообщения, может отвечать или не отвечать на сообщения, повторно отправлять, пересылать их и т.п.

---

[4] *Misener D.* Rise of the socialbots: They could be inuencing you online. URL: http://www.cbc.ca/news/technology/story/2011/03/29/f–vp–misener–socialbot–armies–election.html, March 2011.

[5] *Ratkiewicz J., Conover M., Meiss M., Gon_calves B., Patil S., Flammini A.* and *Menczer F.* Truthy: mapping the spread of astroturf in microblog streams. In Proceedings of the 20th international conference companion on World wide web, WWW'11. P. 249{252, New York, USA, 2011. ACM.

Таким образом, возможно возникновение сотен и тысяч автономных ботнетов, каждый из которых запрограммирован для проникновения в социальные медиа и формирования путем информационных атак различных политических, экономических, религиозных, коммерческих, культурных и иных убеждений и мнений, тем более что с технической точки зрения программное обеспечение, необходимое для запуска информационных атак ботнетов, доступно даже с открытым исходным кодом и имеется в свободной продаже по низким ценам.

Такие социальные медиа, как Twitter и Facebook, часто используются в качестве барометра общественного мнения. Возникают серьезные опасения, что точность измерения общественного мнения, когда известно, что какая-то часть измеряемой аудитории является просто компьютерными программами, крайне недостоверна. В России уже зафиксированы многочисленные случаи применения ботнетов для формирования общественного мнения в социальных медиа.

Из вышесказанного однозначно следует, что последствия использования ботнетов в противостоянии сторон в социальных медиа могут быть очень тяжелыми.

В последнее время предлагается множество методов для автоматического выявления ботов в социальных медиа в зависимости от их ненормального поведения[6].

Например, в США в 2011 г. была представлена Facebook Immune System (FIS), которая в режиме реального времени выполняет проверку и классификацию каждого действия чтения и записи в базе данных Facebook, для защиты своих пользователей и социальных групп от вредоносной деятельности. В то же время FIS трудно представить в качестве защиты против ботнетов, которые имитируют реальных пользователей[7]. Задача, решение которой описывается в данной статье, значительно сложнее, так как требует создания технологий и информационной системы анализа социальных медиа и других интернет-ресурсов для выявления ботнетов, имитирующих реальных пользователей.

---

[6] *Stringhini G., Kruegel C.* and *Vigna G.* Detecting spammers on social networks. In Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC '10, pages 1(9), New York, USA, 2010. ACM.

[7] *Stein T., Chen E.* and *Mangla K.* Facebook immune system. In Proceedings of the 4th Workshop on Social Network Systems, SNS '11. P. 8:1(8:8), New York, USA, 2011. ACM.

Анализ мониторинга социальных медиа для выявления информационных атак, проводимых ботнетами

Создаваемая система, в частности, позволяет:

• выявлять в сети Интернет ботнеты, используемые для организации информационных атак (виртуальные блоги и микроблоги, автоматически наполняемые форумы, виртуальные учетные записи в социальных сетях);

• определять в режиме реального времени информационные атаки, организованные с помощью ботнетов;

• прогнозировать вероятные направления информационных атак на основе анализа статистики информационных вбросов.

Предлагаемый подход к анализу социальных медиа для исследуемых объектов базируется на выделении в информационном сообщении социальных медиа объектов мониторинга, анализа источника информационного сообщения (наименования ботнета и его друзей) и определении информационной окраски сообщения (негативная или позитивная).

Квалификация потока сообщений социальных медиа как информационной атаки основывается на определении превышения пороговых значений количества негативных сообщений.

Результатами анализа потока сообщений социальных медиа являются данные об информационных атаках на объекты мониторинга (атакуемые объекты) с указанием перечней информационных поводов и источников атак (ботнетов).

Для каждой информационной атаки определяются следующие сведения.

• Период проведения. Начало атаки фиксируется при превышении порога количества сообщений на атакуемые объекты мониторинга, окончание атаки – при снижении количества сообщений ниже порога.

• Перечень атакованных объектов мониторинга.

• Сила атаки – значение, вычисляемое на основании суммарной вредоносности источников атаки и значимости атакуемого объекта.

• Информация о поводах информационной атаки: наименование повода, которое отражает краткое описание события,

упоминаемого в сообщениях атаки; перечень ботнетов (источников), публиковавших сообщения по данному информационному поводу и общее количество опубликованных сообщений.

• Информация об источниках (ботнетах, опубликовавших сообщения атаки): URL-адрес источника, перечень атакованных информационных объектов, коэффициент вредоносности источника, вычисленный на основе накопленных статистических данных с учетом количества опубликованных сообщений, количество и заметность атакованных (упоминаемых) объектов.

В системе формируется информация о динамике жизненного цикла ботнета: об изменении коэффициента вредоносности источника, количества атакуемых объектов и числа публикуемых сообщений.

Перспективы создаваемой системы

Создаваемая система на этапе экспериментальной проверки позволила обработать 10 млн записей из десяти социальных медиа и на основе их анализа выявить 3112 ботнетов, которые произвели 221 информационную атаку на 770 атакуемых объектов. Суммарная мощность информационных атак составила около 200 тыс. сообщений. К перспективным направлениям использования системы относится выявление ботнетов, предназначенных для сбора частных данных пользователей, таких как адреса электронной почты, номера телефонов и других личных данных. Эти данные являются ценными и могут быть использованы для кампаний интернет-профилирования, крупных спам-рассылок и фишинга[8]. Еще одно перспективное направление – создание средств защиты от проникновения ботнетов в социальные медиа.

[9] Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.