Л. А. ВИТКОВА
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
Санкт-Петербург

ОЦЕНКА УГРОЗ В СОЦИАЛЬНЫХ СЕТЯХ ПРИ ИСПОЛЬЗОВАНИИ БОТОВ

Объектом угроз в социальных сетях являются как пользователи, так и организации или общество в целом. При этом пользователи социальных сетей по добровольному согласию с условиями использования социальной сети раскрывают личные данные о себе, такие как статус отношений, дата рождения, школа, адрес электронной почты, номер телефона или геопозиция. Когда такая информация попадает в руки злоумышленника, она используется для нанесения вреда пользователям. В статье предложена систематизация и оценка угроз в социальных сетях, реализованных при использовании ботов.

Введение. Социальная сеть – это информационная система, позволяющая зарегистрированным пользователями размещать информацию о себе, делиться медиа файлами, текстами и устанавливать социальные связи с другими пользователями [1]. Популярность социальной сети напрямую зависит от количества пользователей. Поэтому главной задачей является привлечение как можно большего числа людей за счет дизайна, удобства, функциональности. При этом вопросы безопасности и конфиденциальности уходят на второй план, что приводит к возникновению ряда информационных угроз. Объектом угроз могут выступать как пользователи и организации, так и общество в целом. В соответствии с условиями эксплуатации информационной системы пользователь раскрывает данные о себе. При заполнении профиля по желанию может быть предоставлена дополнительная информация о месте проживания, работе, образовании, религии, интересах и пр. В руках злоумышленника эти сведения могут быть использованы для нанесения ущерба. Известно множество инструментов реализации угроз в социальных сетях, однако в последнее время наиболее популярным способом является использование фейковых аккаунтов или ботов. Бот в классическом понимании термина – это программа, созданная для выполнения однотипных повторяющихся задач в автоматическом режиме. В социальных сетях также используются боты, ключевой особенностью которых является имитация поведения живого пользователя. Данный тип бота называется социальным и активно используется злоумышленниками для совершения мошеннических действий, дезинформации, манипуляций, социальной инженерии [2]. Именно сходство с настоящим аккаунтом позволяет войти в доверие к пользователю. В статье рассматриваются различные угрозы, предложена их классификация и систематизация, а также подход к их оценке.

Угрозы в социальных сетях при использовании ботов. Угрозы в социальных сетях при использовании ботов могут быть разделены по классам [3] и связаны с категориями ботов и сценариями их создания.

Классификация угроз:

1. *Классические угрозы:*
   a. конфиденциальность, объект – пользователь, то есть данные пользователя; история жизни, переданная пользователем в постах; интересы пользователя; окружения пользователя.
   b. целостность, объект – данные, то есть неизменность данных при их передаче, хранении или отображении.
   c. доступность, объект – аккаунт, то есть доступ к аккаунту, доступ к связям аккаунта.
2. *Современные угрозы:*
   a. кликджекинг, объект – сервис в сети Интернет. Существуют программные реализации ботов для кликджекинга, при помощи которых бронируются отели, билеты, что приводит к недоступности коммерческого объекта для реальных пользователей.
   b. фейковый профиль;
   c. клонирование профиля.
3. *Совмещенные угрозы:*
   a. манипуляция общественным мнением;
   b. дезинформация.

4. *Таргетированные угрозы*
   a. хейтинг;
   b. буллинг;
   c. блокировка аккаунта;
   d. социальный инжиниринг;
   e. перехват управления аккаунтом.

Классификация сценариев создания бота.

Для оценки угрозы предлагаются следующие сценарии создания бота:

1. *Автоматический*. Данный сценарий подразумевает использование онлайн-сервиса или программы авторегистрации с готовой базой характеристик профиля: ФИО, телефон, электронная почта, медиафайлы. Также возможна аренда «авторег» аккаунта на бирже. Боты, созданные по такому сценарию, чаще всего выполняют функции спама, накрутки статистики и трафика, вброса дезинформации.
2. *Автоматизированный.* Боты по автоматизированному сценарию создаются аналогично первому пункту, но совершенствуются или управляются человеком вручную. При регистрации требуется участие человека для верификации через смс и сохранения информации об аккаунте. Кроме того, возможно ручное заполнение характеристик профиля. Аренда подразумевает покупку верфицированного аккаунта, в том числе взломанного или угнанного, с последующей заменой номера телефона. Такие боты часто используются для выполнения функций дезинформации, манипуляций общественным мнением, троллинга.
3. *Ручной.* Аккаунт создается и управляется вручную. Данный способ самый ресурсозатратный, т. к. помимо заполнения данных профиля, в течение продолжительного времени формируется легенда, добавляются посты, комментарии, формируются социальные связей. Данные боты используются для имитации поведения человека, формирования страницы лидера мнений.

Оценка угроз в социальных сетях при использовании ботов

Для формирования показателя используется следующая формула:

$$S = C + I + A + Robotic + Automated + Manual \quad (1)$$

где S – это рейтинг (анг. Score), C – это угроза конфиденциальности (анг. confidentiality), I – угроза целостности (анг. integrity), A – угроза доступности (анг. availability).

Для оценки угрозы была проведена экспертная оценка. В оценке участвовали эксперты из рекламных агентств, специалисты кафедры PR факультета журналистики университета СПбГУ, специалисты-эксперты международного центра цифровой криминалистики при СПб ФИЦ РАН. Была сформирована таблица. В таблице на основании исследования ботов и сценариев их создания были отмечены плюсом (+) угрозы конфиденциальности, целостности и доступности, и сценарии создания ботов, через которых могут быть угрозы реализованы. Далее были получены значения путем усреднения голосов экспертов. Среднее значение показателей: (1) автоматический сценарий = 5,45; (2) автоматизированный сценарий = 5,18; (3) ручной сценарий = 4,9. (1) угроза конфиденциальности = 7,48; (2) угроза целостности = 7,2; (3) угроза доступности = 6,63.

Таблица

Оценка угроз в социальных сетях при использовании ботов

Угроза	К	Ц	Д	Авто	Автом	Руч.	Рейтинг
Накрутка лайков	-	+	-	+	-	-	1
Дезинформация	+	+	-	+	+	+	6
Спам	-	+	-	+	+	-	1
Сбор данных	+	-	-	+	+	-	1
Блокировка аккаунтов	-	+	+	+	+	-	2
Хейтинг	+	+	-	-	-	+	10
Буллинг	+	+	-	-	-	+	10
Манипуляция общественным мнением	+	+	-	+	+	+	6
Наведенная активность	+	+	-	+	+	+	6
Социальный инжиниринг	+	+	+	-	+	+	10
Перехват управления аккаунтом, угон	+	+	+	+	+	-	5
Клонирование профиля	+	-	+	+	+	-	2
Копирование части профиля	+	+	-	+	+	-	2

Рейтинг угроз позволяет оценить ущерб и сложность реализации тех или иных угроз. Так, например, по мнению экспертов опасными и сложными в реализации являются угрозы: (1) Хейтинг, (2) Буллинг, (3) Социальный инжиниринг.

Заключение. Проблема информационной безопасности в пространстве социальных сетей сегодня является актуальной и не решенной. Финансовая мотивация, недобросовестная конкуренция, дезинформация, манипулирование общественным мнением – это лишь часть предпосылок для роста разнообразия атак и появления новых угроз. Социальная сеть, как информационная система, требует от пользователя предоставления конфиденциальной информации в процессе регистрации. Однако часть «чувствительных данных пользователь сам раскрывает в процессе взаимодействия с публикой, с друзьями и подписчиками. Когда такие данные попадают в руки злоумышленников, то они используется для нанесения вреда. Предложенные классификации, систематизация и оценка угроз, реализованных при использовании ботов позволяют оценить ущерб и сложность реализации угроз в социальных сетях.

Работа выполнена при финансовой поддержке Гранта РНФ № 18-71-10094-П в СПб ФИЦ РАН.

ЛИТЕРАТУРА

1. **Виткова Л.А., Кураева А.М., Проноза А.А., Чечулин А.А.** Анализ методов выявления и оценки страниц лидеров мнений в социальных сетях. *Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019)*: сборник научных статей VIII Международной научно-технической и научно-методической конференции в 4 т. 2019. С. 233-237.
2. **Gavra D., Namyatova K., Vitkova L.** Detection of induced activity in social networks: model and methodology // *Future Internet*. 2021. Т. 13. № 11.
3. **Fire M., Goldschmidt R., Elovici Y.** Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*. 2014. Т. 16. №. 4. С. 2019-2036.
4. **Sahani R., Randhawa S.** Clickjacking**:** Beware of Clicking. *Wireless Personal Communications*. 2021. Т. 121. №. 4. С. 2845-2855.
5. **Desai N., Das M.L.** DeSAN: De-anonymization against Background Knowledge in Social Networks. *2021 12th International Conference on Information and Communication Systems* (ICICS). IEEE, 2021. С. 99-105.

L.A.Vitkova (St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg)

Evaluation of threats in social networks using bots

The object of threats in social networks are users or organizations. At the same time, users of social networks, by voluntary agreement with the terms of use of the social network, disclose personal data about themselves, such as relationship status, date of birth, school, email address, phone number or geolocation. When such information falls into the hands of an attacker, it is used to harm users. The paper proposes the systematization and assessment of threats in social networks implemented using bots.