УДК 338.47

SMS-BOMBER И ЕГО ОПАСНЫЕ АНАЛОГИ В СОЦИАЛЬНЫХ СЕТЯХ: ПРИМЕРЫ И МЕТОДЫ ЗАЩИТЫ

МУСАЕВА ДИАНА НАДИРОВНА
Экономический факультет СНИГУ им. Н. Г. Чернышевского, г. Саратов, Российская Федерация, di.musaeva2018@yandex.ru

Аннотация

В данной научной работе подробно рассмотрены феномены дестабилизации морального и финансового состояния человека с помощью SMS-бомберов, – программ, оправляющих множество SMS-сообщений с различных сервисов на один номер телефона, – и их не менее опасных аналогов в социальных сетях. Актуальность данной темы есть следствие массового распространения данных негативных феноменов, а также личный опыт переживания «спам-атаки» от SMS-бомберов. Факт массового распространения негативных случаев подтвердило и проведенное мною социологическое исследование. Результаты опроса показали, что 41,3% респондентов подвергались SMS-бомбингу, а жертвами различных спам-атак в социальных сетях становились 48,8% респондентов. Целью анализа является изучение прецедентов спам-атак, а также поиск методов эффективной защиты от них. Особое внимание в ходе исследований уделяется аналогам SMS-бомберов в социальных сетях, таких как Telegram, TikTok, Instagram, ВКонтакте (VK), методам воздействия на жертву, а также способам защиты от них. Кроме того, в статье было акцентировано внимание на одной из важнейших причин опасности данных бомберов – ботах, которые призывают подписчиков/пользователей переходить на сайты/каналы, пропагандирующие экстремизм, потенциальный вред здоровью человека, а также на всё то, что запрещено текущим законодательством Российской Федерации. В ходе изучения темы был сделан вывод о том, что SMS-бомбер в целом не является особо опасным видом хакерской атаки, в отличие от его аналогов для социальных сетей, негативные воздействия которых могут привезти вплоть до удаления, блокировки аккаунтов без возможности для восстановления.

Ключевые слова: SMS-бомбер; спам; бомбинг; социальные сети; блогер; боты; экстремизм

Введение

SMS-бомбинг является одним из самых распространённых видов спам-атак по всему миру. 12 апреля 2022 года на меня была реализована спам-атака с помощью sms-бомбинга (смс-бомбинга). Сообщения поступали от различных магазинов и банков, от портала государственных услуг Российской Федерации, от приложения «Telegram» и от других социальных сетей. После проверки истории входов во всех социальных сетях и консультации у программистов выяснилось, что это был sms-бомбинг. Чтобы понять масштабность и актуальность данной проблемы, мною было реализовано социологическое исследование, в котором приняли участие 122 человека разных возрастов и социальных статусов по виду деятельности (см. рис.1).

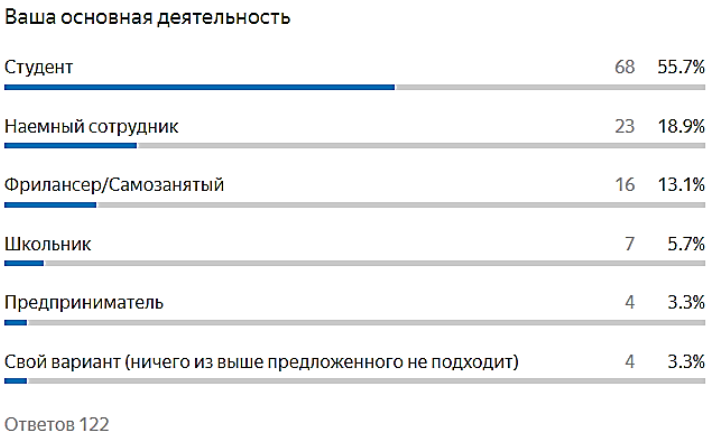

Рис. 1. Социальные статусы по виду деятельности участников исследования [составлено автором на основе исследования]

Опрос показал, что 41,3% респондентов подвергались SMS-бомбингу, из них 30,3% людей становились жертвой больше одного раза, 9,8%- подвергались бомбингу 1 раз, и 2 человека из 122 респондентов постоянно подвергаются SMS-бомбингу (см. рис.2).

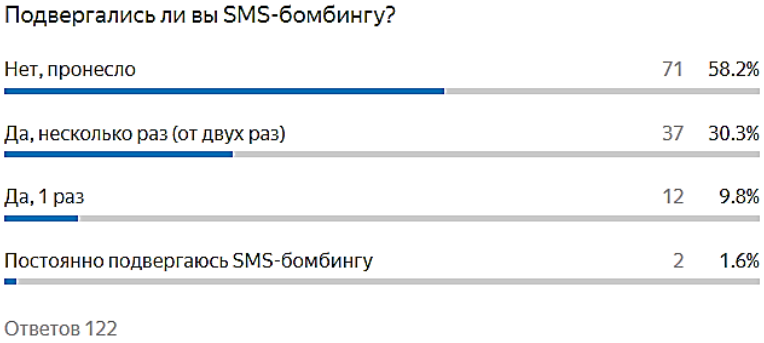

Рис. 2. Результаты опроса [составлено автором на основе исследования]

Данные высокие показатели подтверждают актуальность этой проблемы и необходимость распространения способов защиты от подобных хакерских атак.

Основная часть

1. Понятие SMS -бомбинга, его сущность и методы воздействия на жертву.

SMS-бомбер — это программа или сервис, предназначенный для массовой рассылки сообщений на заданный номер. Фактически это означает, что пользователь неожиданно начинает получать огромное количество входящих сообщений из разных источников. Существует десятки таких программа, и работают они как в обычной вкладке браузера, так и в форме полноценного приложения. А главной причиной популярности таких бомберов является их доступность.

Целями подобной спам-атаки обычно являются розыгрыш или отомстить обидчику. А если изучать примеры опасных аналогов бомберов в социальных сетях, то мотивами их использования могут быть в том числе шантаж в целях наживы или дестабилизации морального и финансового состояния человека.

Жертвой бомбинга может стать каждый, а интенсивность спама зависит от нескольких факторов:

- от мобильного оператора. Например, некоторые операторы могут блокировать подозрительный трафик. Тогда дело может ограничиться всего несколькими сообщениями.

- от качества бомбера. В настоящее время большинство бомберов работают малоэффективно. Однако существуют и весьма качественные платные софты, мощность которых достигает до 10 сообщений в минуту. При этом стоимость такого «розыгрыша» обойдется злоумышленнику очень демократично - примерно от 200 до 1500 рублей.

- от намерений злоумышленника. Одна ситуация, если человек решил таким неприятным образом посмеяться над жертвой; тогда навряд ли он будет издеваться

больше часа. Другая ситуация - если на номер жертвы напал ненавистник или злой конкурент; дело может дойти до смены номера. А в третьей ситуации, если рассматривать социальные сети – то последствия могут быть вплоть до блокировок и вынужденного удаления аккаунтов.

Механизм данных сервисов можно проследить на примере одного из популярных спам-ботов в Telegram (см. рис.3).

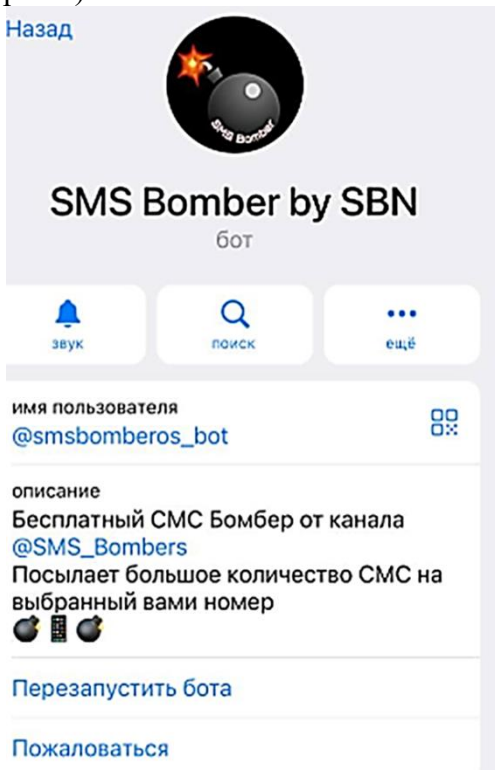

Рис. 3 – пример популярного спам-бота в Telegram

Для бомбинга доступно несколько режимов. Обычно спаминг продолжается от 5 до 40 минут. Самый мощный режим запускает отправку более 1000 сообщений и звонков.

Рассмотрим механизм бомбинга, благодаря которому SMS и звонки приходят от имени официальных компаний и брендов. Разработчики создают определенный скрипт, посредством которого отправляется запрос различным компаниям. Это подобно тому, как если мы попробуем зарегистрироваться, например, на сайте доставки каких-либо товаров. В таком случае после ввода номера телефона нам придет код подтверждения. Таким образом, и в скрипт можно заложить адресацию к огромному количеству сайтов, а также установить определённую цикличность отправления запросов. Стоит заметить, что данный хакерский метод негативно влияет как на жертву, так и на сами компании.

Важно знать, что Telegram-боты используются злоумышленниками не только для того, чтобы спамить или «развлекаться», но и чтобы перехватывать у жертв одноразовые пароли. Примером такого бота является SMSRanger. [3]

С его помощью можно совершать автоматические звонки и отправлять сообщения пользователям, манипулируя и побуждая их прислать одноразовый пароль вместе с другой информацией об учетной записи [1]. В случае успеха злоумышленник может обойти систему проверки банка, захватить учетную запись пользователя и вывести денежные средства.

Рассмотрим несколько эффективных способов, с помощью которых можно безопасно выдержать смс-бомбинг.

Самый простой и эффективный способ - это включение режима «не беспокоить». Данным методом пережить атаку будет проще всего. Этим способом временно заглушаются все уведомления, при этом технически смартфон продолжает их получать. А значит, телефон не получит резкой перегрузки, как в случае с полным отключением

устройства. Следующий шаг: когда атака прекратится, отключить режим «не беспокоить». После этого стоит отметить прочитанными или удалить накопившиеся сообщения, чтобы они не мешали ориентироваться в действительно нужных SMS.

Второй способ – это исключение своего номера с сайтов бомберов. Часто в ответ на атаки SMS-бомберы предлагают услугу «Антиспам». За небольшую стоимость пользователь может добавить свой номер в «белый список» и тем самым миновать назойливую спам-атаку.

Третий способ - это скрыть номер телефона в приложениях, например в Telegram, и со всех сайтов, где профиль человека видят другие пользователи. Данный метод нужен для предостережения спам-атак, так как запустить SMS-бомбинг может любой человек, который увидел ваше объявление на сайтах. Стоит отметить, что этот метод не подойдёт, если атака уже началась. Однако он может защитить от SMS-бомберов в будущем.

2. Опасные аналоги SMS-бомберов в социальных сетях. Примеры атак и методы защиты

Важно отметить, что помимо SMS-бомберов распространены и их аналоги, воздействующие на жертву через социальные сети. Проведенное исследование показало, что 48,8% респондентов подвергались различным спам-атакам в социальных сетях. Из них 3 человека постоянно подвергаются спаму или наплыву ботов, 15,6% участников опроса единожды сталкивались с таким негативным явлением, а 31,1% респондентов становились жертвой спам-атаки или наплыву ботов больше одного раза (см. рис.4).

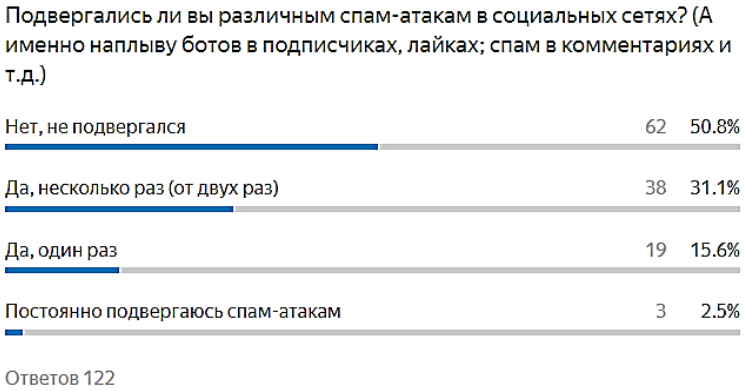

Рис. 4. Результаты опроса [составлено автором на основе исследования]

Рассмотрим аналоги SMS-бомберов в социальных сетях, примеры, методы воздействия на жертву, а также способы защиты.

Для начала стоит уточнить, что всех контент-мейкеров можно обобщить одним словом - «блогеры». Блогеры – это люди, бизнес-страницы, группы, компании, которые создают контент и выкладывают его в социальные сети и платформы.

Аналогом SMS-бомберов в социальных сетях является тандем спама с ботами.

Рассмотрим опасные бомберы в приложении «Telegram».

Существуют программы, в которых покупается пакет ботов, которые подписываются на канал блогера. Они начинают спамить в чате жертвы, если он открыт для всех, или в комментариях под постами. Тем самым рушится статистика канала и снижается вовлеченность подписчиков. Существует и более опасные варианты, когда алгоритм программы заложен в ботах так, что они в скриптах сообщений начинают призывать аудиторию переходить на запрещенные тематические каналы, в которых продаются оружие, наркотики, эротические услуги и т.п., либо распространяется пропаганда экстремизма в разных форматах.

Между тем, наравне с такими бомберами существуют и сервисы, способные изгнать спам из чата. Например, бот «DaySandBox _bot» реагирует на время присутствия юзера/пользователя в беседе (см. рис.5). Далее если человек зашел в чат и провел в нем менее суток, то любые ссылки или сообщения от этого пользователя удаляются.

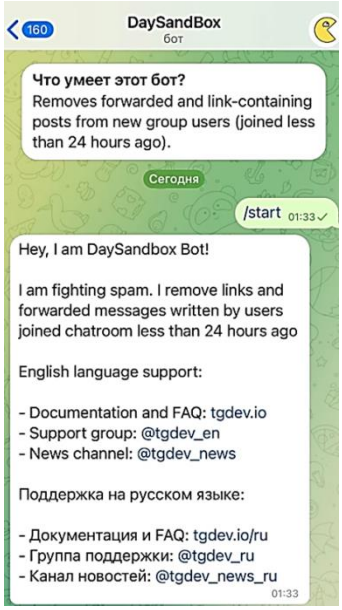

Рис. 5. Бот «DaySandBox_bot» в действии

Другой бот-помощник «SpamKillerRobot» может очистить все нежелательные сообщения, если поступит жалоба от трех человек (см. рис.6). В таком случае блогер может воспользоваться ситуацией и еще больше сплотиться со своей аудиторией, попросив у них помощи в очистке канала от нежелательных спам-ботов.

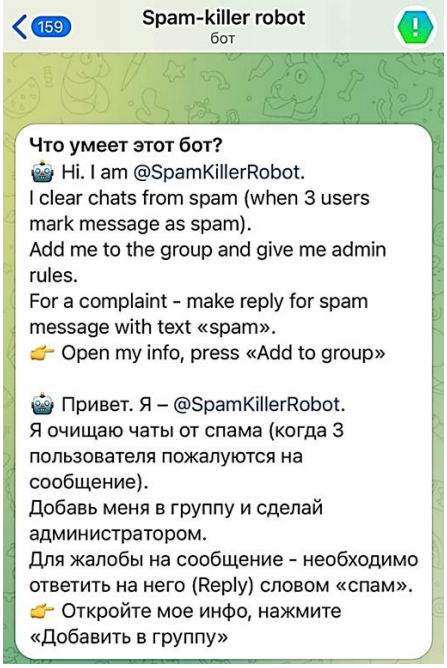

Рис. 6. Бот «SpamKillerRobot» в действии

Далее рассмотрим опасные бомберы, негативно воздействующие на профили блогеров в таких социальных сетях, как «Instagram», «TikTok», «ВКонтакте» («VK»).

Существуют программы, в которых покупается пакет ботов, которые подписываются на аккаунт блогера. Это уже сильно портит статистику по многим показателям. Эффективность блогера для рекламодателей проявляется в том числе и в конверсии просмотров, любой активности, переходов на ссылки и так далее. Балласт спам-страниц в подписчиках наносит блогеру только вред, потому что он не активен. Чем меньший процент активной аудитории у блогера, тем хуже для самого контент-мейкера.

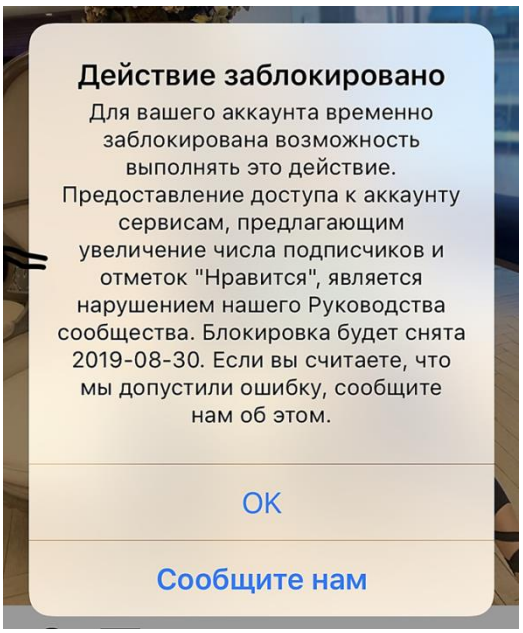

Рис. 7. Пример блокировки действий аккаунта в «Instagram» по причине подозрительной активности [4]

Также нейросеть данной социальной сети начинает подозревать блогера в странной непонятной активности аккаунта, спама и так далее. Стоит напомнить, что обычно на канал/страницу/блог подписываются из видео, или из ссылок, репостов или из запроса в интернете или поисковике социальной сети. В случае спам-атаки часто эти неактивные страницы подписываются из неизвестного источника. Поэтому социальная сеть может заблокировать блогера за злоупотребление программами для накручивания количества аудитории и так далее. А если данные «серые» страницы проводят спам-атаку еще и в комментариях, сообщениях и т.д., то вероятность блокировки данного аккаунта приравнивается к 80-100% в зависимости от эффективности нейросети. Безусловно, аккаунты можно восстановить, убрать все ограничения, но это весьма затруднительный процесс.

Стоит отдельно рассказать об относительно новом, но очень опасном способе бомбинга в социальной сети «TikTok».

Нужно напомнить, что одним из важнейших табу TikTok является распространение спама и опасного трафика. В данном случае имеется в виду перелив в telegram-каналы или другие сайты, в которых распространяется или пропагандируется экстремизм, пропаганда потенциального вреда здоровью человека, продажа оружия, опасных веществ и так далее. Все эти темы находятся под жестким запретом у комитета безопасности TikTok. Такие переливы в контенте и в комментариях алгоритм считывает быстро и, соответственно, быстро удаляет.

Злоумышленники поняли, что если под каким-то роликом идут массовые комментарии на перелив в подобные платформы, или идет пропаганда того, чего запрещено в TikTok, в обществе и в законе РФ, то удаляются не только комментаторы, но и сами ролики. Сегодня можно найти и купить услуги таких опасных бомберов, которые под массовыми фейковыми страницами на абсолютно любом видео будут распространять такие опасные комментарии и переливы. Далее алгоритм социальной сети находит и удаляет ролики. Затем при нарушении трех правил и бана трех видео по причине опасного перелива, аккаунт удаляют навсегда, даже если блогер не виноват. Восстановить аккаунт практически невозможно, поскольку нейросеть считывает эту страницу как площадку для распространения категорически запрещенной информации.

Тот же алгоритм касается прямых эфиров (стримов) в TikTok. Если в комментариях произошла спам-атака на перелив в экстремистские сайты/каналы, модераторы блокируют функцию выхода в стримы на всегда. Если на аккаунте были и другие нарушения, то модерация имеет право удалить аккаунт блогера без возможности восстановления.

Существует несколько вариантов предотвращения опасного бомбинга в TikTok:

1) Ставить фильтр комментариев (помимо слов, оскорбляющих человека, добавить в список такие слова, как «наркотики», «порно», «оружие», «убить», «ice», аналогичные жаргоны, а также слова «заходи», «в телеграме» и т.п).

2) Если происходили единичные случаи опасных комментариев, то нужно удалить данные комментарии, заблокировать пользователя или ограничить его действия. Стоит отметить, что это можно делать без обоснования причин.

3) Можно полностью отключить комментарии на любом видео.

4) Можно перенести видео в приватный режим.

5) Важно сообщать о преследовании самому TikTok, так как функционирует отдельная команда модераторов, которая следит за отсутствием преследования блогеров и т.д.

6) Если произошла обширная атака на множества видео, то нужно временно самостоятельно удалить аккаунт, написать в поддержку, рассказать обо всей ситуации, прислать скрины комментариев. Далее служба поддержки подскажет, что нужно делать. Также блогер может посоветоваться с технической поддержкой, узнать, через какое время стоит восстановить аккаунт.

На сегодняшний день, к сожалению, найти хакера или программу бомбинга, через которую была реализована спам-атака, практически невозможно, поскольку сам спам будет исходить из нейтральных номеров. Вычислить человека, который решил произвести на вас атаку, также практически невозможно, поскольку все улики очень легко скрыть.

Заключение

Подробно изучив тему SMS-бомбинга и спам-атак в социальных сетях, можно сделать выводы:

1. Не стоит бояться SMS-бомберов. В целом они никак не навредят, разве что займут телефон и потреплют жертве нервы. А в социальных сетях стоит заранее предотвратить возможные опасные ситуации с помощью описанных ранее способов, всегда при необходимости обращаться в техническую поддержку, а также постоянно следить за активностью в блоге.

2. Не стоит пользоваться SMS-бомберами и бомберами социальных сетей, так как это плохой и абсолютно неэтичный инструмент в независимости от конечной цели.

Список литературы

[1] Telegram-бот SMSRanger помогает киберпреступникам красть одноразовые пароли. URL: https://news.rambler.ru/internet/47300262-telegram-bot-smsranger-pomogaet-kiberprestupnikam-krast-odnorazovye-paroli/ (дата обращения: 27.04.2022)

[2] Бомберы переключились на микрокражи. Эксперты обнаружили новый способ кибермошенничества. URL: https://www.rbc.ru/newspaper/2021/10/25/6172908a9a79472d4c8e56b9 (дата обращения: 27.04.2022)

[3] Ботом данный: как пользователей заваливают спамом. Сервисы в мессенджерах способны атаковать бесчисленными звонками и перехватить пароль. URL:https://iz.ru/1230817/mariia-nemtceva/botom-dannyi-kak-polzovatelei-zavalivaiut-spamom (дата обращения: 20.04.2022)

[4] Ответы Mail.ru. Временная блокировка действий в Instagram. URL:https://otvet.mail.ru/question/216176324 (дата обращения: 22.04.2022)

SMS-BOMBER AND ITS DANGEROUS ANALOGUES IN SOCIAL NETWORKS. EXAMPLES AND PROTECTION METHODS

MUSAEVA DIANA NADIROVNA
Faculty of Economics SNIGU them. N. G. Chernyshevsky, Saratov, Russian Federation, di.musaeva2018@yandex.ru

Abstract

This scientific work examines in detail the phenomena of destabilizing the moral and financial state of a person with the help of SMS bombers, programs that send many SMS messages from various services to one phone number, and their no less dangerous counterparts in social networks. The relevance of this topic is a consequence of the mass distribution of these negative phenomena, as well as personal experience of experiencing a “spam attack” from SMS bombers. The fact of the mass distribution of negative cases was also confirmed by my sociological study. The survey results showed that 41.3% of respondents were subjected to SMS bombing, and 48.8% of respondents became victims of various spam attacks on social networks. The purpose of the analysis is to study the precedents of spam attacks, as well as to find methods for effective protection against them. Particular attention in the course of research is paid to analogues of SMS bombers in social networks such as Telegram, TikTok, Instagram, VKontakte (VK), methods of influencing the victim, as well as ways to protect against them. In addition, the article focused on one of the most important reasons for the danger of these bombers - bots that encourage subscribers / users to go to sites / channels that promote extremism, potential harm to human health, as well as everything that is prohibited by the current legislation of the Russian Federation . During the study of the topic, it was concluded that the SMS bomber as a whole is not a particularly dangerous type of hacker attack, unlike its counterparts for social networks, the negative effects of which can bring up to deletion, blocking accounts without the possibility of recovery.

Key words: SMS bomber; spam; social media; blogger; bots; extremism