УДК 004.056
DOI: 10.31673/2409-7292.2021.034954

Костирєв Л.В., Кучер В.І.

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ЗАХИСТУ МЕСЕНДЖЕРА TELEGRAM ВІД БОТІВ ТА СПАМУ

У статті розглянуто потенціальні уразливості та вивчена схема роботи месенджера Telegram. Було проведено порівняння і аналіз переваг і недоліків захисту месенджера, внаслідок чого був обраний Telegram Bot API як найзручніший і доступний в плані документації месенджера Telegram. На основі цього були виявлені вимоги для розробки чат-бота. Останнім етапом виконаного завданням було обрано технології та середовище для розробки чат-бота серед яких Python, SaaP Heroku і VS Code та вбудовані засоби адміністрування Windows.

Ключові слова: Telegram, месенджер, бот, спам, технологія захисту.

Вступ

Проблема спаму у сервісі для миттєвого обміну повідомленнями Telegram набула особливу гостроту в останнє десятиліття, у зв'язку з вкрай неефективним функціонуванням системи забезпечення безпеки користувачів такого сервісу та необізнаності самих користувачів меседжерів. Сучасні європейські дослідження показують, приблизно 90% усіх кіберзагроз припадають на приватний сектор. Тобто, це не є цільові атаки на великі компанії, або окремих користувачів. Джерелом більшості таких кібератак є спам. Багато кібератак розраховані саме на неуважність та необізнаність користувачів. Наприклад Homograph Attack (фішінг), де URL фішінгового сайту має мінімальні, а іноді і неспостерігаємі відрізності від сайту оригіналу (наприклад англійську літеру «о» замінили на кириличну літеру «о»). Користувач відкриває фішинговий сайт, бачить знайомий (зкопійований з оригіналу) дизайн сайту, вводить туди свій логін та пароль, або данні кредитної карти і ними заволодіває зловмисник. У зв’язку з середнім щорічним збільшенням кількості викрадених данних банківських карт в Україні на 4-5 %, відповідальність за безпеку персональних данних лягає на плечі користувача.

Мета роботи – полягає в проектуванні та дослідженні методу забезпечення захисту сервісу для миттєвого обміну повідомленнями Telegram від спаму та ботів.

Аналіз особливостей безпеки сервісу для миттєвого обміну повідомленнями Telegram

В умовах сучасного інформаційного суспільства комп'ютерні технології настільки вкоренилися в нашому житті, що повністю змінили способи обміну інформацією, які ми використовуємо для спілкування з друзями, членами сім'ї і діловими партнерами. Незважаючи на те, що електронна пошта стає все більш мобільною, ділові люди все більше і більше звертаються до тих же самим засобам комунікації, які звичайні користувачі застосовують давно і з величезним успіхом: до миттєвого обміну повідомленнями (Instant Messaging, IM).

Telegram – Кросплатформенна програмне забезпечення, яке дозволяє обмінюватися текстовими, аудіо та відео повідомленнями та файлами, а також безкоштовно телефонувати іншим користувачам програми. Месенджер, який набуває популярності по всьому світу. Telegram сміло можна називати найбільш швидко зростаючим за популярністю месенджером. Станом на листопад 2020 він уже пересік відмітку у 400 мільйонів активних користувачів.

Творці месенджера заявляють про гарантії безпеки у відношенні передачі зашифрованих даних. В основі протоколу обміну лежить оригінальна комбінація симетричного алгоритму шифрування AES (в режимі IGE), протокол Діффі-Хеллмана для обміну 2048-бітними RSA-ключами між двома пристроями та ряд хеш-функцій. Протокол допускає використання шифрування end-to-end з опціональною звіркою ключів. Варто також згадати, що Telegram пропонує можливість секретних чатів, за яких практично не можливо отримати доступ до його вмісту.

© Костирєв Л.В., Кучер В.І., 2021

Ідентифікація користувача Telegram пов’язана з номером телефону користувача. Користувач вводить номер телефону до якого привязаний аккаунт. Потім сервер Telegram надсилає SMS із кодом підтвердження, користувач подає код із отриманого текстового повідомлення та створює, або входить в свій обліковий запис. В Telegram якщо користувач вже має авторизацію на пристрої цей код він може отримати в спеціальний офіційний чат. Також в цей чат приходять інші системні повідомленя, та списки оновлень від сервісів.

Така модель авторизації користувача є доволі безпечною, і наприклад сервіс для віртулізації робочих місць VMware Horizo Viev (VDI) використовує схожий алгоритм входу. А це є одним з найбезпечніших рішень для формату віддаленої роботи в корпоративному сегменті. Проблематикою безпеки в цьому випадку є забезпечення безпечної доставки СМС з унікальним кодом авторизації та спам що може містити кіберзагрози та роспвсюджується в цих меседжерах.

Проект бота модератора для групового чату з важливими повідомленнями.

Розвиток Телеграм багато в чому визначається наявністю великого числа ботів - невеликих сервісних програм-роботів. Їх може створити кожен користувач, знайомий з програмуванням на середньому рівні. Telegram API Bot – це програмний інтерфейс, що дозволяє програмувати власного бота.

В Бот Телеграм API всі елементи управління є об'єктами, які представлені в JSON, тобто у вигляді рядка, заданої за певними правилами. Це дозволяє проводити обмін даними по мережі максимально швидко і найменш ресурсно затратно, так як передається не програмний код, а набір пар «ключ: значення» в текстовому вигляді. Велика частина об'єктів призначена для створення команд бота. Ключі дадуть більш розширене уявлення про можливості об'єкта.

Телеграм пропонує два види API для розробників. Перше - це API Telegram, який призначений для створення сторонніх клієнтів для платформи Телеграм. В даній роботі він використовуватися не буде. Другий - Bot API, що дозволяє легко створювати програми, які використовують повідомлення Телеграм як інтерфейс у спілкуванні із користувачем.

Власне Bot API – це те, що дозволяє легко та зручно створювати чат-ботів. Цей API дозволяє підключати ботів до системи Телеграм. З точки зору системи Телеграм, боти – це спеціальні облікові записи, для яких не потрібно встановлювати додатковий номер телефону. Ці облікові записи служать інтерфейсом для коду, який буде працювати на сервері.

Для цього не потрібно заглиблюватися в схему роботи протокола шифрування MTProto, який застосовується у системі Телеграм – їх проміжний сервер буде обробляти всі шифрування та спілкування з API Телеграм. Для зв'язку з цим серверомвикористовується простий HTTPS-інтерфейс, який пропонує спрощену версію API Телеграм. Будь-які запити до Bot API Телеграм повинні передаватися через протоколHTTPS і мати наступну форму: https://api.telegram.org/bot<ТОКЕН>/<ІМЯМЕТОДУ>. На місці <ТОКЕН> відповідно повинен міститися токен авторизації бота, а на місці <ІМЯ МЕТОДУ> – метод який необхідно використати з API.

В API підтримуються GET і POST HTTP запити. GET-запит використовується за необхідності отримання певної інформації від API, а GET-запит – при необхідності передати якусь інформацію засобами Bot API.

Відповідь на будь-який запит містить об'єкт JSON, який завжди має логічне поле «ok», яке вказує на успішність запиту, а також може мати необов'язкове поле «description» з описом результату. Якщо «ok» встановлено в «true», запит бузуспішним, а результат запиту можна знайти в полі «result». У випадку невдалого запиту «ok» містить «false», а помилка описується в полі «description». Поле числового типу «error_code» вказує на код помилки. Деякі помилки також можуть мати необов'язкове поле «parameters», яке може допомогти автоматично опрацювати помилку.

HTTP-запити, REST API та JSON. REST – це стиль архітектури програмного забезпечення для побудови розподілених масштабованих веб-сервісів, які використовують http запити. HTTP використовується у всесвітній павутині дляпередачі даних і є одним з

© *Костирєв Л.В., Кучер В.І., 2021*

найбільш широко застосовуванихприкладних протоколів. HTTPS – це звичайний HTTP, що працює через шифровані транспортні механізми SSL і TLS. Він забезпечує захист від атак, заснованих на прослуховуванні мережевого з'єднання - від сніфферскіх атак і атак типу man-in-the-middle, за умови, що будуть використовуватися шифрувальні засоби і сертифікат сервера перевірений і йому довіряють. JSON (javascript object notation) – простий формат обміну даними, зручний для читання і написання як людиною, так і комп'ютером. Вінзаснований на підмножині мови програмування javascript, визначеного в стандарті ecma-262 3rd edition – december 1999. Json -текстовий формат, повністю незалежний від мови реалізації, але вінвикористовує угоди, знайомі програмістам с-подібних мов, таких як C, C++, C#, Java, Javascript, Perl, Python і багатьох інших. Ці властивостіроблять JSON ідеальним мовою обміну даними JSON заснований на двох структурах даних: колекція пар ключ/значення. У різних мовах, ця концепціяреалізована як об'єкт, запис, структура, словник, хеш, іменованийсписок або асоціативний масив - упорядкований список значень.

Об’єкти Telegram Bot API. Важливо що Телеграм, як платформа, дозволяє ботам проводити різноманітні операції як із повідомленнями, так і з чатами, а також підтримує та навіть заохочує використання ботів для різноманітної взаємодії. Факт того, що для покращення взаємодії із користувачами, вони обрали бота, як інтерфейс для створення інших ботів, тільки підтверджує те, що боти стали невід’ємною частиною сучасного спілкування. Крім того, як частина месенджера доступний бот для надсилання стікерів – спеціальних картинок, які заміняють Emoji.

API включає в себе об'єкти і команди, призначені для установки поведінки бота Telegram. Використовуючи інтерфейс, ви можете створювати власні програмні коди, які при запуску в Telegram починають працювати як боти.

Всі методи (а їх досить багато) діляться на групи:

отримання оновлень і інформації;

робота в чаті;

відправка різних елементів;

робота зі стікерами;

оновлення повідомлень;

режим inline;

платіжний функціонал;

для ігор.

Bot API представляє собою HTTP-інтерфейс для роботи з ботами в Telegram. Кожен бот – це спеціальний аккаунт, створений для автоматичного оброблення та відправлення повідомлень. існує двапротилежних за логікою способу отримання оновлень від бота:

Long pulling - додаток автоматично опитує сервера Telegram на наявність будь-яких оновлень для бота. За замовчуванням 100мс;

Webhook - сервера Telegram самі сповіщають додаток насервері як тільки з'являться будь-які оновлення.

Незалежно від способу отримання оновлень, у відповідь отримуємо об'єкт update, серіалізований в JSON.

Перший і найбільш простий варіант полягає в періодичному опитуванні серверів telegram на предмет наявності нової інформації.

Все цездійснюється через так званний Long polling, тобто відкривається з'єднання на нетривалий час і всі оновлення відправляються боту просто, але не дуже надійно. По-перше, сервери Telegram періодичнопочинають повертати помилку 504 (gateway timeout), через що деякі боти зупиняються.

По-друге, якщо одночасно запущено кілька ботів, ймовірність зіткнутися з помилками зростає.

Webhook працює трохи інакше. Під установкою Webhook мається на увазі, що тепер якщо в чат приходить повідомлення, то Telegram сам говорить про це. Відпадає необхідність періодично опитувати сервери, тим самим, зникає причина падінь спамерських пошукових

© *Костирєв Л.В., Кучер В.І., 2021*

роботів. Однак за цедоводиться платити необхідністю установки повноцінного веб-серверана ту машину, на якій планується запускати спамерських пошукових роботів. Так само для роботитреба мати власний SSL-сертифікат (secure sockets layer), тому що Webhook Telegram працюють тільки по HTTPS.для роботи з telegram bot api була вивчена документація, в якійописані всі методи і передані параметри, всі відповіді приходять в JSON-форматі. В ході написання чат-бота були протестовані івикористані наступні методи і типи. Метод polling() використовується для отримання оновлень через long polling. Відповідь повертається у вигляді масиву об'єктів update.

Принцип роботи взаємодії чат-бота і користувача зображений на рисунку 1 в вигляді високорівневої схеми.

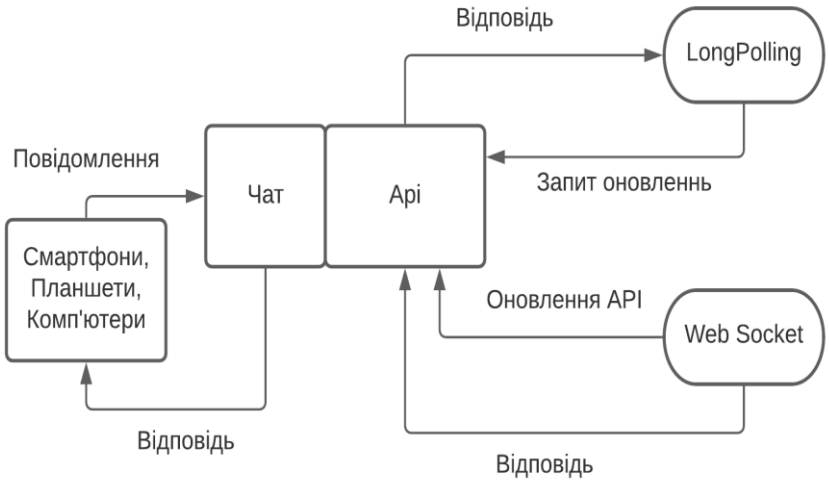

Рис 1. Принцип роботи чат-бота на платформі Telegram

Крім об'єктів API має набір методів, які дозволяють відправляти повідомлення, файл, фото стікери, редагувати і багато іншого. Всі ці команди можна знайти в описі API на офіційному сайті.

Таблиця 1

Перелік об’єктів Telegram API

Назва	Опис	Ключі
User	Користувач	Id, first_name, last_name, username
Chat	Чат	Id, type, title, username, first_name last_name, all_members_are_administrators
UserProfilePhotos	Фото профіля	total_count, photos
Location	Точка на карті	Longitude, latitude
Message	Повідомлення	message_id, from date, chat, forward_from, forward_date, reply_to_message, text, entities, audio, document, photo, sticker, video, voice, caption,contact, location, venue, new_chat_member, left_chat_member, new_chat_title, new_chat_photo, delete_chat_photo, group_chat_created, supergroup_chat_created, channel_chat_created migrate_to_chat_id, migrate_from_chat_id pinned_message

© *Костирєв Л.В., Кучер В.І., 2021*

Назва	Опис	Ключі
MessageEntity	Окрема частина повідолення	Type, length, url, offset
PhotoSize	Зображення.	file_id, width, height, file_size
Audio	Аудіозапис	file_id, duration, performer, title, mime_type file_size
Document	Будь який файл, що не є зображенням, стікером, аудіо, або відеозаписом.	file_id, thumb, file_name, mime_type, file_size
Sticker	Стікер – наліпка, аналог смайлів	file_id, width, height, thumb, file_size
Video	Відеозапис	file_id, width, height, duration, thumb, mime_type, file_size
Voice	Голосове повідомлення	file_id, duration, mime_type, file_size
Contact	Контакт	phone_number, first_name, last_name, user_id
Venue	Обьєкт на карті	Location, title, address, foursquare_id
File	файл	file_id, file_size, file_path
ReplyKeyboardMarkup	Клавіатура з можливістю відповіді	Keyboard, resize_keyboard, one_time_keyboard Selective,
KeyboardButton	Кнопка на клавіатурі для відповіді	Text, request_contact, request_location
ReplyKeyboardHide	Стандартна клавіатура Telegram	hide_keyboard, selective
InlineKeyboardButton	Кнопка на вбудованій клавіатурі.	Text, url, callback_data, switch_inline_query, switch_inline_query_current_chat, callback_game
CallbackQuery	Запит для зворотнього зв'язку	Id, from, message, inline_message_id, data
ForceReply	Ємулює дії користувача	force_reply, selective
ResponseParameters	Повідомляє про статус виконная запиту	migrate_to_chat_id, retry_after
InlineKeyboardMarkup	Вбудована клавіатура під повідомленням	inline_keyboard

Обмін повідомленнями відбувається у вигляді запитів. У таблиці 2 наведено приклади деяких з них.

Джерелом спаму саме у цій роботі було обрано картинки та стікери. Це є актуальним для робочих груп, або для груп у яких ведеться документообіг. Бот модеруює повідомлення типи яких додано до його конфігурації. Це в свою чергу оптимізує роботу модератора, оскільки бот автоматизую видалення контенту, в нашому випадку видалення зображень, та стікерів, щоб користувачі групи змогли зоосередитися на важливих текстових повідомленнях, в яких наприклад обговорюються робочі моменти. Тобто автоматизовано

© *Костирєв Л.В., Кучер В.І., 2021*

процес, пошуку, виділення та видалення контенту за його context-type. В ручному режимі ці дії б зайняли декілька, або і декілька десятків хвилин.

Таблиця 2

Методи Telegram API

Метод	Дія
getMe	Дозволяє отримати інформацію про користувача
sendMessage	Відправляє повідомлення
sendPhoto	Відправляє фото
sendAudio	Відправляє аудіозапис
sendDocument	Відправляє документ
sendVideo	Відпраляє відеозапис
sendContact	Відпраляє контакт
getUpdates	Отримує оновлення з чату

Висновки

Варто відзначити зростання популярності такого виду програмних продуктів як чат-боти, які працюють на платформах месенджерів. Цілодобова служба підтримки користувачів, конвертація документів і медіафайлів, замовлення таксі, пошук необхідних даних і багато іншого в даний час може бути реалізовано в рамках лише одного месенджера. Користувачам не доведеться завантажувати безліч додатків для вирішення різноманітних завдань, тому що досить мати лише клієнт месенджера і необхідний набір чат-ботів, які не займають місце на сховищі смартфона, а розміщені на хмарних платформах, або вашій власному ПК.

Перелік посилань

1. Скороход В. Визначення засобів розробки чат-бота «помічник абітурієнта» для сучасних месенджерів. Володимир Скороход. – 2017.
2. Seth Rosenberg. How To Build Bots for Messenger (12 April 2016) [online]. Fa- cebook; URL: https://developers.facebook.com/blog/post/2016/04/12/bots-for- messenger/ Accessed 8 April 2017.
3. Claudia-bot-builder [online]. Claudiajs; URL: https://github.com/claudiajs/claudia- bot-builder Accessed 8 April 2017.
4. Developer Survey Results 2017 [online]. StackOverflow; URL: http://stackover-flow.com/insights/survey/2017 Accessed 14 April 2017.

Надійшла: 18.07.2021 Рецензент: д.т.н., професор Кожухівський А.Д.

© *Костирєв Л.В., Кучер В.І., 2021*