Republic of the Philippines
National Police Commission
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City
E-mail: acg@pnp.gov.ph

ACG-CYBER SECURITY BULLETIN NR 201

ACG-CSB 112720201

Reference Number ACG-CSB 112720201

UNDERSTANDING THE HIDDEN DANGERS OF HIJACK TELEGRAM

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

Telegram is a messaging app with a focus on speed and security, it’s super-fast, simple and free. You can use Telegram on all your devices at the same time your messages sync seamlessly across any number of your phones, tablets or computers.

To steal Telegram cache and key files, the malware is not taking advantage of software flaws. The malware is capable of targeting only the desktop version of the popular messenger because it does not support Secret Chats and does not have the auto-logout feature active by default.

This means that the attacker can use those stolen files to access the victim’s Telegram session (if the session is open), contacts and previous chats.

With Telegram, you can send messages, photos, videos and files of any type doc, zip and mp3, as well as create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. You can write to your phone contacts and find people by their usernames. As a result, Telegram is like SMS and email combined and can take care of all your personal or business messaging needs. In addition to this, we support end-to-end encrypted voice calls.

Hackers who had access to the Signaling System 7 (SS7) have managed to target high-level employees within the crypto-currency industry. The hackers used SS7 to steal 2-Factor Authentication (2FA) codes sent to victims through SMS. The attacker spoofed a message of a mobile network operator to send an update location request to the targeted phone number. The update request asked the provider to send the fake message service center all of the calls and messages that the phone would get. Since the attacker was in control of the spoofed message service center, they managed to gather all of the messages sent to the phone. With previously compromised credentials, the attackers were able to use them and the 2FA codes to

log in to the accounts of victims. Telegram was the main application that was targeted where the attackers would private message others trying to exchange crypto currency. It is not believed anyone fell for the scam once the accounts were compromised.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the Hijack Telegram, to wit:

- Before entering personal info on any Web page, check that the connection is secure, and take a close look at the domain name of the page in the address bar. In this case, it should be telegram.org, not telegram-antispam.org, antispam-verification.com, or any such variant.
- Be wary of messages from accounts that are not in your address book, and don't follow suspicious links. Telegram administrator accounts have verification badges in the account information. If you receive a message supposedly from Telegram, but there is no such badge, it's a scam. Another telltale sign is if Telegram prompts you about marking the message as spam. Obviously, the service won't detect a message from itself as spam.

For additional information, please refer to the following websites:

- https://www.binarydefense.com/threat_watch/hackers-hijack-telegram-accounts-by-stealing-2fa-codes-sent-through-sms/
- https://cyware.com/news/hackers-hijack-telegram-email-accounts-in-ss7-mobile-attack-fbfc6ab3
- https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here

POINT OF CONTACT

Please contact **PMAJ JOSEPH ARVIN L VILLARAN**, Police Communication Relation officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.