REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

Analysis of the phishing attempt and the Telegram account compromise.

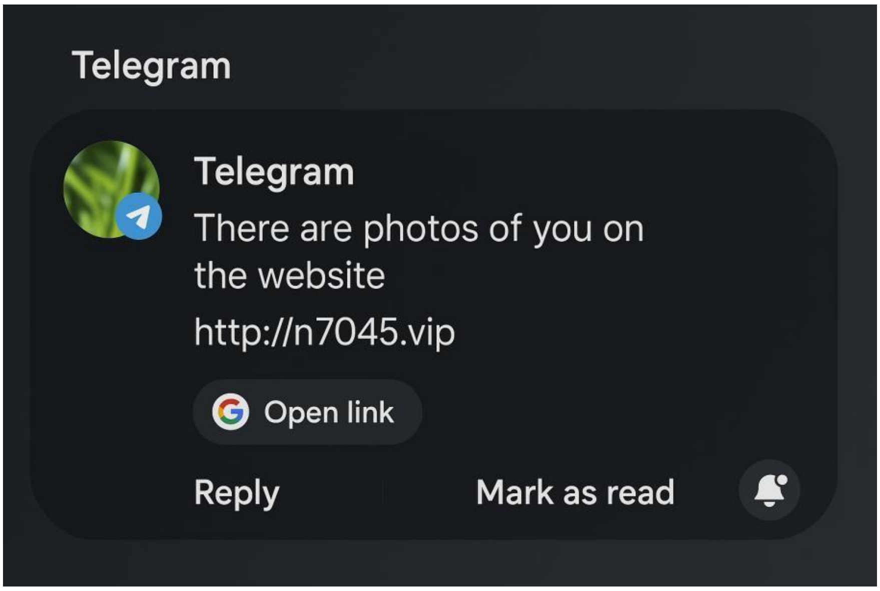
Version:1.0
Date:14.08.2025

CONTENTS

Table of Figures

Attack scenario: phishing technique used

The National Cybersecurity Authority (AKSK) has identified and analyzed a new phishing campaign targeting the compromise of Telegram accounts. This campaign relies on social engineering techniques, sending manipulative alerts intended to provoke user interaction**,** such as**.** "Your photos are online," which contain a malicious link. The link redirects the victim to a fake website crafted by threat actors to mimic the appearance and functionality of the official Telegram platform.



Telegram

Telegram

There are photos of you on the website

http://n7045.vip

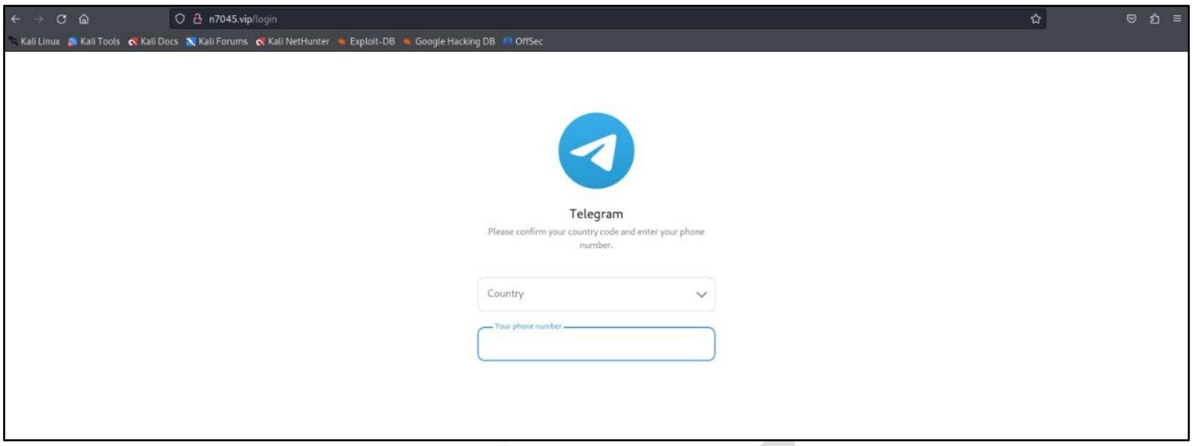
Figure 1- Example of a phishing message on Telegram

Account compromise process via malicious, illegitimate link

In the initial phase, the user enters their phone number on a fake website created by malicious actors to mimic the legitimate service provided by the official Telegram application. Without the user's knowledge, the attackers use the submitted number to initiate a real authentication process on Telegram (e.g., via the API or web application). As part of the standard procedure, Telegram sends a verification code (OTP) to the provided number via SMS.

In the second phase, the user is prompted to enter the verification code (OTP) to complete Telegram's multi-factor authentication (MFA) process. Once the victim submits the code, the attacker immediately gains access and begins using the Telegram account in real time, simultaneously with the legitimate user (the victim).

This compromise enables the malicious actor to read conversations, deploy additional phishing messages to the victim's contacts, and perform other malicious actions with the same intent—significantly increasing the risk of attack propagation.



n7045.vip/login

Telegram

Please confirm your country code and enter your phone number.

Country

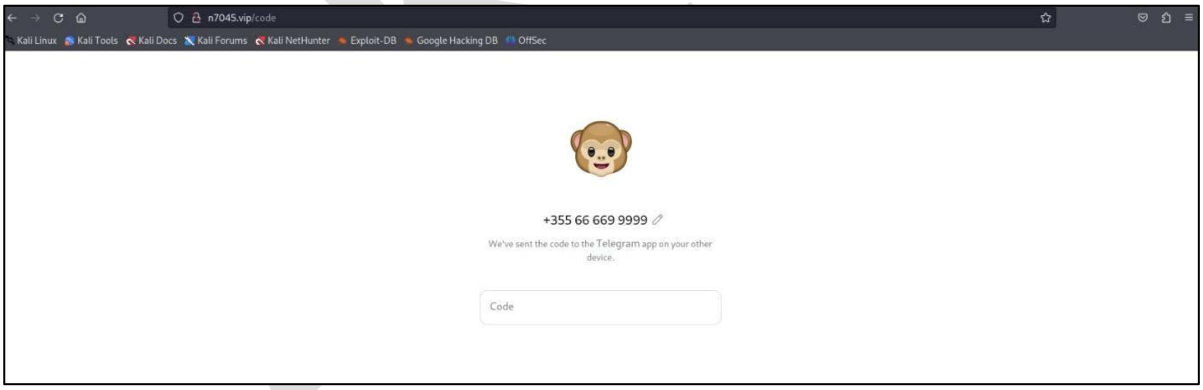
Your phone number

Figure 2- The spoofed Telegram page

The analysis of the attempted attack revealed that the IP address hosting the malicious page contains a series of similar domains, suggesting the use of automated methods for scalable deployment and spread of spoofed domains. The full list of Indicators of Compromise (IOCs) is included in this report to support identification, blocking, and awareness efforts for all social media users and beyond.

The social engineering techniques used in the campaign

The attacker impersonates a known contact in the message, exploiting the existing trust between users. Its content uses elements designed to create urgency and curiosity. The phishing page is carefully crafted to closely mimic the official Telegram interface, replicating the logo, color scheme, and login layout—making users feel as though they are in a secure and legitimate environment.



n7045.vip/code

+355 66 669 9999

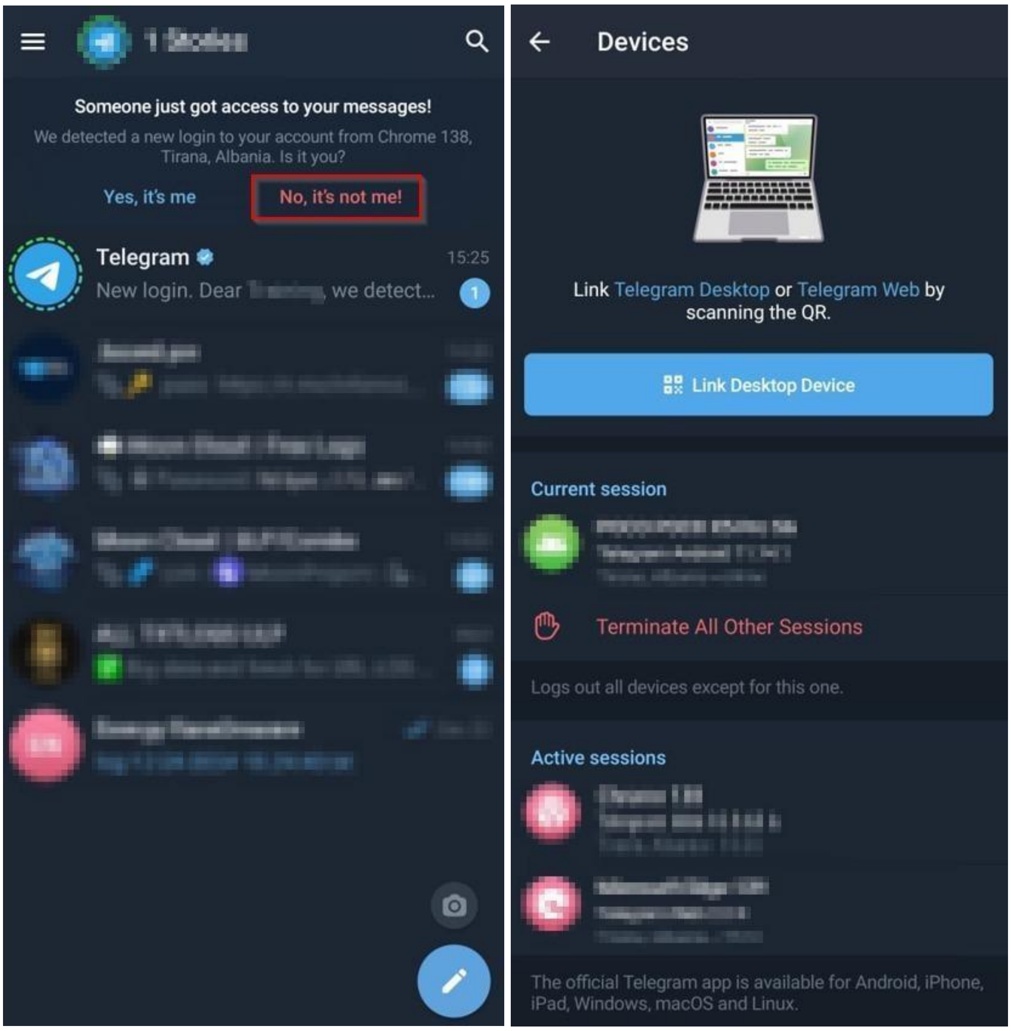
We've sent the code to the Telegram app on your other device.

Code

Figure 3-Prompt for the authorization code (OTP) during login

In cases where access has been authorized, the following steps are recommended to take
immediate action:

1) Click “No. It’s not me!” – This indicates that the person who accessed your Telegram account is not authorized.
2) Check the list of devices connected to your Telegram account, and terminateall unauthorized sessions



Someone just got access to your messages!

We detected a new login to your account from Chrome 138, Tirana, Albania. Is it you?

Telegram

New login. Dear [redacted], we detect...

Link Telegram Desktop or Telegram Web by scanning the QR.

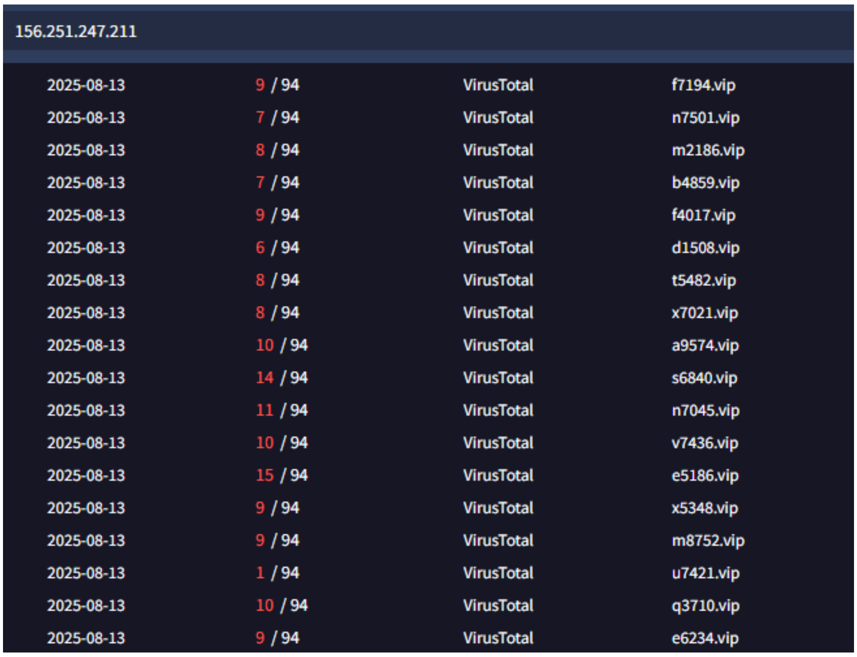
Logs out all devices except for this one.

The official Telegram app is available for Android, iPhone, iPad, Windows, macOS and Linux.

Figure 4-Steps taken to revoke unauthorized access

Technical Information

Through verification and comparison with previous IOC databases, it was found that the IP address 156[.]251[.]247[.]211 and its associated domains follow a predictable naming pattern (e.g., n#####.vip, f#####.vip). This pattern aligns with structures previously used in phishing campaigns targeting messaging applications such as WhatsApp and Facebook Messenger.



156.251.247.211

2025-08-13	9 / 94	VirusTotal	f7194.vip
2025-08-13	7 / 94	VirusTotal	n7501.vip
2025-08-13	8 / 94	VirusTotal	m2186.vip
2025-08-13	7 / 94	VirusTotal	b4859.vip
2025-08-13	9 / 94	VirusTotal	f4017.vip
2025-08-13	6 / 94	VirusTotal	d1508.vip
2025-08-13	8 / 94	VirusTotal	t5482.vip
2025-08-13	8 / 94	VirusTotal	x7021.vip
2025-08-13	10 / 94	VirusTotal	a9574.vip
2025-08-13	14 / 94	VirusTotal	s6840.vip
2025-08-13	11 / 94	VirusTotal	n7045.vip
2025-08-13	10 / 94	VirusTotal	v7436.vip
2025-08-13	15 / 94	VirusTotal	e5186.vip
2025-08-13	9 / 94	VirusTotal	x5348.vip
2025-08-13	9 / 94	VirusTotal	m8752.vip
2025-08-13	1 / 94	VirusTotal	u7421.vip
2025-08-13	10 / 94	VirusTotal	q3710.vip
2025-08-13	9 / 94	VirusTotal	e6234.vip

Figure 5- List of malicious domains

The analysis further reveals that threat actors are leveraging the .vip top-level domain (TLD) due to its affordability, limited oversight by registrars, and the ease with which new sites can be launched after existing ones are taken down. This data suggests a strong likelihood that these elements are part of a centralized and resilient infrastructure, operated by a group specializing in *phishing* attacks across multiple platforms, with the ability to rapidly scale and adapt to evolving security measures

This type of attack poses a high risk to individuals and institutions, especially when there is a lack of awareness regarding the clicking of incoming links or interaction with malicious actors. The compromise of a Telegram account directly affects the confidentiality of communications and the integrity of personal data. Once malicious actors gain control of the account, they can distribute phishing messages to all contacts within minutes, triggering a chain reaction of spread. For institutions, there is a risk that employee accounts may be used to conduct fraudulent campaigns, collect sensitive information, or damage their reputation. Since this attack model can be easily replicated using new domains and infrastructure, the potential for rapid and widespread propagation remains high

Indicators of Compromise (IOCs)

The Indicators of Compromise (IOCs) presented below were identified during the technical analysis of the phishing campaign and represent key elements that can be used to detect and block malicious activity. This data is crucial for cybersecurity professionals and system administrators, as it enables proactive identification of suspicious traffic and timely implementation of preventive measures:

156[.]251[.]247[.]211
n7045[.]vip
f7194[.]vip
n7501[.]vip
m2186[.]vip
b4859[.]vip
f4017[.]vip
d1508[.]vip
t5482[.]vip
x7021[.]vip
a9574[.]vip
s6840[.]vip
v7436[.]vip
e5186[.]vip
x5348[.]vip
m8752[.]vip
u7421[.]vip
q3710[.]vip
e6234[.]vip

Recommendations

AKSK provides practical guidelines for citizens aimed at preventing account compromise and protecting against similar phishing campaigns. The following recommendations are based on case analysis and include immediate steps to minimize risk and safeguard personal information:

1) Avoid clicking on links sent by unknown individuals or channels.
2) Verify the URL before entering any confidential or sensitive information.
3) Report phishing messages immediately within the platform and notify the affected user.
4) If you have entered a one-time code sent by the platform, check active sessions in Telegram and remove any unknown connected devices.
5) Conduct internal awareness campaigns for employees about phishing risks in messaging applications.
6) Block IPs and domains listed in the Indicators of Compromise (IOCs) via firewall, proxy, and endpoint security systems.