BREAKING CYBERSECURITY NEWS: CROCODILUS - A NEW MOBILE BANKING TROJAN STEALING OTPS AND CRYPTOCURRENCY WALLETS

Vairav Cyber Security News Report

Date: April 1, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A newly discovered mobile banking Trojan, Crocodilus, is emerging as a serious threat to Android users, with capabilities far beyond traditional credential theft. ThreatFabric says Crocodilus employs overlay attacks, keylogging, and remote access tools to steal banking credentials, OTP codes from Google Authenticator, and cryptocurrency wallet seed phrases. The malware is designed for full device takeover, using black overlay attacks to hide its presence and muting device sounds to avoid detection.

DETAILED ANALYSIS

Crocodilus is deployed via a proprietary dropper that bypasses Android 13+ security measures. Once installed, it tricks users into enabling Accessibility Services, granting itself extensive control over the device. The malware connects to a command-and-control (C2) server to receive target application lists and execute fraudulent transactions.

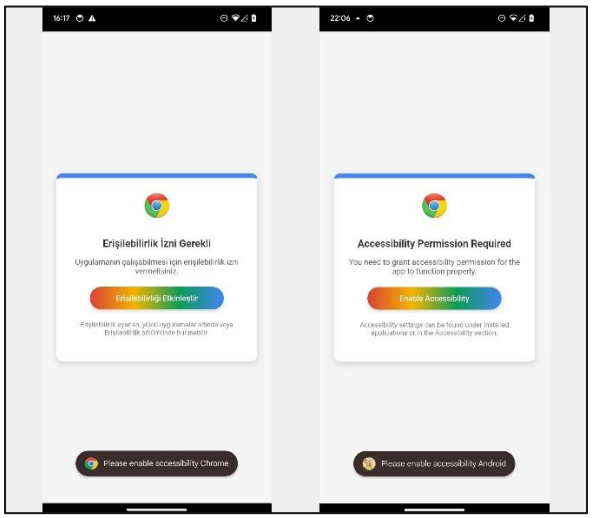

Figure 1: Requesting accessibility service

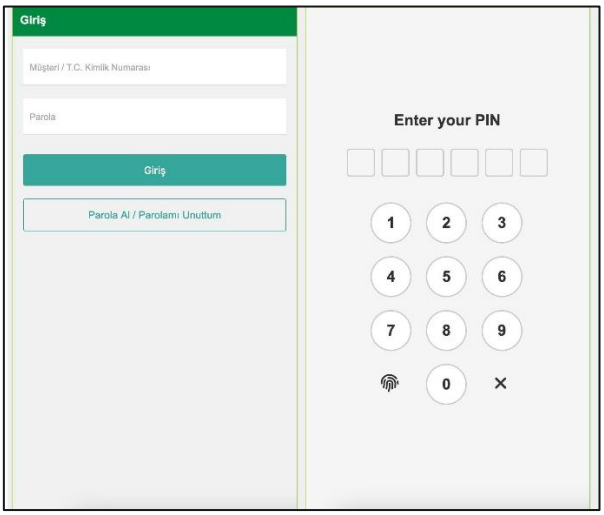

Figure 2: Displaying overlays to intercept credentials

The key attack techniques include:

- Instead of traditional keylogging, the malware monitors all on-screen events, logging text changes and capturing OTPs.
- Attackers can remotely control infected devices while concealing their activity behind a black screen overlay.
- A specialized command (TG32XAZADG) allows Crocodilus to extract one-time passwords.
- Victims are tricked into revealing their seed phrases through deceptive overlays.

IMPACT AND EXPLOITATION

- Attackers gain persistent access, execute remote commands, and manipulate banking applications.
- Stolen OTPs allow bypassing multi-factor authentication (MFA), leading to unauthorized transactions.
- Victims unknowingly reveal their private keys, leading to asset theft.
- The malware uses black screen overlays, muting alerts, and running in the background to avoid detection.

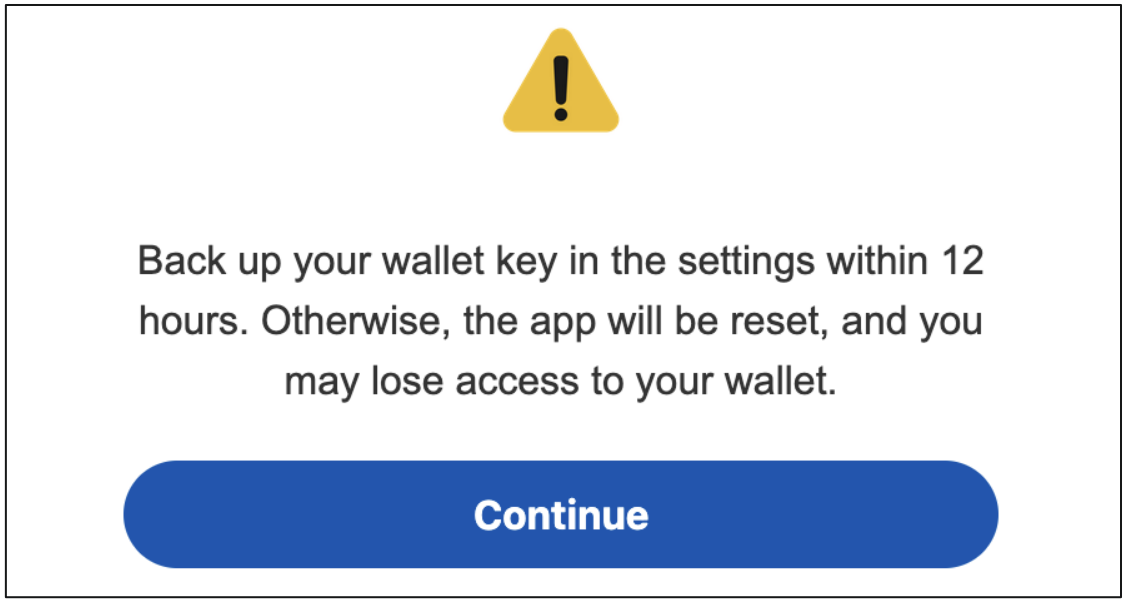

Figure 3: Overlays targeting cryptocurrency wallet

- The targeted sectors are banking institutions and crypto wallets of Spain and Turkey.

INDICATORS OF COMPROMISE (IOCs)

SHA256 hash - c5e3edafdfda1ca0f0554802bbe32a8b09e8cc48161ed275b8fec6d74208171f

C2 - register-buzzy[.]store

RECOMMENDED ACTIONS

- Users should avoid granting Accessibility Service permissions to unknown apps.
- Security teams should deploy behavior-based detection systems to identify abnormal activities like black screen overlays and unauthorized remote access.
- Organizations should block associated C2 domains and IPs linked to Crocodilus.

- Awareness campaigns should emphasize the risks of granting excessive app permissions and recognizing social engineering tactics.
- Use hardware-based authentication methods instead of SMS or app-based OTPs.

Crocodilus represents a new era of Android banking malware, combining stealth, sophistication, and full-device control. As its operators continue refining their capabilities, organizations must proactively enhance mobile security defenses to mitigate the risks posed by this emerging threat.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices

https://securityonline.info/android-under-attack-crocodilus-trojan-captures-otps-from-google-authenticator/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com