Crocodilus Mobile Malware: Evolving Fast, Going Global

threatfabric.com/blogs/crocodilus-mobile-malware-evolving-fast-going-global

Jump to

Introduction

In March 2025, the Mobile Threat Intelligence team discovered Crocodilus, a new device-takeover Android banking Trojan entering the threat landscape. The first observed samples were mostly related to test campaigns, with sporadic instances of live campaigns.

Ongoing monitoring of the threat landscape revealed a growing number of campaigns and continuous development of the Trojan. In this report, we cover the latest findings, including:

- New campaigns expanding the target list to European countries and extending overseas to South America
- Malicious advertising campaigns distributing Crocodilus via social networks
- An updated feature set, including the creation of new contacts in the victim's contact list (likely for social engineering), and an automated seed phrase collector
- Improved obfuscation techniques applied to the dropper and malicious payload

Croco-bonus - Get Free Malware!

Initial Crocodilus samples showed evidence of operations in Europe, although early campaigns largely targeted Turkey. Recent activity reveals multiple campaigns now targeting European countries while continuing Turkish campaigns and expanding globally to South America.

One notable campaign that caught our analysts' attention was targeting users in Poland. Mimicking the apps of banks and e-commerce platforms, the malware was promoted via Facebook Ads. These ads encouraged users to download an app to claim bonus points. One of the identified ads is shown below:

Malicious advertisement leading to Crocodilus dropper download

According to Facebook's ad transparency data, these advertisements were live for just 1–2 hours, but each was shown more than a thousand times. The majority of viewers were over 35, indicating a focus on a solvent audience.

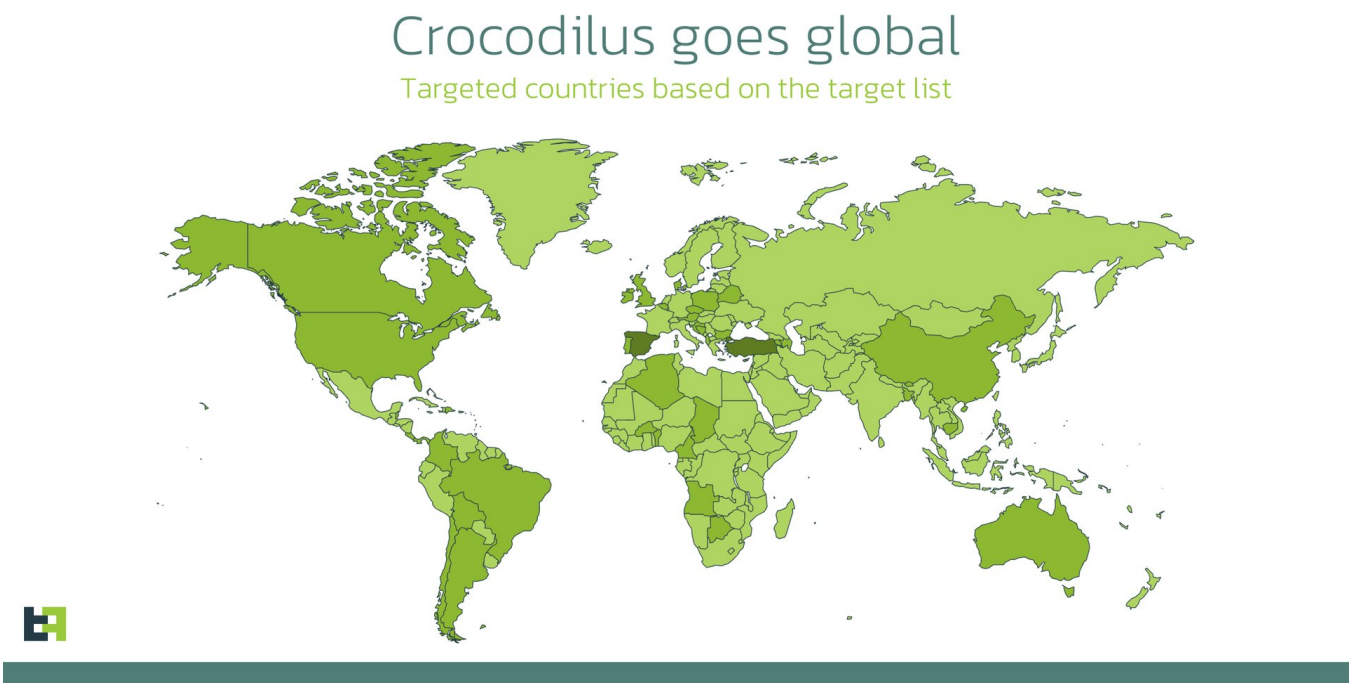
Upon clicking the "Download" button, users were redirected to a malicious site that delivered the Crocodilus dropper, capable of bypassing Android 13+ restrictions.

Going Global - While Keeping It's roots

Crocodilus continues to run campaigns in Turkey, targeting users of major banks and cryptocurrency platforms. One such campaign disguised itself as an online casino. We suspect the distribution method remained malicious ads. Once installed, Crocodilus actively monitors the launch of Turkish financial apps, overlaying them with fake login pages.

Another campaign is targeting Spanish users, distributing Crocodilus disguised as a browser update. The target list includes nearly all Spanish banks, clearly showing a regional focus.

In addition to these targeted efforts, MTI has also observed smaller campaigns with very "global" target lists, involving apps from Argentina, Brazil, Spain, the US, Indonesia, and India.



Interestingly, the masquerading used in this campaign include cryptocurrency mining and digital banks in Europe.

New Developments

The latest campaigns not only broaden Crocodilus' geographic scope but also introduce enhancements to both the dropper and payload components.

Malware developers have worked to improve obfuscation techniques in an attempt to hinder analysis and detection. These include:

- Code packing for both the dropper and payload
- Additional XOR encryption of the payload (Crocodilus) to conceal it during analysis
- Entangled, convoluted code to complicate reverse engineering

In addition to improved obfuscation, the MTI team observed a new Crocodilus variant with several significant new features.

Making New Friends - Adding Contacts to The Device

A key feature update is the ability to modify the contact list on an infected device. Upon receiving the command "TRU9MMRHBCRO", Crocodilus adds a specified contact to the victim's contact list.

This further increases the attacker's control over the device. We believe the intent is to add a phone number under a convincing name such as "Bank Support", allowing the attacker to call the victim while appearing legitimate. This could also bypass fraud prevention measures that flag unknown numbers.

Improving the Quality of Stolen Data – Seed Phrase Collector

Just like its predecessor, the new variant of Crocodilus pays a lot of attention to cryptocurrency wallet apps. This variant was equipped with an additional parser, helping to extract seed phrases and private keys of specific wallets.

It is based on the AccessibilityLogging feature, already present in first variants but further improved with pre-processing of the logged data displayed on the screen, extracting data of specific format based on regular expressions.

Targeted apps and regular expressions used to extract data

In our previous blog about Crocodilus we highlighted the interest of cybercriminals in cryptocurrency wallets as they were making victims open the wallet apps to further steal the data displayed on the screen. With additional parsing done on the device side, threat actors receive high-quality preprocessed data, ready to use in fraudulent operations like Account Takeover, targeting cryptocurrency assets of victims.

Conclusion

The latest campaigns involving the Crocodilus Android banking Trojan signal a concerning evolution in both the malware's technical sophistication and its operational scope. With newly added features, Crocodilus is now more adept at harvesting sensitive information and evading detection. Notably, its campaigns are no longer regionally confined; the malware has extended its reach to new geographical areas, underscoring its transition into a truly global threat.

This shift not only broadens the potential impact but also suggests a more organised and adaptive threat actor behind its deployment. As Crocodilus continues to evolve, organisations and users alike must stay vigilant and adopt proactive security measures to mitigate the risks posed by this increasingly sophisticated malware.

Appendix

IoCs

App name	Package name	SHA256 Hash	C2
IKO	nuttiness.pamperer.cosmetics	6d55d90d021b0980528f56d040e78fa7b85a96f5c244e23f330f24c8e80c1cb2	rentvillcr[.]homes
ETH Mining app	apron.confusing	fb046b7d0e385ba7ad15b766086cd48b4b099e612d8dd0a460da2385dd31e09e	rentvillcr[.]online