Expanding the Investigation: Deep Dive into Latest TrickMo Samples - Zimperium

By Aazim Yaswant

Published: 2024-10-11 · Archived: 2026-04-05 13:39:51 UTC

Executive Summary

On September 10, Cleafy publicly disclosed a new variant of the Banking Trojan called *TrickMo*. This variant employed innovative techniques to evade detection and analysis, such as zip file manipulation and obfuscation. While Cleafy did not release any Indicators of Compromise (IOCs), our research team conducted its own research and identified 40 recent variants of this threat, 16 droppers and 22 active Command and Control (C2) as well as additional functionalities.

Our analysis suggests that many of these samples remain undetected by the broader security community.

Quick Features Recap

The 40 variants analyzed by our research team show identical capabilities to those shared by Cleafy, including:

- OTP interception
- Screen recording
- Data exfiltration
- Remote control
- Automatic permission granting and auto-click on prompts
- Accessibility service abuse
- Overlay display and credential theft

These capabilities enable the malware to effectively access any type of information stored on the device. Moreover, these capabilities can be combined to facilitate unauthorized access to bank accounts and financial transactions, potentially resulting in significant financial losses for victims.

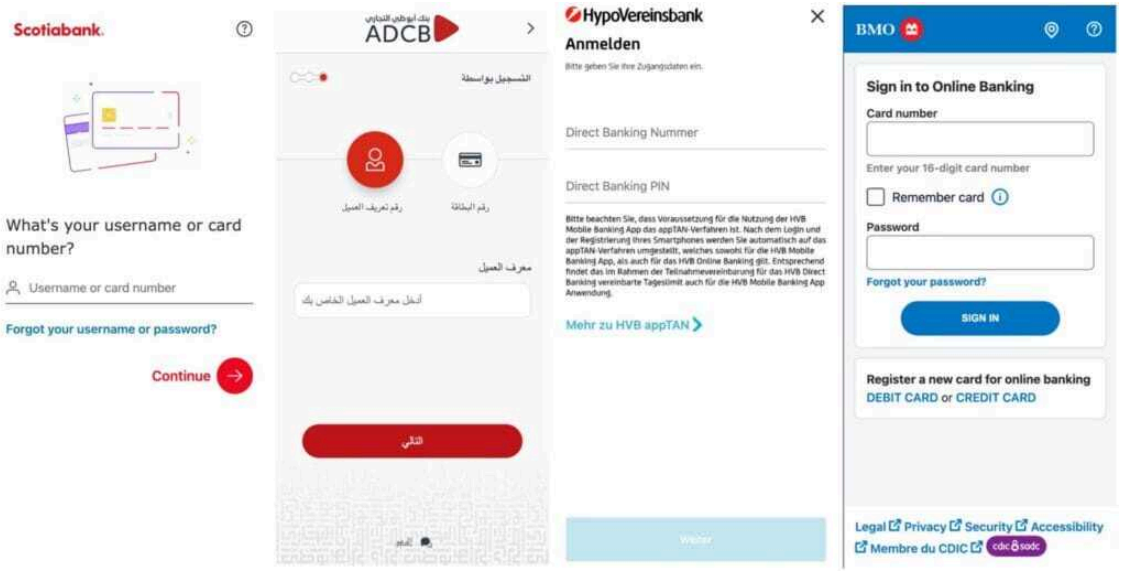


Fig.1 deceptive overlays

A New Dangerous Twist: Unlock Code Theft

In addition to the core capabilities mentioned above, we also discovered a new capability in some of the samples that allows these variants to steal the device's unlock pattern or PIN. This new addition enables the threat actor to operate on the device even while it is locked. To obtain the necessary unlock information, the malware presents a deceptive User Interface (UI) that mimics the device's actual unlock screen.

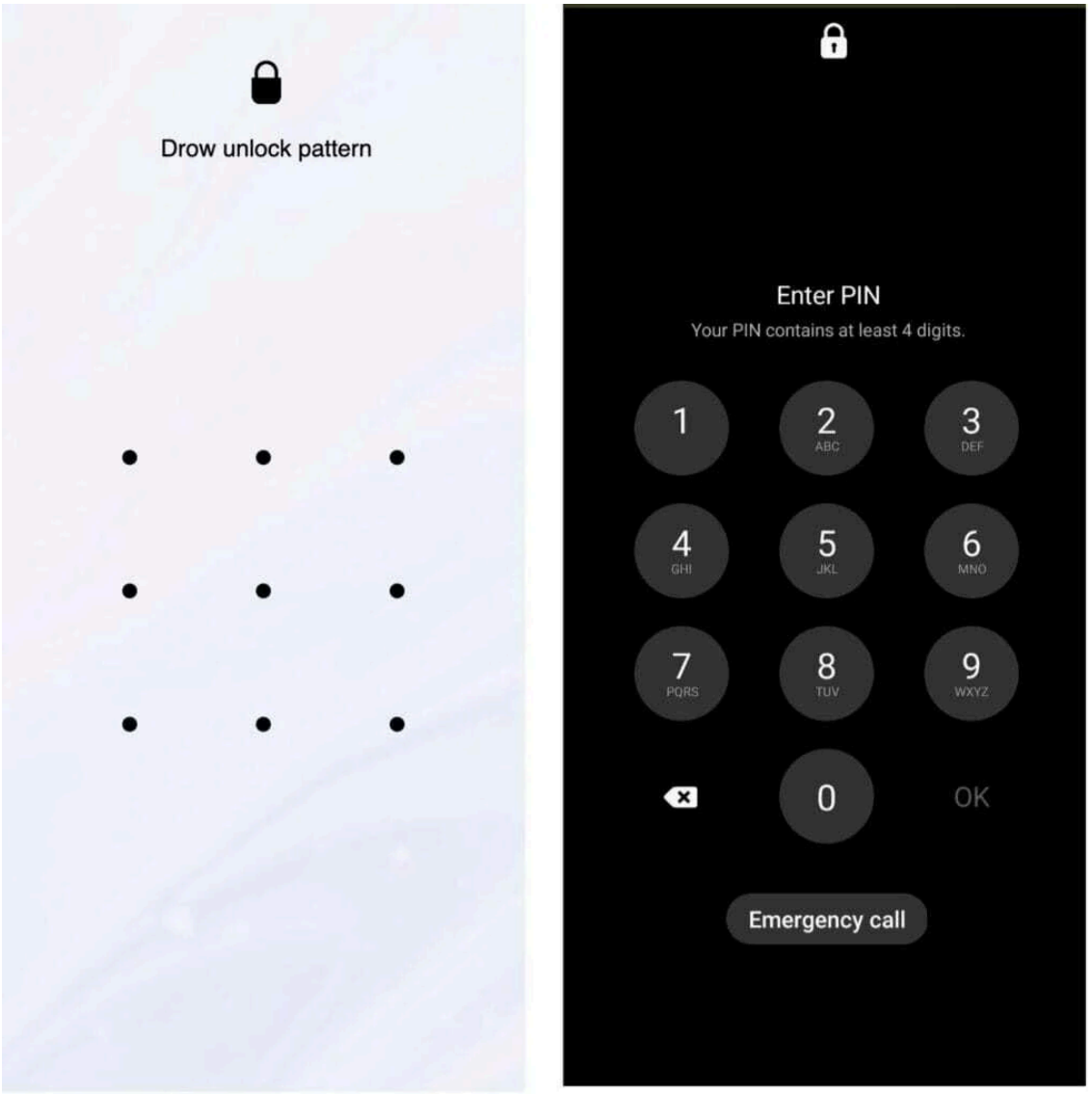


Fig.2 fake unlocking UI

The deceptive User Interface is an HTML page hosted on an external website and is displayed in full-screen mode on the device, making it look like a legitimate screen. When the user enters their unlock pattern or PIN, the page transmits the captured PIN or pattern details, along with a unique device identifier (the Android ID) to a PHP script. To obtain the Android ID, the WebView binds a method named “getAndroidID”. This method retrieves the corresponding value from the device and appends it to the POST request after the PIN or pattern is acquired.This mechanism allows the Threat Actor (TA) to link the stolen credentials to the specific victim’s device.

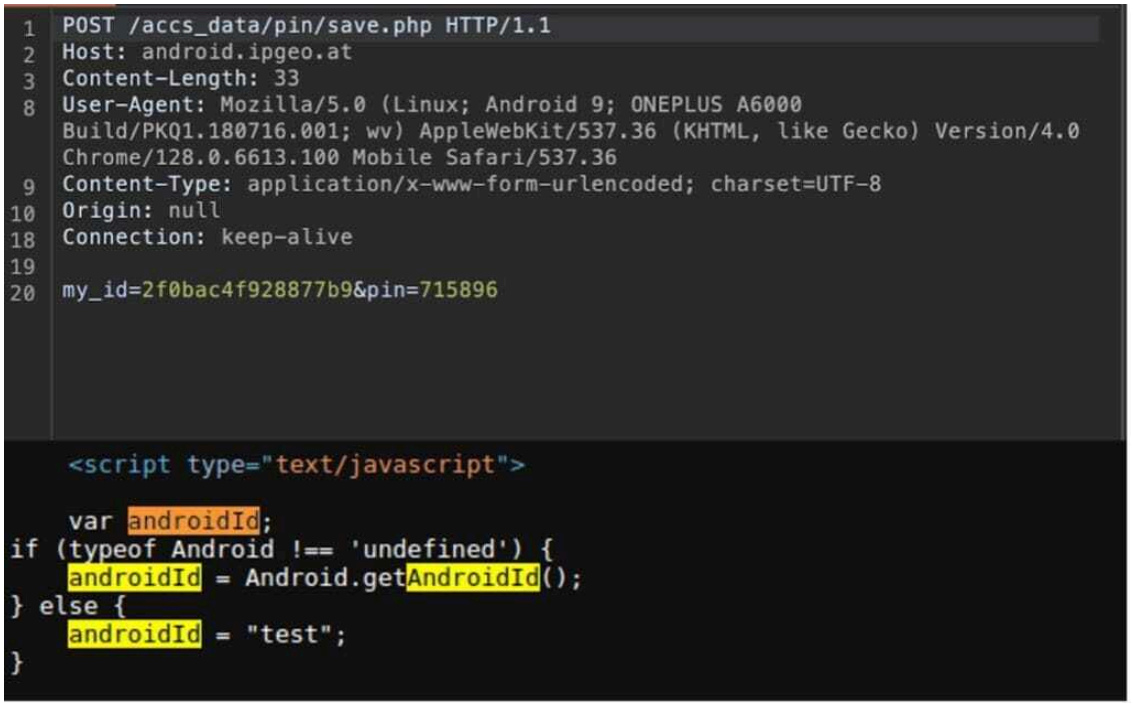


Fig.3 request sent to the C2 and JS code to get the AndroidID

Exposed C2 Server: Geolocating Victims

During our analysis, we successfully gained access to several C2 servers. Within the directories of the C2 servers, we discovered files with approximately 13,000 unique IP addresses belonging to the victims of this malware. After obtaining the list of IP addresses, we geolocate them to check the region targeted by this malware and its variants.

Our analysis revealed that the primary targets of this malware were:

- Canada
- United Arab Emirates
- Turkey
- Germany

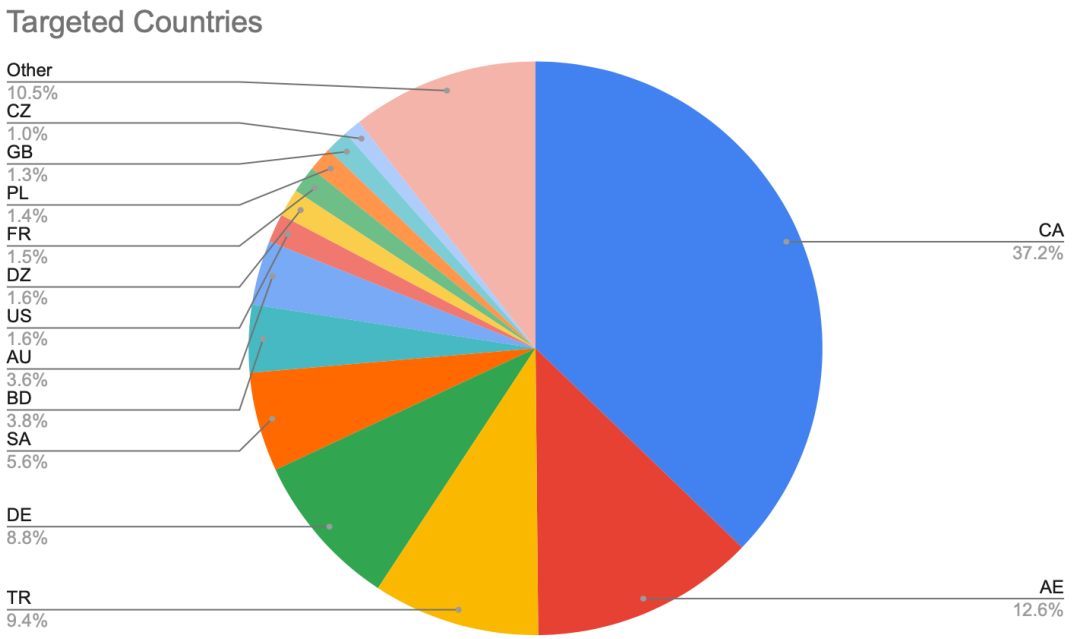


Fig.4 Percentage of victims per targeted country

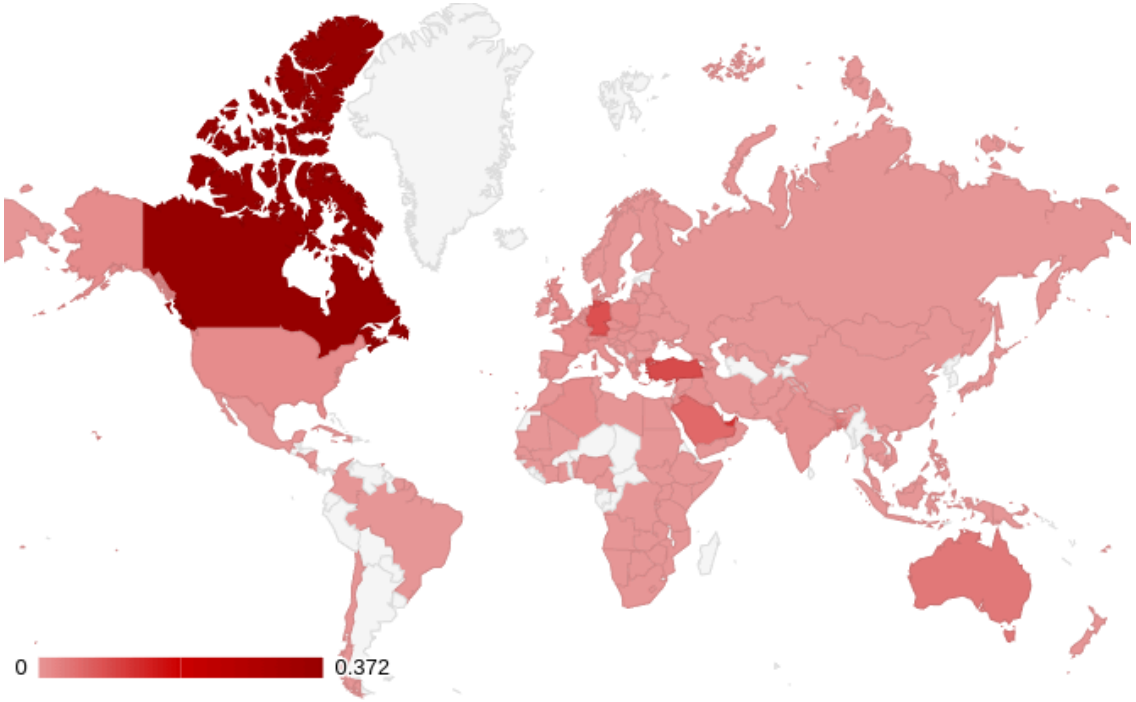
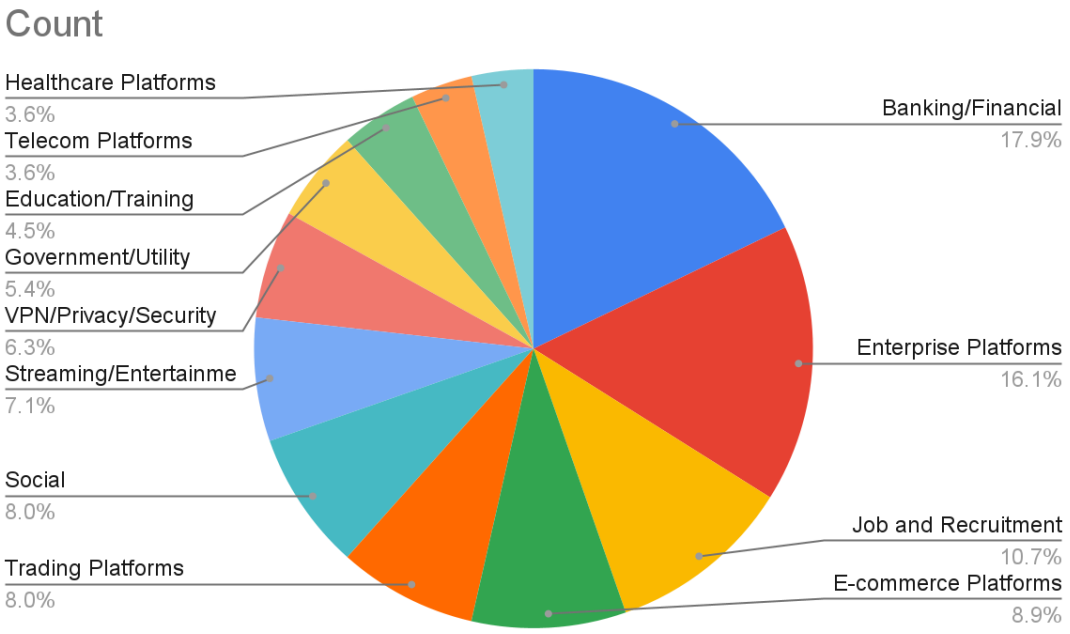


Fig.5 Targeted countries color-coded to represent the % of victims per region

Despite the absence of data leakage issues observed in these newer C2 servers, our analysis revealed that the IP list file is regularly updated whenever the malware successfully exfiltrates credentials. We discovered millions of records within these files, indicating the extensive number of compromised devices and the substantial amount of sensitive data accessed by the Threat Actor.

These stolen credentials are not only limited to banking information but also encompass those used to access corporate resources such as VPNs and internal websites. This underscores the critical importance of protecting mobile devices, as they can serve as a primary entry point for cyberattacks on organizations.

Through our analysis of exfiltrated data, we identified a diverse range of targeted applications spanning multiple categories. This comprehensive analysis enabled us to compile a list of most targeted application types, which are summarized in the following chart.



Zimperium vs. Trickmo

Given the malware's advanced capabilities and extensive control over infected devices, to safeguard your users and devices from this malware and others similar, it is critical to deploy proactive, robust protection and mitigation measures to prevent data or financial loss.

Zimperium is uniquely equipped to support enterprises (MTD) and app developers (MAPS) in defending against the constantly evolving threat landscape targeting mobile devices. Powered by our proprietary On-Device Dynamic Detection Engine, both MTD and MAPS products leverage local, on-device advanced machine learning, behavioral analysis and deterministic detection, to deliver comprehensive threat detection and mitigation without compromising user experience or development timelines.

Our cutting-edge detection engine has successfully identified and neutralized all malware samples and malicious URLs discussed in this blog post, underscoring its unmatched effectiveness in protecting against emerging cyber threats.

MITRE ATT&CK Techniques

To help our customers and the industry understand the impact of this malware, Zimperium has compiled the following table containing the MITRE Tactics and Techniques as reference.

Tactic	ID	Name	Description
Initial Access	T1660	Phishing	Adversaries send malicious content to users in order to gain access to their device.
Persistence	T1398	Boot or Logon Initialization Scripts	The malware is executed at boot.
	T1624.001	Event Triggered Execution: Broadcast Receivers	It creates a broadcast receiver to receive SMS events and outgoing calls.
	T1541	Foreground Persistence	It puts itself on foreground for abusing notifications.
Defense Evasion	T1407	Download New Code at Runtime	It can download and execute DEX dynamically.
	T1628.001	Hide Artifacts: Suppress Application Icon	It hides the application icon.
	T1629.001	Impair Defenses: Prevent Application Removal	It prevents the user from uninstalling the app by showing a prompt.
	T1630.002	Indicator Removal on Host: File Deletion	It can delete all his traces.
	T1516	Input Injection	It abuses user accessibility APIs to grant permissions.
	T1655.001	Masquerading: Match Legitimate Name or Location	It is using the Google services app’s name and icon.
	T1406.002	Obfuscated Files or Information: Software Packing	It is using obfuscation and packers (JSONPacker) to conceal its code.
Credential Access	T1517	Access Notifications	It has a notification listener.
	T1414	Clipboard Data	It extracts data stored on the clipboard.
	T1417.001	Input Capture: Keylogging	It has a keylogger feature.

	T1417.002	Input Capture: GUI Input Capture	It is able to get the shown UI.
	T1635	Steal Application Access Token	It steals OTPs.
Discovery	T1420	File and Directory Discovery	It enumerates all the videos and pictures on the device.
	T1418	Software Discovery	It gets the list of installed applications.
	T1426	System Information Discovery	It gets info about the device as the androidID.
Collection	T1517	Access Notifications	It registers a receiver to monitor incoming SMS messages.
	T1429	Audio Capture	It has the ability to steal audio from the device.
	T1414	Clipboard Data	It has the ability to steal data from the clipboard.
	T1533	Data from Local System	It searches for files of interest before the exfiltration.
	T1417.001	Input Capture: Keylogging	It has a keylogger feature.
	T1417.002	Input Capture: GUI Input Capture	It is able to get the shown UI.
	T1430	Location Tracking	It accesses the precise location of the device.
	T1636.002	Protected User Data: Call Log	It exports the device’s call logs.
	T1636.003	Protected User Data: Contact List	It exports the device’s contacts.
	T1636.004	Protected User Data: SMS Messages	It exfiltrates all the incoming OTP SMS messages.
	T1513	Screen Capture	Ability to capture the device screen.
Command	T1637	Dynamic Resolution	It receives the injected HTML payload endpoint dynamically

and Control			from the server.
	T1481.002	Web Service: Bidirectional Communication	It uses websocket communication to poll the TA's server and get the commands to execute.
Exfiltration	T1639.001	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	The stolen credentials are sent to a different C2.
Impact	T1516	Input Injection	It displays inject payloads like pattern lock and mimics banking apps login screen through overlay and steal credentials.
	T1582	SMS Control	It can read and send SMS.

Indicators of Compromise (IOCs)

The IOCs of this campaign can be found here.

Source: https://www.zimperium.com/blog/expanding-the-investigation-deep-dive-into-latest-trickmo-samples/