Cleafy | LABS

Medusa Reborn: A New Compact Variant Discovered

Technical Analysis

24.06.2024

TLP-WHITE

Key Points

- In May 2024, the Cleafy Threat Intelligence team tracked new fraud campaigns involving the Medusa (TangleBot) banking trojan, which had been under the radar for almost a year.

- Medusa is a sophisticated malware family with **RAT** capabilities discovered in 2020. Its features include a keylogger, screen controls, and the ability to read/write SMS. Those capabilities enable Threat Actors (TAs) to perform one of the riskiest fraud scenarios: **On-Device Fraud** (ODF).

- During these last months, it has been possible to identify some discrepancies between new Medusa samples and the previously known ones, including a **lightweight permission set** and **new features**, such as the ability to display a **full-screen overlay** and remotely **uninstall applications**.

- We identified **five** different **botnets** operated by several affiliates that show distinct characteristics regarding geographical targeting and decoy used. The results confirm previously known country targets, such as Turkey and Spain, but also new ones, such as **France and Italy**.

- We observed an apparent shift in the distribution strategy among the detected campaigns. TAs have started experimenting with "**droppers**" to distribute malware via fake update procedures.

Introduction

In late May 2024, Cleafy's Threat Intelligence team observed a surge in installations of a previously unknown app called "4K Sports," whose characteristics didn't perfectly align with known malware families.

Initial investigations suggested a possible connection between the behaviour of the "4K Sports" app and the **Medusa** family. However, a more in-depth analysis revealed discrepancies between the app and previously documented variants. These differences highlighted an evolution in the Medusa malware, with significant changes in its command structure and overall capabilities.

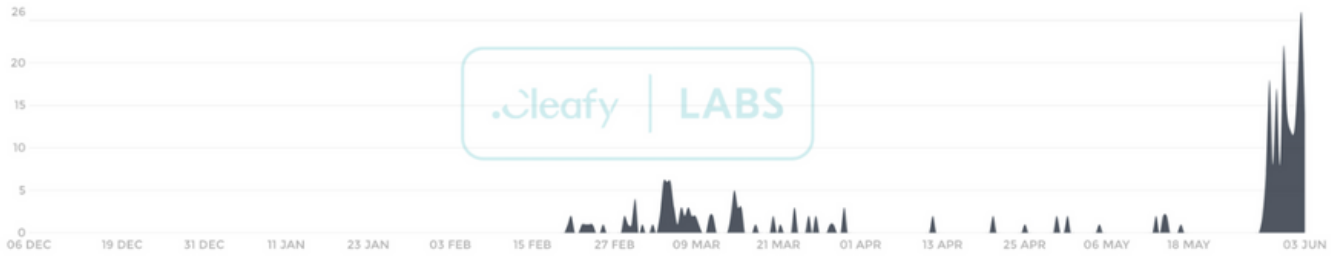

Figure 1 - Sports 4K Activities (Cleafy telemetries)

Analysing the evolution of Medusa samples over the past few months, it is clear that TAs aim to enhance the **efficiency** of the available features while simultaneously strengthening the botnet by **refactoring the permissions** required during the installation phase. Because of the MaaS (Malware-as-a-Service) model carried out by Medusa, this phase of "optimisation" could be influenced by various factors. The entry of new affiliates has likely driven developers to create **less detectable variants**, potentially to test their reliability in previously unexplored geographical regions.

In this article, we will uncover the details of our findings and understand the full scope of Medusa's evolution, the latest detected variant, and their implications.

Historical Overview

First identified in 2020, the Turkish-linked Medusa banking Trojan has grown on the world stage to become a significant threat. Initially targeting **Turkish financial institutions**, Medusa's scope expanded rapidly by 2022, launching major campaigns in **North America and Europe**.

This RAT (Remote Access Trojan) grants TAs complete control of compromised devices by exploiting VNC for real-time screen sharing and accessibility services for interaction. These capabilities provide TAs the ability to perform **On-Device Fraud** (ODF). ODF is one of the most dangerous types of banking fraud since wire transfers are initiated from the victim's device and can be adapted for manual or automatic approaches, such as Account Takeover (ATO) or Automatic Transfer System (ATS).

Figure 2 - VNC Service Routine

By exploiting accessibility services, Medusa extends its functionality beyond simple remote control. This allows the Trojan to automate several features commonly associated with modern banking Trojans, including continuous **Key-Logging** and **Dynamic Overlay Attacks**.

The following Figure represents a high-level overview of the network communications between an infected device (bot) and the assigned C2 infrastructure, taking the Key-Logging feature as an example:

Figure 3 - Key-logging in Action

The malware coordinates its functionalities through a **Web Secure Socket** connection to the TA's infrastructure. The C2 server URL is dynamically fetched from public social media profiles like Telegram, Twitter, and ICQ for enhanced obfuscation. This dynamic retrieval allows attackers to update the C2 server without modifying the malware, increasing its resilience against takedown attempts. Additionally, the malware employs backup channels on these social media platforms for further redundancy.

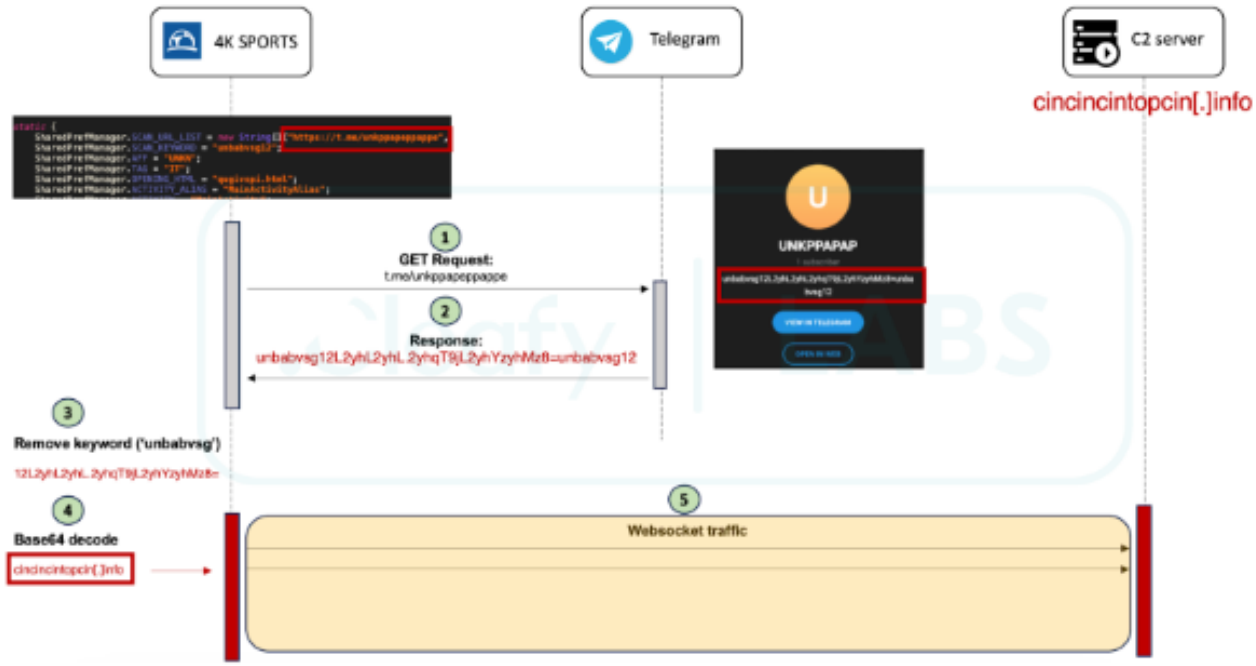

Figure 4 - C2 extracted from Social Media profiles (e.g., Telegram)

Recent Campaigns

Since **July 2023**, Medusa campaigns have been reborn with a **new variant**, changing TTPs and country targets. The following table represents all the high-level TTPs retrieved from recent analysis:

First evidence	July 2023
State	Active (June 2024)
Affected entities	Data not available
Targets	Android devices
Target countries	CA, ES, FR, IT, UK, US, TK
Infected chain	Social engineering (e.g., smishing) and Dropper -> Side-loading
Fraud scenario	On-device fraud (ODF)
Preferred cash-out	Data not available
Amount handled (per transfer)	Data not available

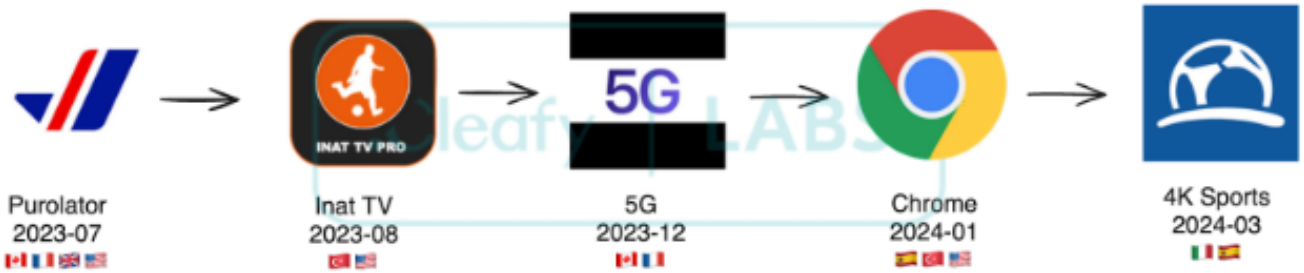

Figure 5 - Most used icons/names in recent Medusa campaigns

A characteristic of Medusa's campaigns has always been a high degree of **adaptability**: the malware's backend infrastructure is designed to support **multiple botnets** simultaneously, each differentiated by specific **tags** and operational **goals**.

This was confirmed in recent campaigns: Cleafy's investigations revealed five different active botnets, differing in the types of decoy used, distributional strategy, and geographical targets. In-depth analyses made it possible to obtain the identifiers of the botnets used by the affiliates, the countries targeted, and the decoys most frequently used in the campaigns:

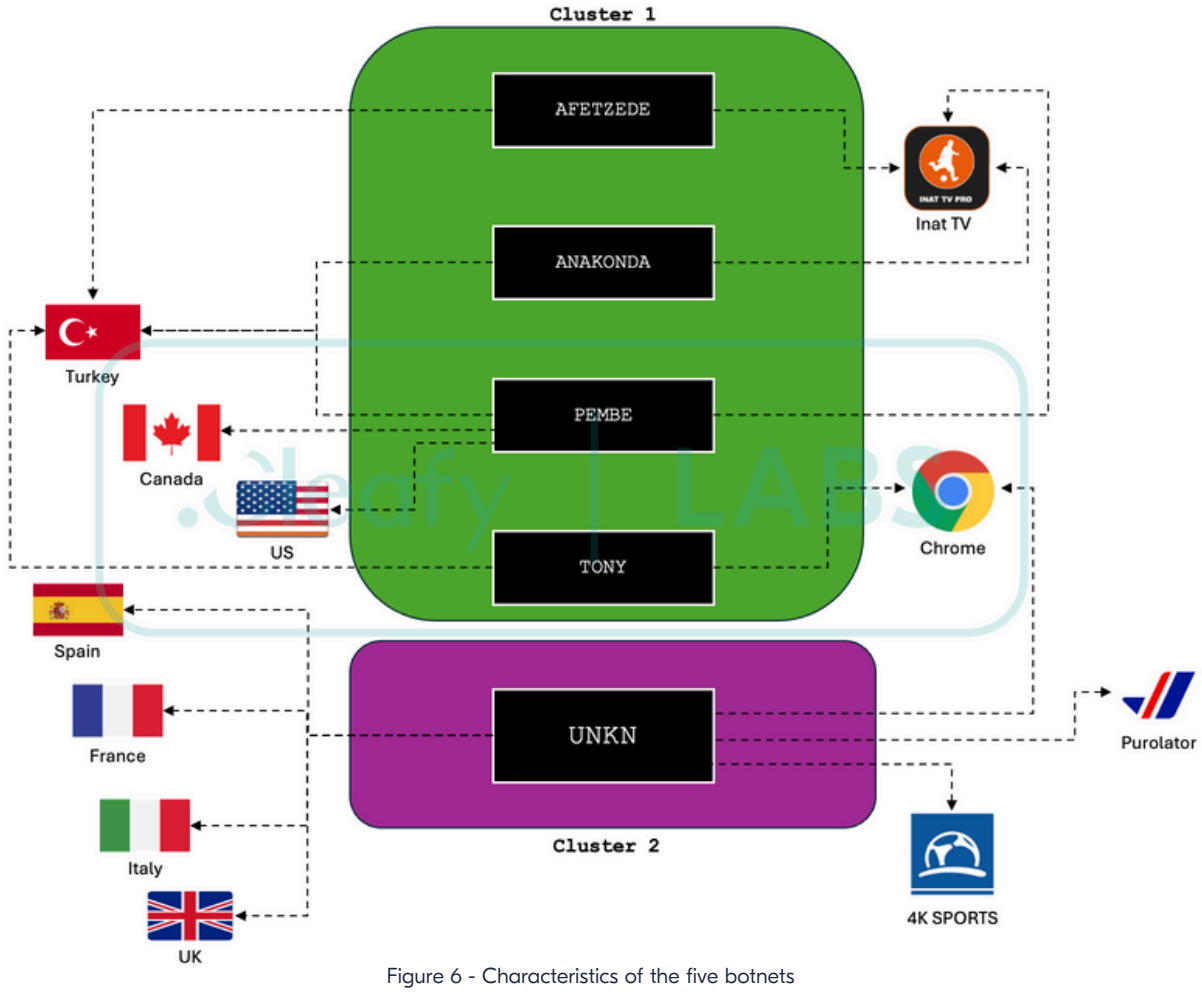

Figure 6 - Characteristics of the five botnets

Analysis revealed two distinct Medusa botnet clusters, each with different operational characteristics:

- **Cluster 1 (AFETZEDE, ANAKONDA, PEMBE, TONY):** these botnets primarily targeted users in Turkey, with some campaigns extending to Canada and the United States. They follow Medusa's traditional modus operandi, relying on methods like phishing campaigns to spread the malware. Interestingly, these variants often shared decoys, C2 servers, and campaign names, suggesting a potential connection to the same TAs.

- **Cluster 2 (UNKN):** this botnet marks a shift in Medusa's operational strategy. It mainly targets European users, with specific campaigns focusing on Italy and France. Unlike traditional variants, some instances of the innovative cluster were installed via droppers downloaded from untrusted sources. This suggests the TAs behind this botnet are **experimenting** with novel distribution methods beyond traditional phishing tactics.

Refer to the appendix for detailed information on botnet names, associated campaigns, dates, and decoy names.

One of the most intriguing aspects of these new campaigns is the strategic use of samples that employ a **lightweight permission set,** requiring only essential functionality for its core operations. Cleafy's investigations tracked the **evolution** of the permissions used over time for the most active botnets. As depicted in Figure 7, a negative trend was observed in all cases, especially in the botnets belonging to Cluster 1.

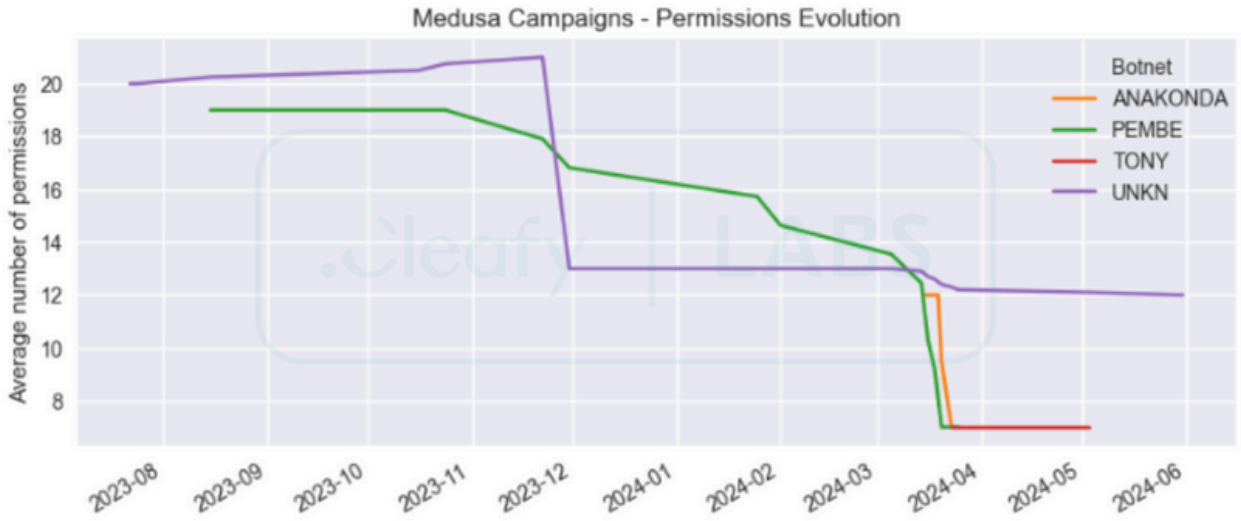

Figure 7 - Evolution of permission over time

From a Threat Intelligence and malware analysis perspective, examining the refactoring of permissions at the Manifest level is crucial. This analysis can reveal significant insights into the TTPs employed by TAs. **By reducing the number of permissions, the malware becomes less conspicuous during initial analysis**, potentially bypassing automated security checks and manual inspections. This stealthier approach can significantly lower detection rates, allowing the malware to persist undetected for extended periods.

This refactoring of permissions indicates that TAs continuously evolve their methodologies to stay ahead of detection technologies. By understanding these changes, security researchers and practitioners can better anticipate future threats and develop more effective countermeasures.

In-depth analyses of the early Medusa campaigns indicated the presence of valuable permissions to perform complementary malware functionality, such as:

- **Camera and Microphone**
- **GPS Location**
- **Phone Call**
- **Read and Send SMS**
- **Read Contacts**
- **Read Phone State**
- **Write Settings**

Instead, summarising all recent campaigns, we noticed that only permissions related to the malware's core functionality were requested. The minimum set of permissions is:

- **Accessibility Services**
- **Broadcast SMS**
- **Internet**
- **Foreground Service**
- **Query and Delete Packages**

The following Figure depicts a side-by-side comparison of the Android manifest files from early and recent Medusa campaigns. On the left, the manifest from an early Medusa campaign illustrates the extensive set of permissions requested. On the right, the manifest from a more recent Medusa campaign shows a streamlined permissions set.

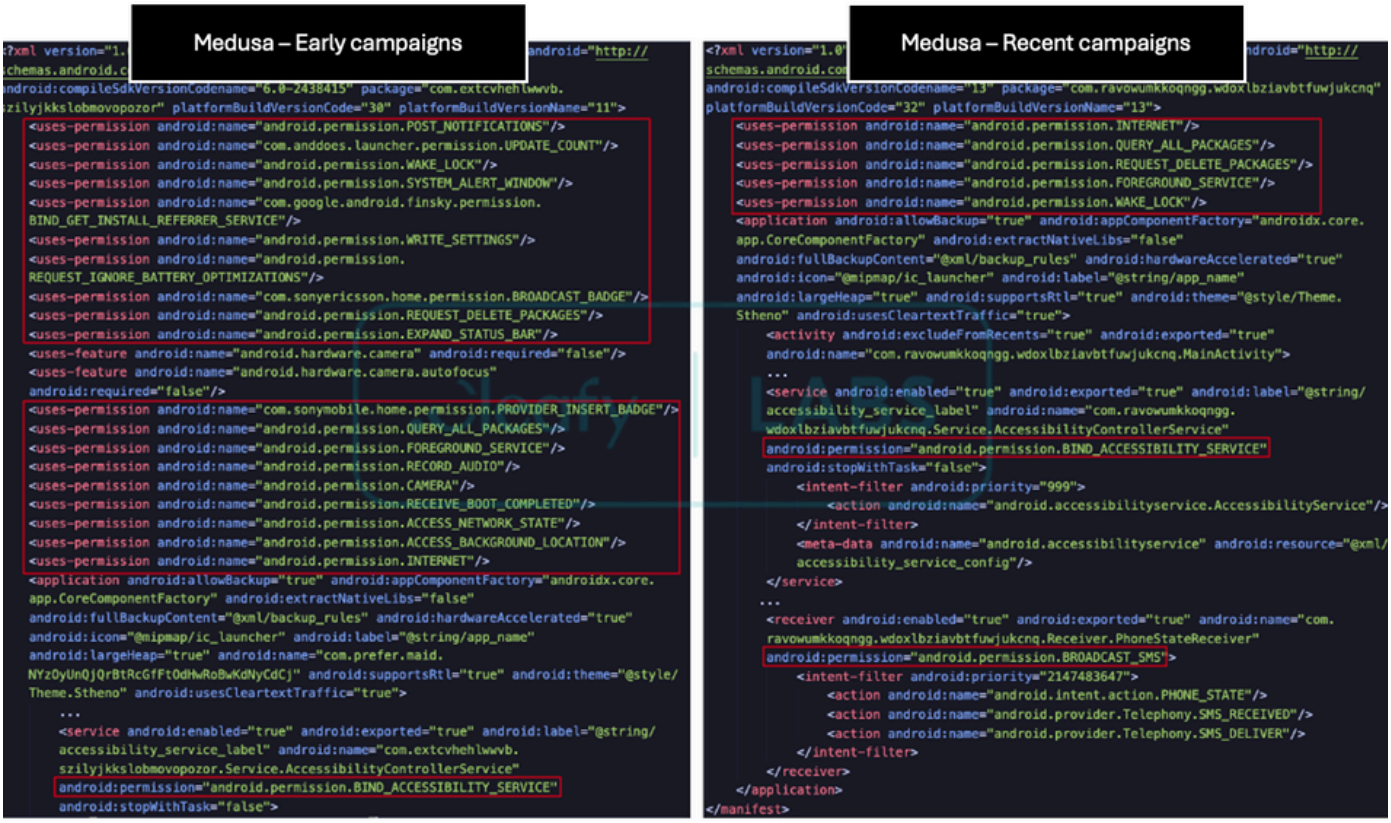

Figure 8 - Comparison of permissions required in early and recent campaigns

Capability Evolution

Cleafy's analysis revealed a significant change in the set of commands available in this new Medusa variant. Although the exact number of commands may vary, our investigation identified that 17 commands in the previous variant have been removed. This strategic reduction aligns with the earlier observed trend of minimising permissions in the manifest file, a move aimed at decreasing detectability and enhancing the overall stealth and reliability of the malware.

While many commands were removed, this new variant also introduces five new commands, showcasing an evolution in its capabilities:

Command	Description
destroyo	Uninstall Specific Application
permdrawover	Request Drawing Over Permission
setoverlay	Set Black Screen Overlay
take_scr	Take Screenshot
update_sec	Update User Secret

The removal of certain functionalities, alongside the introduction of these new commands, reflects a deliberate effort by the TAs to streamline Medusa's operations. By focusing on essential and more impactful features, they can ensure the malware remains effective while evading detection. This approach mirrors the earlier strategy of reducing the number of permissions requested during installation, further solidifying the botnet's robustness and adaptability.

In particular, commands like "**set overlay**" emphasise controlling the victim's device screen, facilitating more sophisticated phishing and social engineering attacks. This command allows the malware to **display a black screen overlay** on the victim's device. While the exact purpose remains under investigation, this functionality presents a potential threat: by obscuring the underlying screen content, the attacker can use this overlay to mask other malicious activities.

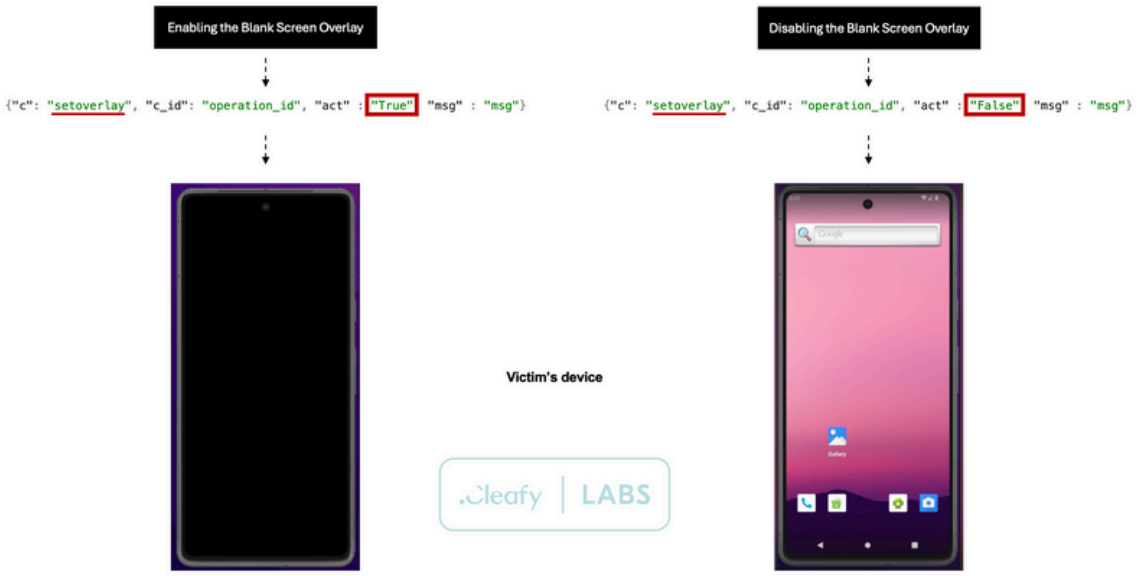

Figure 9 - Command "setoverlay" in action

Interestingly, **all the original functionalities have remained implemented** even in campaigns without associated **permissions**. For example, commands such as "**sendsms**" or "**getcontacts**" are present in all samples (also in the recent ones), but their execution is blocked by Android in the case of missing permissions.

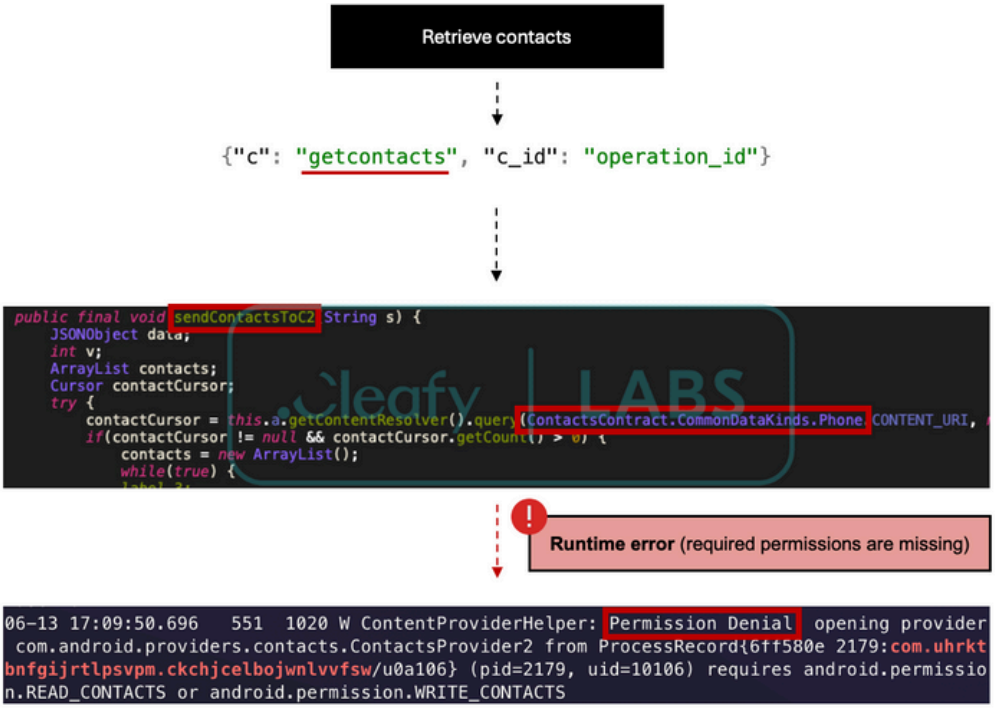

Figure 10 - Get Contacts Blocked

The following table shows the differences between the command sets of the previous version and those of the new version.

Medusa V2	Medusa V3
actallinj	-
actinj	
actpro	-
actvnc	
allsms	
bloapp	
blocall	-
blonot	-
blosms	-
call	
copyclip	
deactinj	
destroy	
-	destroyo
displaypro	-
endcall	-
fillfocus	
forcedisplaypro	-
getcontacts	
ghost	
hb	-
ini	
instapps	
keylog	
lockscr	
log	

Medusa V2	Medusa V3
mutesound	
permadmin	-
permbat	
-	permdrawover
permnotify	-
permperm	
permvnc	-
permwrite	
reg	
remjob	
remprot	
runapp	
sendpresms	-
sendsms	
setbright	
-	setoverlay
showalert	-
shownot	-
singlelock	
-	take_scr
tranot	-
trasms	
traussd	-
unbloapp	
-	update_sec
updateinfo	

Conclusion

In conclusion, the latest Medusa variant demonstrates a strategic shift towards a lightweight approach. Minimising the required permissions evades detection and appears more benign, enhancing its ability to operate undetected for extended periods. Geographically, the malware is expanding into new regions, such as Italy and France, indicating a deliberate effort to diversify its victim pool and broaden its attack surface.

The recent adoption of droppers as a distribution method signals a significant evolution in Medusa's threat capabilities. While we have yet to observe these droppers on the Google Play Store, this does not preclude the possibility of future deployments via this channel. This distribution strategy, shared among other banking malware families like TeaBot and SharkBot, leverages the inherent trust associated with official app stores, resulting in broader distribution and higher infection rates.

The combination of reduced permissions, geographical diversification, and sophisticated distribution methods underscores Medusa's evolving nature. As the TAs refine their tactics, cyber-security experts and anti-fraud analysts must stay vigilant and adapt their defences to counter these emerging threats. The detailed findings presented in this article offer valuable insights into Medusa's current state, providing a foundation for continued monitoring and analysis.

Appendix 1: Active campaigns

Botnet	Campaign	C2 URL	First Seen	App Name
PEMBE	Guncelke	a2a2a2a[.]life	2023-07-05	Aidat İadesi
	SONVERS		2023-07-31	Youtube Premium
	reklam		2023-08-08	Cimer Aidat İadesi
	reklam2		2023-08-15	İnat TV PRO Video Oynatici
	AvastV1		2023-09-25	Avast Premium
	17 Agustos reklami		2023-10-24	İnat TV Video Oynatici
	reklam 3		2023-10-24	İnat TV PRO
	propeller android	pemmbebebebebebe[.]info	2024-03-20	Android 14 Guncellemesi
	Mart19		2024-03-20	Inat Tv Video Oynatici
UNKN	PUROFR1	a4a4a4a[.]life	2023-07-22	Purolator
	TestTag		2023-07-22	Purolator
	PURO1		2023-07-22	Purolator
	FR-PURO		2023-07-22	Purolator
	FFPR	unkunknunkkkkk[.]info	2023-11-22	Purolator
	99-CHR		2024-01-25	Actualizacion de Chrome
	Lin-CHR		2024-02-01	Chrome
	FFPR	cincincintopcin[.]info	2024-03-05	Purolator
	IT		2024-05-31	4K Sports
AFETZEDE	ALEX-2	pembe1303sock[.]top	2024-03-14	İnat TV PRO
ANAKONDA	drop1	tony1303sock[.]top	2024-03-15	Inat Tv Video Oynaticisi
	inat1		2024-03-19	Inat Tv Video Oynaticisi
	22mart		2024-03-23	Inat Tv Video Oynaticisi
TONY	Chrome	tony1303sock[.]top	2024-03-23	Chrome Güncelleme
	Chrome	baahhhs21[.]info	2024-05-03	Chrome Güncelleme

Appendix 2: Indicator of Compromise (IoC)

Medusa Variant

C2 URL	App Name	MD5
cincincintopcin[.]info	4K Sport	b9ee66c96b110622f4608581e77b0e4d
	5G	7031c88ea3a306c4e4d786d3b0625a20
	Purolator	432cd820424c1a9ae0abac63a4f130c7
		ae53e2d732523c460d31e2805989e480
		c6153acefb8d3724f7defc177cff9ca9
		db097d837681d059a63725bc4ad93515
tonymayisayininfilancagunu[.]info	Inat Tv Video Oynaticisi	1db5ce9cbb3932ce2e11e5b3cd900ee2
		811bcc33027f3784d800e75dea81f277
tonyttnnntnn1704[.]top	Inat Tv Video Oynaticisi	97abc0aa3819e161ca1f7f3e78025e15
		8468c1cda925021ed911fd9c17915eec
a6a6a6a6a6a6a6[.]info	-	-
pembe1303sock[.]top	Chrome	fb3d3bdc13f445df3f4dd55f547aa92a
		b6bbf8ed1cf8ec67b25bbcf26de483b4
		1ed0d97491afd5c2d27f74f18e254cc3
	İnat TV PRO	469dfea6446a8bb5fada116bd28483d7
pembemayisayininfilancazamani[.]info	-	-
pemmbebebebebebe[.]info	Chrome	62faff68d6e3957973e91810a0abf166
	Android 14 Guncellemesi	e501752247d32e908e4db70f457ced42
	Inat Tv Video Oynatici	bbecdd2513981eb9573b163151747e3b
		08344a2575efed552f2688b371ebac67
baahhhs21[.]info	Chrome Güncelleme	185f8c23fd680cae560aad220e137886
bimtambir[.]top	-	-
tony1303sock[.]top	Chrome Güncelleme	3b7df8e68eca9a4bcc559d79a2c5a4c7
		6b05a1e9faf5b77bad1826bacf322b24
	Inat Tv Video Oynaticisi	4c12987ac5d56a35258b3b7cdc87f038
		3fbe1323bdef176a6011a534e15a80f0
		0e7c37e28871f439539b3d87242def55
		646077aaf1ced1b32ae6519beced080f
		8d232fd0bfc9e1e4e77b8d719f24b48f
		d98386401edf18ddbf45a40febf80c40

Appendix 2: Indicator of Compromise (IoC)

C2 URL	App Name	MD5
topisbim[.]top	-	-
tonyyyyyyyyyy[.]info	-	-
unkunknunkkkkk[.]info	Chrome	5a807cb36fdb3eaa50004351cb83a348
	Purolator	3ccb77a10497a32efcaa42ac646ca6cf
		da92fc812b84137cef1571fb6c0285f0
		2fb098a1868c7162aff9aa84fcc45071
		ac7741bca86793d28659b358f734a65e
		e8ab402124e19af08d5ddc924d463991
		e65f01591ae40802748b09f9964bc61e
	Google Chrome	8a4928ac9089adc4a153741d2f1c784a
	5G	cffad0170fc13756cab142d3989c26a9
	Actualizacion de Chrome	29dd2f61f1d402ab46d963ed25c591d5
		a6157e3e5e1aef93ae71b3cff3ec9d80
a2a2a2a[.]life	İnat TV Video Oynatici	2ecce74a26fe3f76252d0fc29cdc3ed3
		b9f3782c3d6034cdd12b6854e49b5fcf
		2a94a9157e7cb3259531cfb1bf9f1f83
		25139a3dde2d6b9ded29de97452a8774
		9437ea7aa931bfed9e6cdd76fe27d811
	İnat TV PRO	b2ae7eb30163c8b004dc354ebb973e49
	İnat TV PRO Video Oynatici	df29a4a16af5da6e24aa3361b204a664
		5d3958940abab05acee4b9dbab6bc4c3
	Dilan Polat Resimleri	0f83a144483ba17f4e3154d717361381
	Cimer Aidat İadesi	59735a4123c664f1795fb7154c95af67
		920bdb47c0c060ecc5a06461c9715e26
	Avast Premium	3dac7bb95b01676d24cb194c3c47029f
	Youtube Premium	d8e8eb2714c91b9968ffd409f771e7e1
	Aidat İadesi	53970ff7dd8edaec7fc0cdd030c0b038
		e69248a7308436d8c6dde803c22821cb
a4a4a4a[.]life	Purolator	cb1280f6e63e4908d52b5bee6f65ec63
		a5aeb6ccc48fea88cf6c6bcc69940f8a
		bd7b9dd5ca8c414ff2c4744df41e7031
		9ceef4129ea27388018c0d1bb8554bcc
		3e0ee083fa9fce493383d75db1c69eee
		776b5b3c18a10b7e04f238478408f057
		4bace6e0b61f5169bb0ca7f48c38aea2
		c9f30775469ef4ba09b1c09fdb13fd2d
		2580f696f903b11f4ca06754fa82b5a7
		dbf7b5f6faeacbed7adb0880d50380b4
		f7deb4066b016df32e8cd47b7ad44225
		02c7e63ffa0c5488dd080b64bc297852

Appendix 3: Social Media Profile

Social URL	Target Apps
icq[.]im/AoLH58pXY8ejJTQiWg8	Inat TV, Avast
icq[.]im/AoLH58xYS0_leBOpXFI	4K Sports, Purolator, Chrome
icq[.]im/AoLH5bRXfAE6eCtbwIl	Inat TV
t[.]me/anbsh26	Inat TV
t[.]me/anbshaa	Inat TV
t[.]me/anbshbb	Inat TV
t[.]me/bntonal23	Chrome
t[.]me/kalnbsb	Chrome
t[.]me/pempeppepepep	Inat TV, Avast
t[.]me/unk22k2k2k2	4K Sports, Purolator, Chrome
t[.]me/unkppapeppappe	4K Sports, Purolator, Chrome
t[.]me/utabsg23	Chrome
t[.]me/xpembeppep2p2	Inat TV, Avast
icq[.]im/AoLH58pXY8ejJTQiWg8	Inat TV, Avast
icq[.]im/AoLH58xYS0_leBOpXFI	4K Sports, Purolator, Chrome
icq[.]im/AoLH5bRXfAE6eCtbwIl	Inat TV
t[.]me/anbsh26	Inat TV
t[.]me/anbshaa	Inat TV
t[.]me/anbshbb	Inat TV
t[.]me/bntonal23	Chrome
t[.]me/kalnbsb	Chrome
t[.]me/pempeppepepep	Inat TV, Avast
t[.]me/unk22k2k2k2	4K Sports, Purolator, Chrome
t[.]me/unkppapeppappe	4K Sports, Purolator, Chrome
t[.]me/utabsg23	Chrome
t[.]me/xpembeppep2p2	Inat TV, Avast
icq[.]im/AoLH58pXY8ejJTQiWg8	Inat TV, Avast
icq[.]im/AoLH58xYS0_leBOpXFI	4K Sports, Purolator, Chrome
icq[.]im/AoLH5bRXfAE6eCtbwIl	Inat TV
t[.]me/anbsh26	Inat TV
t[.]me/anbshaa	Inat TV
t[.]me/anbshbb	Inat TV
t[.]me/bntonal23	Chrome
t[.]me/kalnbsb	Chrome
t[.]me/pempeppepepep	Inat TV, Avast
t[.]me/unk22k2k2k2	4K Sports, Purolator, Chrome
t[.]me/unkppapeppappe	4K Sports, Purolator, Chrome
t[.]me/utabsg23	Chrome
t[.]me/xpembeppep2p2	Inat TV, Avast
icq[.]im/AoLH58pXY8ejJTQiWg8	Inat TV, Avast
t[.]me/zedezededeed	Inat TV
twitter[.]com/doplghas	Inat TV

Appendix 4: Dropper

Package Name	Target App
appcodetest.stufioa.sporrrtv	4K Sports
bvxba.poiuytt.nbbvcf	4K Sports
cvxb.dhshuw.xnxbxvvxvxvxvxvxhzhs	4K Sports
hxbx.cisisis.sjsusus	4K Sports
getm.psks.sjshxh	4K Sports
gsgs.pwow.mpow	4K Sports
sportvv.iptvon.tvlock	4K Sports
vczbz.sksjs.fieoe	4K Sports
vontoner.pontoner.montoner	4K Sports
vxnxn.oeiue.dhow	4K Sports

Cleafy | LABS

Be the first to get full technical reports of new Threats

Cleafy LABS bulletins series help you stay ahead of cybercriminals by giving you prompt access to deep technical analysis of new threats.

The threats are the ones newly discovered by our best-in-class Threat Intelligence team.
With each bulletin, you will be among the first people worldwide to receive a comprehensive technical report on the new threat.

You'll get detailed information, such as:
- Threat's main features
- Patterns of attacks
- Relevant Screenshots of the compromised mobile/web app
- Snippets of malicious code
- Geographical distribution of the attack
- List of malware commands
- List of IOC's

SUBSCRIBE


Cleafy
LABS