Cerberus RAT: Android malware's dark legacy in 2025

By Norman G.

Published: 2025-06-27 · Archived: 2026-04-05 20:56:15 UTC

In 2020, Cerberus RAT made headlines as one of the most sophisticated Android banking trojans ever seen. In 2025, its shadow still looms.

Originally distributed as a Malware-as-a-Service (MaaS), Cerberus could steal banking credentials, hijack two-factor authentication, and give attackers full remote control over Android devices—all while evading detection. It didn't just compromise personal devices; it redefined mobile threat tactics for years to come.

While Cerberus itself is no longer active, its leaked source code gave rise to a new generation of Android malware—Alien, Hook, Octo, and other Cerberus-class threats—that continue to target users today with even more advanced capabilities. Many of these threats are based on the original Cerberus code, which has been retooled by cybercriminals to create new banking trojans such as Alien, ERMAC, and Phoenix, highlighting the ongoing risks posed to Android users by these evolving malware variants.

These remote access trojans (RATs) exploit Android's accessibility features, mimic legitimate apps, and silently drain credentials, messages, and control from infected devices.

This article explores the evolution of Cerberus, its impact on today's threat landscape, and what IT and security teams must do in 2025 to protect their organizations from mobile malware built on its legacy.

TL;DR: What You Need to Know About Cerberus RAT in 2025

- **Cerberus** was a powerful Android banking trojan active in 2019–2020.
- It gave attackers full remote access, 2FA bypass, keylogging, and phishing via overlays.
- After its **source code leaked**, malware like **Alien, Hook, and Octo** emerged using its code.
- These Cerberus-based threats are still **active in 2025**, targeting finance, crypto, and sensitive user data.
- **IT teams must act**: deploy mobile threat defense (MTD), restrict Accessibility Services, and train users.
- Cerberus may be gone—but its **legacy still endangers Android devices worldwide**.

What is Cerberus RAT?

Cerberus RAT is a sophisticated type of Android malware known as a remote access trojan (RAT). First discovered in 2019, Cerberus was designed to give attackers full control over infected Android devices while stealing sensitive data through a combination of keylogging, screen recording, and overlay attacks.

At its core, Cerberus is also a banking trojan, built to intercept login credentials, hijack SMS-based two-factor authentication (2FA), and extract financial data from banking and cryptocurrency apps. Cerberus delivers a banking trojan payload designed to perform malicious activities, such as stealing login credentials and targeting financial applications, by performing malicious actions and other malicious activities on infected devices.

It abuses Android's Accessibility Services to escalate privileges, evade detection, and persist on devices.

Unlike traditional RATs used on desktops—such as those operating via tools like VNC or TeamViewer—Cerberus was built specifically for mobile environments, with features tailored to Android's architecture. It could even initiate its own TeamViewer session on a victim's phone to grant attackers real-time control—without any user interaction.

Although the original Cerberus operation shut down in 2020, its leaked source code continues to fuel modern Android malware strains like Alien, Hook, and Octo, making its threat legacy very much alive in 2025.

The rise of Android banking malware

As mobile banking adoption skyrocketed over the past decade, so did the interest of cybercriminals in targeting smartphones—especially those running the Android operating system. With millions of users now relying on mobile apps to manage finances, pay bills, and access digital wallets, Android banking malware has become one of the fastest-growing threats in the cybersecurity landscape.

Android's popularity—combined with its open ecosystem and widespread use of third-party app stores—has made it the #1 target for mobile-focused attacks. Threat actors take advantage of the platform's flexibility to distribute malicious APKs, disguise trojans as a legitimate app, and exploit Android's Accessibility Services to gain deeper device control. These malicious apps often specifically target banking apps and are designed to deceive Android users by mimicking the appearance of a legitimate app, making it difficult for users to distinguish between a real and a fake application.

Notable banking trojans such as Anubis, Hydra, Ginp, and Gustuff have dominated mobile threat reports for years. These malware families are capable of stealing login credentials, intercepting SMS codes, and initiating unauthorized transactions. Among them, Cerberus stood out for its advanced remote access capabilities, stealth persistence, and for laying the groundwork for even more dangerous successors like Alien and Hook.

As the mobile threat landscape evolves, banking trojans have become more modular, evasive, and commercialized—posing a growing risk to both individual users and corporate mobile fleets.

Cerberus RAT: core capabilities and infection strategy

Cerberus is not your average Android malware. As an advanced Android remote access trojan (RAT), it was designed with powerful surveillance and credential theft features—turning infected smartphones into fully controllable tools for cybercriminals.

Once installed, Cerberus RAT infiltrates deeply into the Android system by abusing Accessibility Services, allowing it to bypass user permissions and automate interactions without detection. After infection, the compromised device can have its device settings manipulated to facilitate further malicious actions, maintaining persistence and control over the infected device. This opens the door to a wide range of malicious capabilities:

Core capabilities of Cerberus RAT

- Keylogging: Captures every keystroke entered on the device, including passwords, personal data, and messages.
- SMS Forwarding & Interception: Hijacks SMS messages, including one-time passwords (OTPs), enabling bypass of SMS-based 2FA.
- Google Authenticator Code Theft: Extracts time-based authentication codes by capturing screen content or accessing protected UI elements.
- Screen Capture: Captures and transmits screen images using virtual network computing (VNC) techniques, allowing attackers to view and control the device remotely. Cerberus leverages MediaProjection APIs to send screen images or videos, enabling remote access and manipulation of the device.
- TeamViewer Injection: Deploys a silent TeamViewer session to allow full remote control of the device, without the user's knowledge.
- Overlay Attacks: Uses fake login screens (overlays) to trick users into entering banking credentials, credit card details, or email passwords. Cerberus can execute overlay attacks by exploiting accessibility services and integrating VNC-based remote control capabilities.
- Accessibility Services Abuse: Grants itself elevated permissions, disables Google Play Protect, and prevents uninstallation attempts.
- Device Persistence & Evasion: Cerberus hides its icon, deletes traces, disables security tools, and evades detection by antivirus and Google Play Protect by checking for emulator environments and security apps.

This combination of features allows Cerberus to remain hidden, maintain control, and extract valuable data over time—without triggering suspicion from users or common mobile security tools.

Cerberus in the Play Store: The *Calculadora de Moneda* Case

Even the official Google Play Store—considered a trusted source for Android apps—hasn't been immune to Cerberus RAT's infiltration. One of the most revealing incidents involved a seemingly harmless app named "Calculadora de Moneda" (Currency Calculator), which managed to bypass Google Play Protect and infect users in Spain.

The infection process typically involved several steps: the app first acted as a dropper, downloading additional components, such as native libraries and encrypted payloads, onto the device. It then established dynamic communication with its command and control servers, sometimes using domain generation algorithms to avoid detection and maintain persistence. This multi-stage approach represents a sophisticated infection chain designed to evade detection and ensure successful deployment of the malware.

How it happened

Initially, the app behaved exactly like a legitimate currency converter. But hidden deep in the APK was a dormant Cerberus payload—designed to "hibernate" until it received instructions from a remote command-and-control (C2) server.

Once activated, the app triggered a staged malware drop:

1. It connected silently to a C2 server.
2. The server instructed the app to download a second, malicious APK.

3. That APK contained the full Cerberus RAT malware, which then embedded itself into the Android system.

The infection process required no user interaction beyond the initial app installation—and even Play Protect failed to catch it.

Why this matters

- Hibernation and delayed execution are increasingly common tactics in Android malware. They help malicious apps fly under the radar during initial security scans.
- Staged delivery allows attackers to embed only “clean” code in the first submission, then deploy the malicious code later—once the app is already published.
- The incident shows how threat actors are exploiting trust in official app stores to distribute remote access trojans to unsuspecting users.

This case is a sobering reminder that Android malware can still reach users via trusted sources, and why even "safe-looking" apps must be approached with caution.

The source code leak that changed everything

Cerberus wasn’t just dangerous because of its features — it became a cybersecurity nightmare the moment its source code was leaked into the wild.

This leak opened the gates to a flood of clones and derivatives, as threat actors began leveraging the Cerberus codebase to develop new banking Trojan variants such as Alien, ERMAC, and Phoenix. However, these variants were not considered entirely new malware, since they were all based on the original Cerberus code rather than being fresh, original creations.

Collapse of the Original Cerberus Operation

By mid-2020, cracks were showing in Cerberus’ development team. Internal disputes and stagnating sales of their malware-as-a-service (MaaS) platform led the developers to shut down the operation and auction the entire Cerberus toolkit — including the malware code, admin panel, command & control server, and client interface.

Despite the offer being packed with powerful tools and an existing user base, the auction failed to attract serious buyers. Cybercriminals were hesitant to pay thousands of dollars for a project that appeared to be reaching its end

of life.

Source code hits the underground

What happened next changed the Android malware landscape.

Frustrated by the failed sale, the Cerberus operators leaked the full source code for free on underground forums. This included:

- The Android trojan's APK code
- Backend control infrastructure
- Documentation and configuration files
- Malware modules for keylogging, overlay attacks, SMS forwarding, and more

This leak opened the gates to a flood of clones and derivatives—many developed by less skilled but highly motivated actors.

The aftermath: A malware mutation wave

With the code now public:

- New variants like Alien emerged, borrowing heavily from Cerberus' framework.
- Junior threat actors with minimal experience began spinning up their own malware operations, using Cerberus as a plug-and-play kit.
- Security teams worldwide saw a spike in Cerberus-like activity, complicating detection and remediation efforts.
- Antivirus evasion improved, as cloned versions mutated the codebase just enough to bypass standard detection.

What began as a single MaaS threat had now become an open-source foundation for Android financial malware.

Key takeaway: The Cerberus source code leak democratized access to advanced mobile RAT techniques, ushering in a new wave of Android threats that remain active today.

The Evolution of Cerberus RAT: Timeline from 2019 to 2025

2019 – The Birth of Cerberus RAT

Cerberus is first identified as a banking trojan and Remote Access Trojan (RAT) for Android. Sold as a Malware-as-a-Service (MaaS), it offers credential theft, screen recording, 2FA interception, and full remote control capabilities.

Early 2020 – Expansion into Google Play

Trojanized apps using Cerberus code are discovered in the Google Play Store. Attackers deploy multi-stage payloads to bypass Play Protect, activating malicious features post-installation.

Mid-2020 – Cerberus Source Code Leaked

Following internal developer disputes, Cerberus's full source code leaks on hacker forums. The release includes its builder, admin panel, and C2 logic—enabling widespread cloning and modification.

Sources: BleepingComputer, BankInfoSecurity

Late 2020 – The Rise of Alien Trojan

Alien malware emerges as a direct fork of Cerberus, with added capabilities like remote shell execution and improved obfuscation. It becomes more prevalent in LATAM and Europe.

2021 – Proliferation of Cerberus Variants

Leaked code spawns hybrid trojans combining Cerberus with other malware like Anubis. These clones target crypto apps and QR scanners using accessibility abuse and 2FA interception.

2022 – Integration into Custom RAT Kits

Cerberus modules are sold via Telegram and dark web markets as part of modular Android malware kits. These kits are used in attacks on fintech and retail apps.

2023 – Link to Hook and Octo Trojans

Hook and Octo Android RATs emerge, displaying core traits from Cerberus and Alien. Features include real-time screen streaming, file theft, and enhanced overlay attacks.

2024 – Detection Improves, Legacy Lives On

Mobile security tools improve at detecting Cerberus-based behavior through sandboxing and behavioral analysis. Cerberus remains foundational in training AI malware detection models.

2025 – Cerberus-Class Threats Still Circulating

Malware like Teabot, Xenomorph, and BrasDex still reuse Cerberus techniques such as overlay injection and screen capture. Its legacy continues in new variants across Android’s threat landscape.

Sources: MITRE ATT&CK, Cyware, WeLiveSecurity, Digital Shadows, CERT-EU

From Cerberus to Alien and beyond: how Alien became Cerberus’s successor

Alien and Hook are direct successors of the Cerberus banking trojan, with the Cerberus Android banking trojan serving as the foundation for these new threats. The Cerberus Android banking trojan was widely used in malicious campaigns, and after its source code leak, it led to the emergence of new banking trojans like Alien and Hook.

Feature	Cerberus	Alien	Hook
Remote Access (RAT)	Yes	Yes	Yes (enhanced)
Keylogging	Yes	Yes	Yes
Overlay Attacks	Yes	Yes (226 apps)	Yes
Google Authenticator Theft	Yes	Yes	Yes
TeamViewer Injection	Yes	Yes	No
2FA Bypass	Yes (SMS & OTP)	Yes (OTP)	Yes (OTP interception)
Play Protect Evasion	Yes (via staged payloads)	Yes	Yes (root detection bypass)
App List & File Access	Yes	Yes	Yes
Distribution Method	MaaS / Google Play	Dark Web Forums	Telegram & Dark Web
Active Development	No (source leaked)	No (Cerberus fork)	Yes

What Cerberus means for IT teams in 2025

The Cerberus RAT may have faded from the malware spotlight, but its tactics are far from gone. In fact, they've become the foundation for today's most dangerous Android malware variants.

Modern threats targeting mobile devices now build upon the core techniques pioneered by Cerberus—making it a blueprint for a new era of Android banking trojans and Remote Access Trojans (RATs). For IT and security teams, this means that mobile devices remain one of the most exploitable endpoints in the enterprise attack surface. Cerberus-based malware continues to enable financial fraud and increases the risk of data breach for organizations and individuals, leading to significant financial and reputational consequences.

Current threat trends influenced by Cerberus:

- Modular Android RAT kits that let attackers customize payloads on demand
- Banking trojan-as-a-service (BTaaS) business models on the dark web
- Abuse of mobile accessibility services for screen hijacking and data theft
- Remote control malware capable of defeating MFA and security apps
- Bypassing traditional endpoint protection tools, even on updated devices

Despite its original source code leak in 2020, Cerberus remains relevant—especially as threat actors continue to fork and evolve its features under new names like Alien, Hook, and Octo. For IT teams, understanding Cerberus is crucial to anticipating what's next.

How to detect, prevent and respond to Cerberus-class threats

Cerberus and its successors exploit weaknesses in mobile device security—especially when those devices operate outside of MDM or corporate control. The good news? There are concrete, proactive steps IT teams can take to stay ahead. While antivirus software and security researchers play a crucial role in identifying and mitigating threats, human error remains a significant factor in successful malware infections.

Mobile security best practices:

1. Conduct regular mobile risk assessments: Identify unprotected devices, outdated software, and high-risk user behaviors.
2. Audit Accessibility Service permissions: Cerberus-class malware often abuses accessibility features—review and restrict them.
3. Restrict sideloaded APKs: Disable sideloading or enforce MDM policies to limit unverified app installs.
4. Deploy Mobile Threat Defense (MTD) tools: MTD platforms offer behavioral monitoring, anomaly detection, and zero-day threat prevention.
5. Patch operating systems and apps: Keep Android OS and key applications up to date to close known security gaps.
6. Enable Google Play Protect (but don’t rely on it alone): It's a good baseline, but attackers have found ways to bypass it.
7. Train users to recognize fake apps and phishing tactics: Awareness is your first line of defense—users must understand the risks of granting excessive permissions.

FAQs: Cerberus malware & mobile threats in 2025

What is Cerberus RAT?

Cerberus is an advanced Android banking trojan with Remote Access Trojan (RAT) capabilities. It steals banking credentials using overlay attacks, keylogging, and by abusing Android Accessibility Services to take full control of infected devices.

How did Cerberus spread?

Originally offered as malware-as-a-service (MaaS), Cerberus was distributed through phishing campaigns and malicious apps, including at least one case on the official Google Play Store disguised as a currency calculator.

Is Cerberus still active in 2025?

The original Cerberus malware is no longer active, but its leaked source code led to the rise of new variants like Alien, Hook, Octo, and others. These threats still use Cerberus-inspired techniques to target Android devices.

What makes Cerberus dangerous?

Cerberus could remotely control infected phones, log keystrokes, steal SMS and 2FA codes, and even hijack Google Authenticator—all while remaining hidden from users and antivirus tools.

How can I protect my device from Cerberus-like malware?

Avoid sideloading apps, restrict Accessibility permissions, use a mobile threat defense (MTD) solution, and stay up to date with OS and app security patches. IT teams should also educate users about mobile phishing and fake apps.

Conclusion: Cerberus may be gone, but its legacy lives on

Cerberus was a wake-up call for Android security—a trojan that combined traditional RAT techniques with modern mobile attack vectors. But its biggest impact came after its fall.

By leaking its source code, Cerberus didn't just disappear—it multiplied. It enabled a wave of new Android malware strains that still haunt the mobile landscape in 2025, from Alien to Hook and beyond. These threats are faster, stealthier, and more customizable than ever.

For IT teams and CISOs, this is a call to action:
Cerberus-class threats are no longer rare—they're the standard. Defending against them requires a layered approach that includes user training, proactive mobile threat monitoring, and security policies that adapt as fast as the malware does.

Because the next RAT won't knock—it will sneak in quietly, just like Cerberus did.

Source: https://preyproject.com/blog/en/cerberus-and-alien-the-malware-that-has-put-android-in-a-tight-spot/