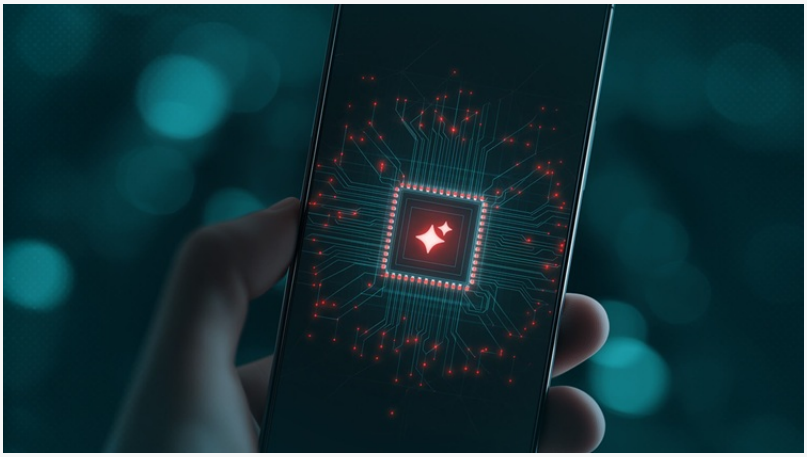
ESET Research discovers PromptSpy, the first Android threat to use generative AI



DUBAI , DUBAI, UNITED ARAB EMIRATES, February 23, 2026 /EINPresswire.com/ -- ESET researchers have discovered PromptSpy, the first known Android malware to abuse generative AI in its execution flow to achieve persistence. It is the first time generative AI has been deployed in this manner. Because the attackers rely on prompting an AI model (specifically, Google's Gemini) to guide malicious UI manipulation, ESET has named this family PromptSpy. The malware can capture lockscreen data, block uninstallation attempts, gather device info, take screenshots, record screen activity as video, and more. This is the second AI-powered malware that ESET Research has discovered, following PromptLock in August 2025, the first known case of AI-driven ransomware.

Based on language localization clues and the distribution vectors observed during analysis, this campaign appears to be financially motivated and seems to primarily target users in Argentina. However, PromptSpy has not been observed in ESET telemetry yet, possibly making it a proof of concept.

While generative AI is deployed only in a relatively minor part of PromptSpy's code — the one responsible for achieving persistence — it still has a significant impact on the malware's adaptability. Specifically, Gemini is used to provide PromptSpy with step-by-step instructions on how to make the malicious app "locked", i.e. pinned, in the recent apps list (often represented by a padlock icon in the multitasking view of many Android launchers), thus preventing it from being easily swiped away or killed by the system. The AI model and prompt are predefined in the code and cannot be changed.

"Since Android malware often relies on UI-based navigation, leveraging generative AI enables threat actors to adapt to more or less any device, layout, or operation system version, which can greatly increase the pool of potential victims," says ESET researcher Lukáš Štefanko, who discovered PromptSpy. "The main purpose of PromptSpy is to deploy a built-in VNC module,

giving operators remote access to the victim's device. This Android malware also abuses Accessibility Services to block uninstallation with invisible overlays, captures lockscreen data, and records screen activity as video. It communicates with its Command & Control server via AES encryption," adds Štefanko.

PromptSpy is distributed by a dedicated website and has never been available on Google Play. As an App Defense Alliance partner, ESET nevertheless shared the findings with Google. Android users are automatically protected against known versions of this malware by Google Play Protect, which is enabled by default on Android devices with Google Play Services.

"Even though PromptSpy uses Gemini in just one of its features, it still demonstrates how implementing these tools can make malware more dynamic, giving threat actors ways to automate actions that would normally be more difficult with traditional scripting," says Štefanko.

With the app's name being MorganArg and its icon seemingly inspired by Morgan Chase, the malware is likely impersonating the Morgan Chase bank. MorganArg, likely a shorthand for "Morgan Argentina", also appears as the name of the cached website, suggesting a regional targeting focus.

Because PromptSpy blocks uninstallation by overlaying invisible elements on the screen, the only way for a victim to remove it is to reboot the device into Safe Mode, where third party apps are disabled and can be uninstalled normally. To enter Safe Mode, users should typically press and hold the power button, long press Power off, and confirm the Reboot to Safe Mode prompt (though the exact method may differ by device and manufacturer). Once the phone restarts in Safe Mode, the user can go to Settings Apps MorganArg and uninstall it without interference.

For a more detailed analysis of PromptSpy check out the latest ESET Research blogpost "PromptSpy ushers in the era of Android threats using GenAI" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner

network. For more information, visit ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
