MARCH 2025

VAPOR THREAT REPORT

IAS
INTEGRAL AD SCIENCE

EXECUTIVE SUMMARY

The IAS Threat Lab has uncovered an extensive and sophisticated ad fraud scheme leveraging fake Android apps to deploy endless and intrusive full-screen interstitial video ads. This fraudulent operation, codenamed **Vapor**, derives its name from its ability to 'evaporate' any real functionality from apps, leaving behind only intrusive ads. Vapor exploits unsuspecting users and ad networks on a massive scale, representing a highly organized and pervasive ad fraud scheme.

Threat Lab has identified over **180 app IDs** since early 2024 as part of the Vapor scheme, collectively amassing **over 56 million downloads** and generating over **200 million bid requests daily**, with no real functionality delivered to users.

Fraudsters behind the Vapor operation have created multiple developer accounts, each hosting only a handful of apps to distribute their operation and evade detection. This distributed setup ensures that the takedown of any single account would have minimal impact on the overall operation. Fraudsters have also incorporated a number of ad SDKs within their applications and set up corresponding seller accounts to monetize this traffic.

The IAS Threat Lab has actively worked to disrupt this fraudulent operation, collaborating with industry partners to minimize its impact. **As a result of our findings, Google has removed all identified apps from the Play Store**. Google Play Protect will warn users and automatically disable these apps, even when they originate from sources outside of Google Play. IAS continues to monitor the Vapor operation as threat actors adapt their tactics and as new apps are added to the scheme.

IAS partners are safeguarded against the impact of the Vapor threat through our fraud pre-bid avoidance solution available within their DSPs. Our advanced machine learning models power our fraud segments to ensure DSPs do not bid on impressions that originate from these apps.

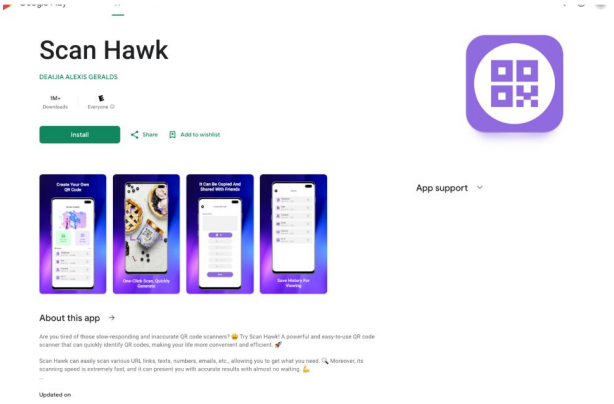
THE VAPOR THREAT: A COMPREHENSIVE ANALYSIS

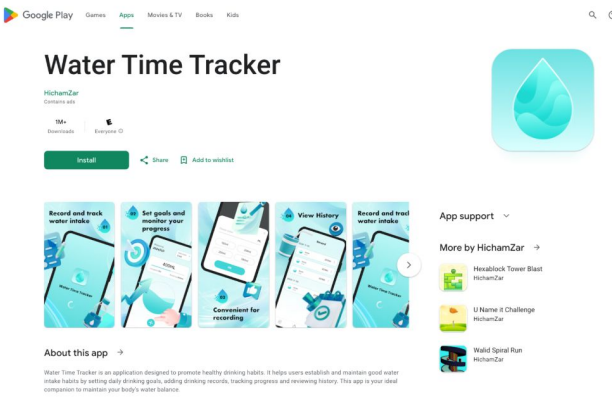
DESIGN OF VAPOR APPS

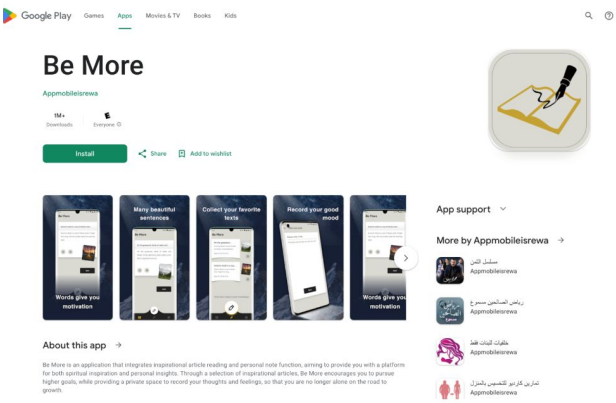
Vapor apps are strategically designed to mimic legitimate apps, blending into common and trusted categories such as utilities (e.g., QR scanners, password managers, flashlights), health and fitness apps (e.g., heart rate monitors, water trackers, weight trackers), and lifestyle applications (e.g., note-taking and motivational quote apps). These deceptive designs allow the apps to infiltrate user devices without raising suspicion, enabling fraudulent activities at scale.

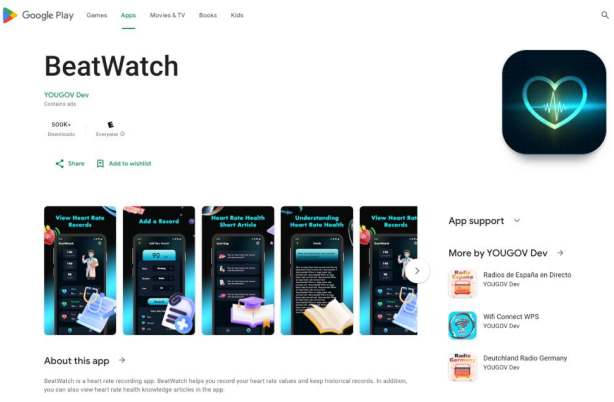
Version 1 of these apps were introduced into Google Play as functional applications. However, subsequent updates removed legitimate functionality, replacing it with tactics to maximize ad revenue through full-screen interstitial video ads. These intrusive ads completely removed app launch icons and visible UI elements at the expense of deteriorating user experience.

Examples of Vapor apps accessible on Google Play Store:









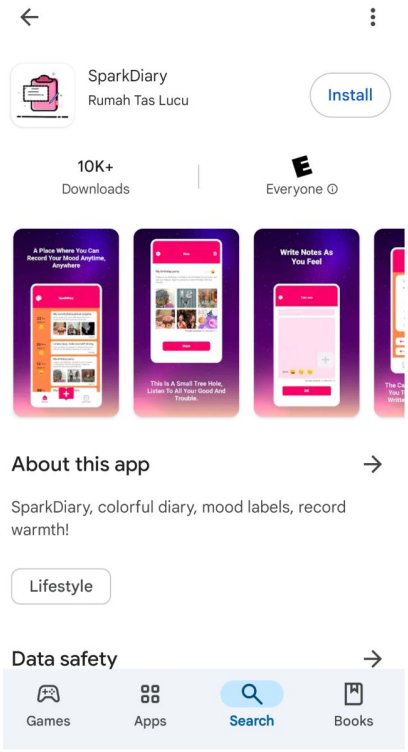
THE VAPOR THREAT: A COMPREHENSIVE ANALYSIS

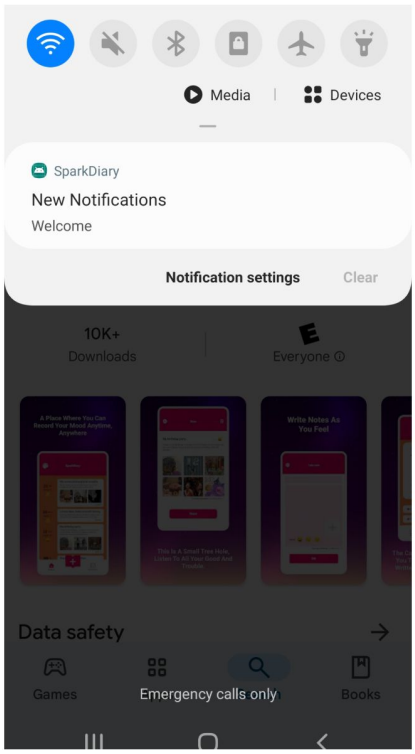
FALSE FUNCTIONALITY

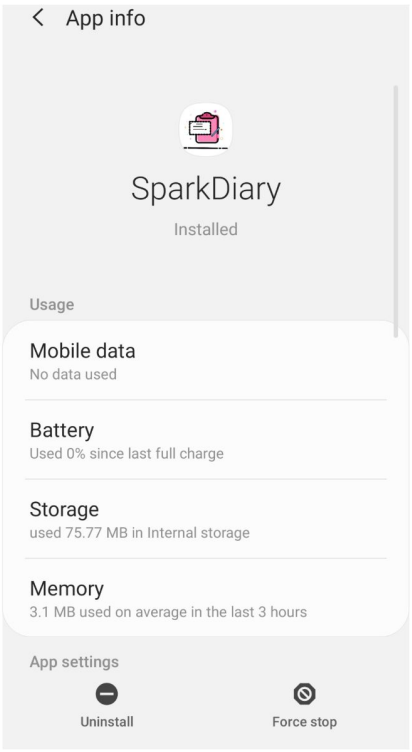
Believing these apps to offer useful functionality, users proceed to install them as further depicted below. However, the true intent of these apps quickly becomes apparent.

Upon installation, these apps are often accompanied with a persistent notification, subtly ensuring their continued operation. Some of these apps have no visible icon or “open” button available for the user to interact with. This is apparent from the app's settings page on Android as shown below.

Vapor app with consistent notification and no “Open” option in settings:





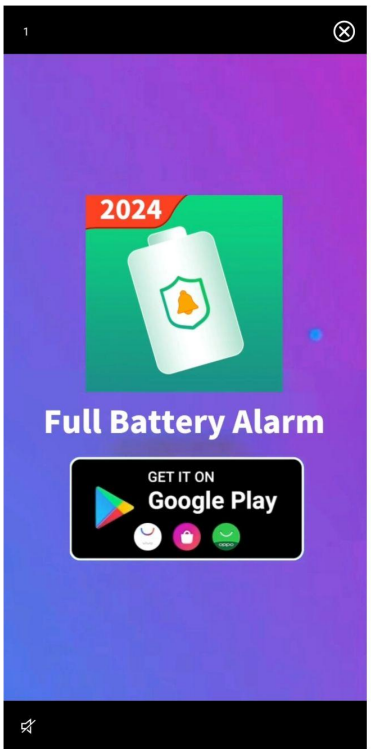


THE VAPOR THREAT: A COMPREHENSIVE ANALYSIS

PERSISTENT FULL-SCREEN ADS

With the app fully setup, it immediately attempts to barrage the user with full-screen interstitial ads, effectively hijacking the device's screen and rendering the user's device largely inoperative.

Screenshots of sample full screen interstitial ads triggered by Vapor apps:



SCALE OF OPERATION

The operation's scale is remarkable, with **over 180 app IDs** collectively achieving over **56 million downloads** and generating over **200 million bid requests daily**. Since the scheme began, new apps have been continuously added and activated daily, ensuring its persistence and growth. This growth has been necessary to replenish users lost due to the overtly intrusive nature of these apps.

THE VAPOR THREAT: A COMPREHENSIVE ANALYSIS

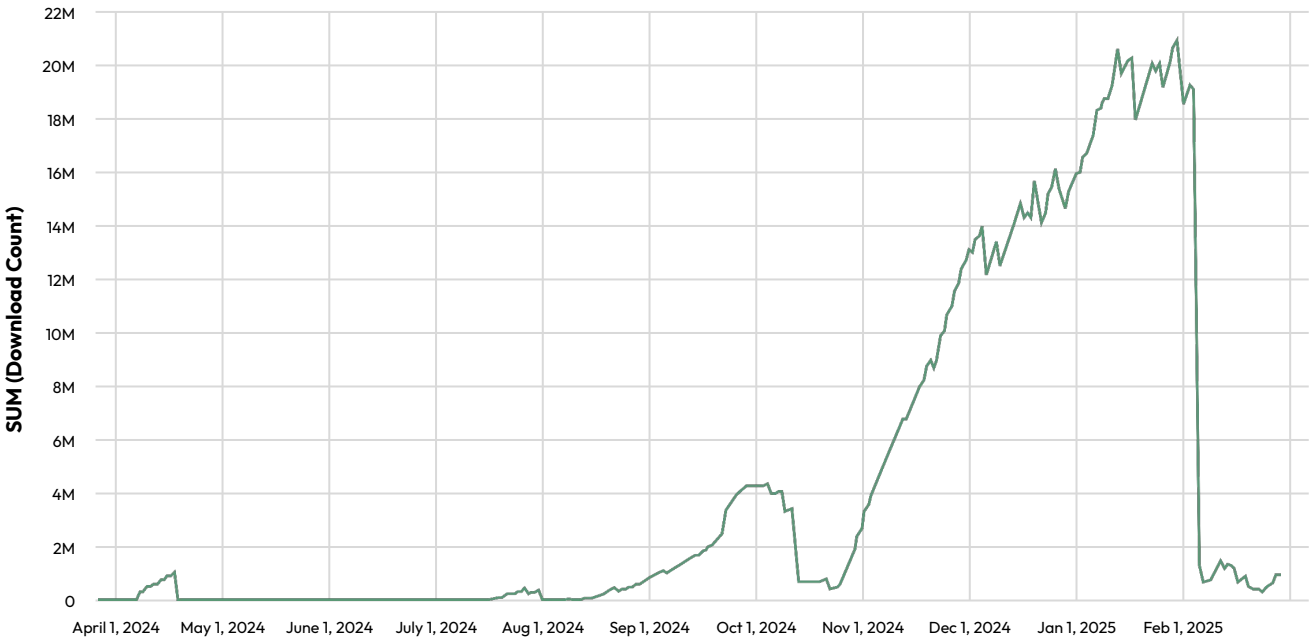
TIMELINE OF ACTIVITIES

The IAS Threat Lab traced the initial phase of the Vapor fraud operation to the beginning of 2024. During this time, simple flashlight and wallpaper apps were updated to restrict external access to the main app entry point, removing its ability to function as the app's launcher. Instead, a new entry point was introduced to handle initialization or redirection, ensuring that ad-related services and SDKs are activated upon launch. This redesign prevents the app from being launched directly, instead relying on system-level triggers such as broadcast receivers, background services, scheduled tasks, or specific user interactions.

The graph below reconstructs the Vapor operation timeline, showing total downloads across all apps on Google Play throughout their lifetime. The fraud operation appears to have started in early 2024, but the scheme was quickly disrupted when apps were removed from the platform. A significant push in Q3 was followed by another sharp drop after additional takedowns. However, from November through January, as significant advertising dollars were funneled into the holiday season, the scheme surged dramatically, with aggregated live downloads reaching over 21 million, showcasing the operation's resilience and scale.

Following IAS's investigation and intel sharing with Google in early February, all identified fraudulent apps associated with the Vapor operation were swiftly removed from the Play Store. As depicted in the graph, this action resulted in an immediate and dramatic drop in total downloads, effectively dismantling the scheme's presence on the platform.

Timeline of Vapor Threat growth and disruption:

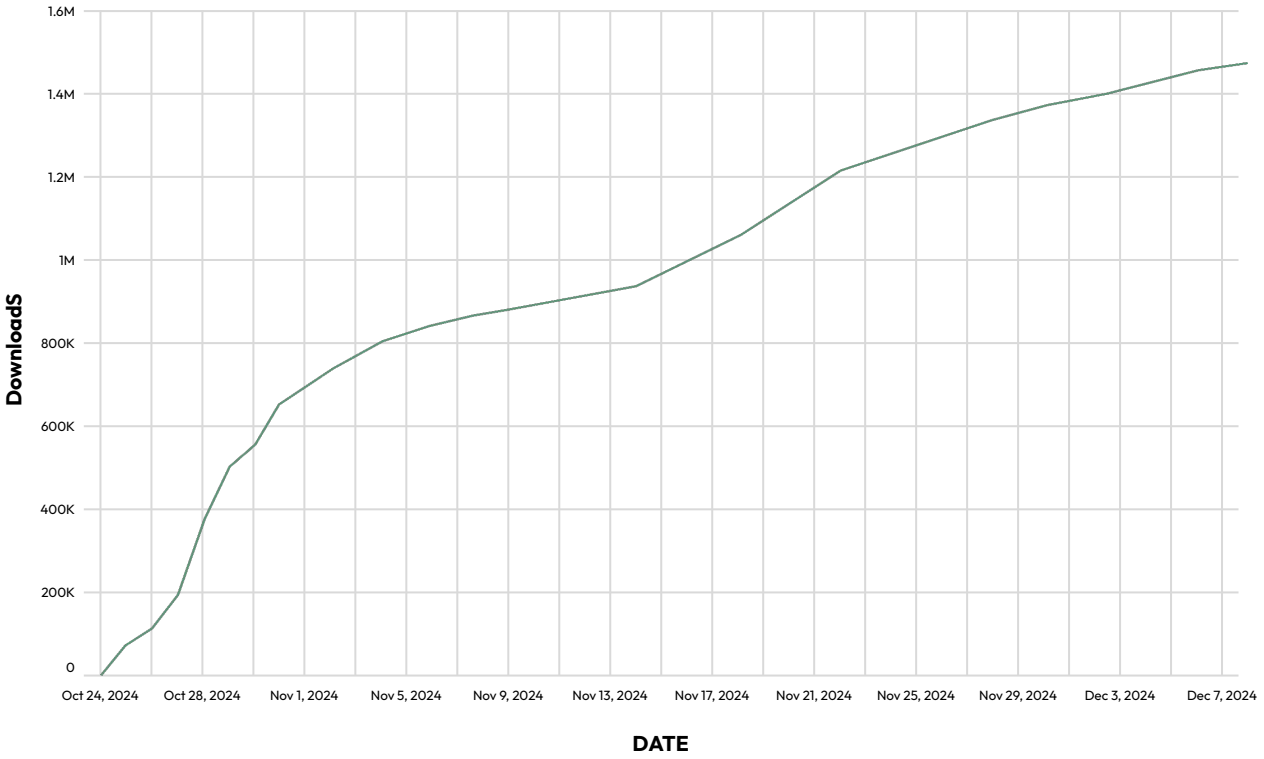


THE VAPOR THREAT: A COMPREHENSIVE ANALYSIS

The Threat Lab observed that a number of apps within Vapor had achieved download counts in excess of 1 million, an unnatural growth pattern given the type of apps involved. To artificially boost rankings and visibility, threat actors likely employed app install schemes, forcing installations onto devices. This strategy not only inflated download numbers but also positioned these apps higher in rankings, eventually leading to legitimate users discovering and installing them.

The evolution of app installs for one app, "com.eatrg.Rise.Motivate," achieving 1 million installs in exactly 24 days, is represented below.

Unnatural install growth rate of sample Vapor app:



INFRASTRUCTURE AND AFFECTED APPS

A critical aspect of the Vapor operation is its use of dedicated domains, per app, for command-and-control (C2) communication, enabling the app to send back critical data, including device type (e.g., Samsung Galaxy S24), regional settings (e.g., en_US), unique device, and user identifiers (e.g., UUIDs). To further obscure the operation, the key values have been intentionally masked, making analysis and attribution even more difficult.

THE VAPOR THREAT: A COMPREHENSIVE ANALYSIS

BEHAVIORAL ANALYSIS

Understanding the behavior of Vapor apps remains a critical focus for the industry. The Threat Lab has examined how these apps exploit Android's system components to perpetrate fraud, revealing a multi-step process that enables these applications to operate effectively without being detected.

Step 1: Initialization Through ContentProvider

- Vapor apps leverage the Android ContentProvider to gain an initial foothold. This component is initialized right after app installation, before any user interaction occurs. This early activation allows the app to start running in the background immediately.

Step 2: Start Ad Rendering Foreground Service

- A foreground service that is used to service interstitial ads is started. On devices with Android 11 and below, this foreground service starts immediately. On devices with Android 12 and up, foreground services running alongside background services are disabled. In these instances, Vapor uses native code to kickstart the foreground service.

Step 3: Foreground Service Persistence

- Foreground service displays persistent notifications—sometimes just an empty message or a simple text. This is crucial as it allows the app to have tasks at a higher priority, retain persistence, and run continuous ad activities.

Step 4: Ad Display and User Interface Control

- The foreground service is used to display full-screen interstitial ads, obscuring the device's system notification and navigation bars, and disabling the return button. This prevents users from easily dismissing the ads or exiting the app, ensuring maximum ad exposure. More than 15 different ad SDKs were observed across the analyzed Vapor samples.

Step 5: Obfuscation and Anti-Analysis Techniques

- The app uses sophisticated techniques like string obfuscation via custom base64 encoding or an open source XOR implementation known as StringFog. Additionally, some use native libraries to hide further functionality, complicating the reverse engineering efforts. These native libraries can load additional native libraries and open specific activities inside the app, as well as run anti-analysis checks such as for the presence of a rooted environment to further hinder analysis.

CONCLUSION

Vapor is a relentless fraud operation, engineered to manipulate and monetize at scale. Threat actors systematically built or acquired a vast arsenal of apps—often simple UI reskins—leveraging app install schemes to manipulate rankings. These tactics ensured that unsuspecting users would discover, install, and ultimately fall victim to the scheme.

With apps rapidly cycling in and out, and many reaching over one million downloads in record time, Vapor's scale, speed, and persistence highlight the evolving nature of ad fraud and the ongoing challenge of staying ahead of these operations.

IAS continues to monitor the Vapor operation. Google has removed all identified apps from the Play Store, and Google Play Protect will warn users and automatically disable these apps, even when they originate from sources outside of Google Play.

IAS partners are safeguarded against the impact of the Vapor threat through our fraud pre-bid avoidance solution available within their DSPs. Our advanced machine learning models power our fraud segments to ensure DSPs do not bid on impressions that originate from these apps.

- IOCs for App IDs and Domains

To learn more about how IAS detects and stops ad fraud across the digital landscape, explore our Ad Fraud solutions.

LEARN MORE