

BitScam & CloudScam

Dozens of crypto apps in the Play Store have scammed money from over 93,000 individuals

Background and Discovery

Researchers in the Lookout Threat Lab have discovered almost 200 Android apps, including 25 on the Play Store, scamming cryptocurrency investors out of money. The apps advertise that they provide crypto mining services for a fee, but upon further analysis Lookout researchers discovered no mining takes place and these services are never delivered.

Capabilities and Affected Parties

BitScam and CloudScam, which are the two families behind the discovered apps, are able to fly under the radar because they don't actually execute any malicious code. By using legitimate payment processes, the families enable these apps to collect money for services that don't exist.

Even though the apps that were found on the Play Store have been removed, the others are still circulating on third-party app stores. In addition, while BitScam and CloudScam have now been exposed, threat actors could continue to build apps with these families and create evolved versions to try to elude security tools.

Key Findings

1. These families enable threat actors to use legitimate functionality to carry out scams.
2. The apps that were on the Play Store have been removed, but hundreds more still exist on third-party app stores.
3. Indicators of Compromise (IoCs) for both families are available [here](#).

How Lookout Detects and Protects

Cybercriminals will oftentimes try to use legitimate capabilities to obfuscate malicious activity. The true intentions of an app are oftentimes hidden in the data access permissions and behaviors, and even then, can be difficult to uncover without the right tools. Static and dynamic analysis of the industry's largest mobile dataset enables Lookout researchers to protect customers by continuously discovering and researching new threats. Devices with Lookout installed can detect and be alerted to these two families as well as any other apps with risky functionality built in.

To learn more about the technical specifications of this campaign, including IOCs, read the full article [here](#).

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

[Click here to learn more about Threat Advisory](#)