



AndroidOS/MalLocker.B



Overview

Microsoft has recently discovered a new variant of ransomware with novel techniques and behavior on Android devices. The malware, known as AndroidOS/MalLocker.B, is the latest variant of an existing family that is widely used and distributed across online forums, apps, and more. The primary way attackers lure victims in is by leveraging social engineering within these platforms.

The ransomware will lock the device and display a ransom note on the home screen. This variant leverages new tactics to circumvent prevention measures put in place by Google that were meant to block creation of an overlay window that could not be dismissed by the user. It appears that there are machine learning capabilities that will enable this malware family to constantly evolve in the future.

Lookout Analysis

In the past, ransomware messages like this one persisted through an infinite loop of creating (drawing) and recreating (re-drawing) the overlay screen. Between the draw and re-draw, it was possible for users to get to their apps and uninstall the malicious app. This latest variant is able to create an infinite loop that avoids that draw and re-draw process that makes it impossible for the user to be able to access the device and remove the offending app.

Lookout Coverage and Recommendation for Admins

Lookout detects AndroidOS/MalLocker.B as a new variant of PLock and has protection against this ransomware in place for its customers. When detected on a user's device, Lookout will block it from executing before it can take the device over and lock the screen. When the user receives an alert, they will receive guidance on how to remediate the threat.

Lookout admins can set policies in the console that block a device's access to corporate resources if AndroidOS/MalLocker.B is detected until it is removed. This is enforced by Continuous Conditional Access, which constantly monitors the risk-level of mobile endpoints to protect your infrastructure by enabling Zero trust Network Access policies.

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 Lookout Threat Advisory](#)