Nation-State Espionage: Hunting Multi-Platform APTs on a Global Scale

Michael Flossman[1],
[1]*Lookout,*

Lookout and EFF will dive into their joint investigation of Dark Caracal, a global, multi-platform actor that has made use of both desktop and Android components to successfully compromise thousands of victims. This threat actor has had numerous long running campaigns over the years and this talk will first recap one of their earlier operations before going into depth on their recent activity and, ultimately, their attribution. As this adversary is relatively unknown in the cyber security world we'll take a look at the various tools in their arsenal. This will cover custom surveillanceware that appears to be in-house developed as well as commodity products for multiple platforms which include a version of FinFisher for Android that hasn't been seen elsewhere. Will also cover OpSec shortcomings that allowed us to follow their activity and gain an insight into just how successful they've been. We'll wrap up this session by discussing the analysis we performed into both their infrastructure and compromised data and walk through the clues we followed in order to track them down to a specific intelligence building that we believe they were administering their tooling from.