How mobile malware carried out the largest Google account breach?

Feixiang He[1]
[1]*Check Point*

In this talk we will discuss one of the largest mobile attacks to date, named Gooligan, which breached the security of over one million Google accounts. This elaborate malware infected and rooted devices, stealing authentication tokens that could be used to access data from Google Play, Gmail, Google Photos, Google Docs, G Suite, Google Drive, and more.

We will delve into Gooligan's malicious tactics, as well as its real objective – ad-fraud. The malware was designed to simulate clicks on app advertisements provided by legitimate ad networks and forces the app to install on a device. This cunning scheme allowed the attacker to be paid by ad networks when such an app is installed successfully. To understand the scale of this business model, we will present real-life data, including logs collected by Check Point researchers which show that during its operation, Gooligan installed over 2 million apps.

Our talk will examine how such malware are able to thrive on mobile devices today, and outline ways in which the security community can join hands in an effort to mitigate them.