Hornbill & Sunbird

Novel Android surveillanceware developed by pro-India APT group Confucius targeting Pakistani officials

Key Findings

1. These malware tools have advanced surveillanceware and data exfiltration capabilities.
2. Social engineering is likely the key distribution channel to targeted individuals.
3. Over 18GB of exfiltrated data from at least six C2 servers was discovered and analyzed.

Background and Discovery Timeline

The Lookout Threat Intelligence team has discovered new Android surveillanceware with sophisticated capabilities. SunBird features remote access trojan (RAT) capabilities that can execute commands on an infected device directly from the attacker while Hornbill operates as a discreet surveillanceware tool that extracts particular data of interest to the attacker.

Capabilities and Affected Parties

Each of these tools has been used to target personnel linked to Pakistan's military, nuclear authorities, and Indian election officials in Kashmir. Both Hornbill and Sunbird appear to be evolved versions of pre-existing commercial surveillanceware. There is also evidence of them being present across Europe, Southeast Asia, Russia, and the United States.

Considering that apps infected with these two pieces of malware are distributed via third party app stores, social engineering is likely the most effective way that they're distributed. Both pieces of malware have extensive surveillance and data exfiltration capabilities including access to:

-Call logs -Geolocation - Contacts - SMS Messages - Photos -Installed apps -Browser history -WhatsApp messages -Calendar -Requesting Admin Privileges -Taking screenshots & photos - Recording audio & calls - Scraping WhatsApp messages and contacts

How Lookout Detects and Protects Against Surveillanceware Campaigns

Lookout Security Intelligence teams are continuously discovering and researching new threats to protect and advise our customers. We do this by combining static and dynamic analysis with our machine learning engine. Devices with Lookout installed can detect and be alerted to these two families and Lookout also protects against other sophisticated surveillanceware that could go undetected.

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