LevelBlue - Open Threat Exchange

By arringtont

Archived: 2026-04-05 18:49:29 UTC

VajraSpy Android Spyware

FileHash-MD5: 4 | **FileHash-SHA1:** 4 | **FileHash-SHA256:** 6

A group known to engage in espionage operations has covertly installed malware, known as VajraSpy, on Android users, according to researchers at ESET, who discovered the malware in the Google Play store.

- 103 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

MONSOON – ANALYSIS OF AN APT CAMPAIGN

CVE: 4 | **FileHash-SHA1:** 60 | **URL:** 57 | **Hostname:** 20

MONSOON is the name given to the Forcepoint Security Labs™ investigation into an ongoing espionage campaign that the Special Investigations team have been tracking and analysing since May 2016. The overarching campaign appears to target both Chinese nationals within different industries and government agencies in Southern Asia. It appears to have started in December 2015 and is still ongoing as of July 2016. Amongst the evidence gathered during the MONSOON investigation were a number of indicators which make it highly probable1 that this adversary and the OPERATION HANGOVER adversary are one and the same. These indicator include the use of the same infrastructure for the attacks, similar Tactics, Techniques and Procedures (TTPs), the targeting of demographically similar victims and operating geographically within the Indian Subcontinent

- 373,973 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:TINYTYPHON