LevelBlue - Open Threat Exchange

By AlienVault

Archived: 2026-04-05 22:48:41 UTC

 Author Url

Suspected APT-C-23 (two-tailed scorpion) tissue camouflage Threema communication software attack analysis

FileHash-MD5: 21 | **FileHash-SHA1:** 12 | **FileHash-SHA256:** 12 | **URL:** 1

APT-C-23 (two-tailed scorpion) is also known as AridViper, Micropsia, FrozenCell, Desert Falcon, and its attack range is mainly in important fields such as educational institutions and military institutions in relevant countries in the Middle East, and important fields such as educational institutions and military institutions in Palestine, a network attack organization that mainly steals sensitive information. It has the ability to attack both Windows and Android platforms. From May 2016, organized, planned and targeted long-term uninterrupted attacks were launched on Palestinian educational institutions, military institutions and other important areas.

- 374,021 Subscribers

New GnatSpy Mobile Malware Family Discovered

Stay updated to the latest updates on Trend Micro's app, which allows users to search for products on a variety of sites across the globe, including Facebook, Twitter, Instagram, Google and YouTube.

- 354 Subscribers

FrozenCell

FrozenCell is the mobile component of a multi-platform attack we've seen a threat actor known as "Two-tailed Scorpion / APT-C-23," use to spy on victims through compromised mobile devices and desktops. The desktop components of this attack, previously discovered by Palo Alto Network, are known as KasperAgent and Micropsia. During this investigation we discovered 561MB of exfiltrated data from 24 compromised Android devices that was publicly accessible on one of dozens of C2s. More data is appearing daily, and it looks like this actor is both still active and pretty successful despite not using any exploits in their mobile component.

- 69 Subscribers

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