techwell

Check Point®
SOFTWARE TECHNOLOGIES

Threat Intelligence Report

# Mobile Attack Report

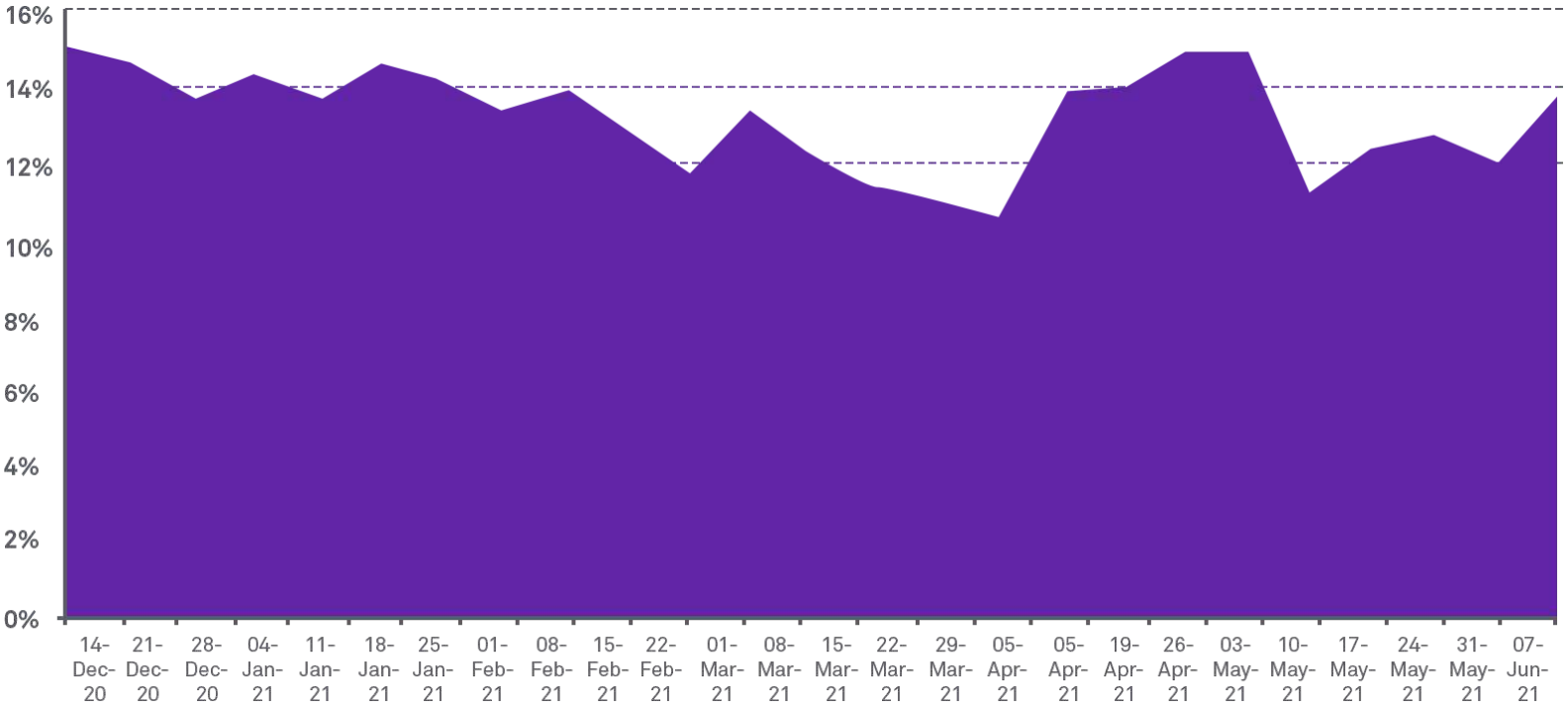
# Mobile Summary Data

- **1** out of every **5** organizations suffers from a malicious incidents.
- **1** out of every **9** entrances to malicious websites is to a Phishing website.
- **1** out of every **4** Phishing attack is over SSL.
- **1** out of every **9** organizations suffered from a Man in the Middle malicious activity while connecting to Wifi network.
- **373** different malicious applications and 22260 risky applications were found.

# Major Mobile Attacks

- 05-2021 - US Intelligence officials have reported that Chinese state-sponsored threat actors have leveraged an exploit dubbed Chaos for iPhone devices in an espionage campaign that targets the Uyghur minority in China. The exploit has been developed by a researcher from Qihoo 360 in 2018 as part of a Chinese hackathon.
- 05-2021 - Despite designated arrests by Spanish police, the FluBot Android botnet has resumed its activities, and has been spreading through Europe via an SMS package delivery scheme, in which tens of thousands of SMS messages are sent per hour with the FluBot download link.
- 04-2021 - Apples AirDrop, a feature that allows Mac and iPhone users to wirelessly transfer files between devices, has been leaking users hashed emails and phone numbers. The flaw is known since 2019 and Apple has yet to find a fix.
- 04-2021 - A new Linux and macOS malware has been found hidden in a malicious package named web-browserify, imitating the popular Browserify npm component.
- 04-2021 - After the March breach of the ParkMobile parking app, data stolen in the incident is now offered for sale on a cybercrime forum. The data consists of 21 million user records, including email, phone number, hashed passwords and license plate number, belonging to customers like Donald Trump, Hillary Clinton, security Journalist Brian Krebs, and more.
- 04-2021 - Check Point Research has discovered a new Android malware capable of spreading itself and distributing further payloads via WhatsApp conversations. The malware disguises itself as a Netflix content enabler application called FlixOnline, that can be found on Google Play store.

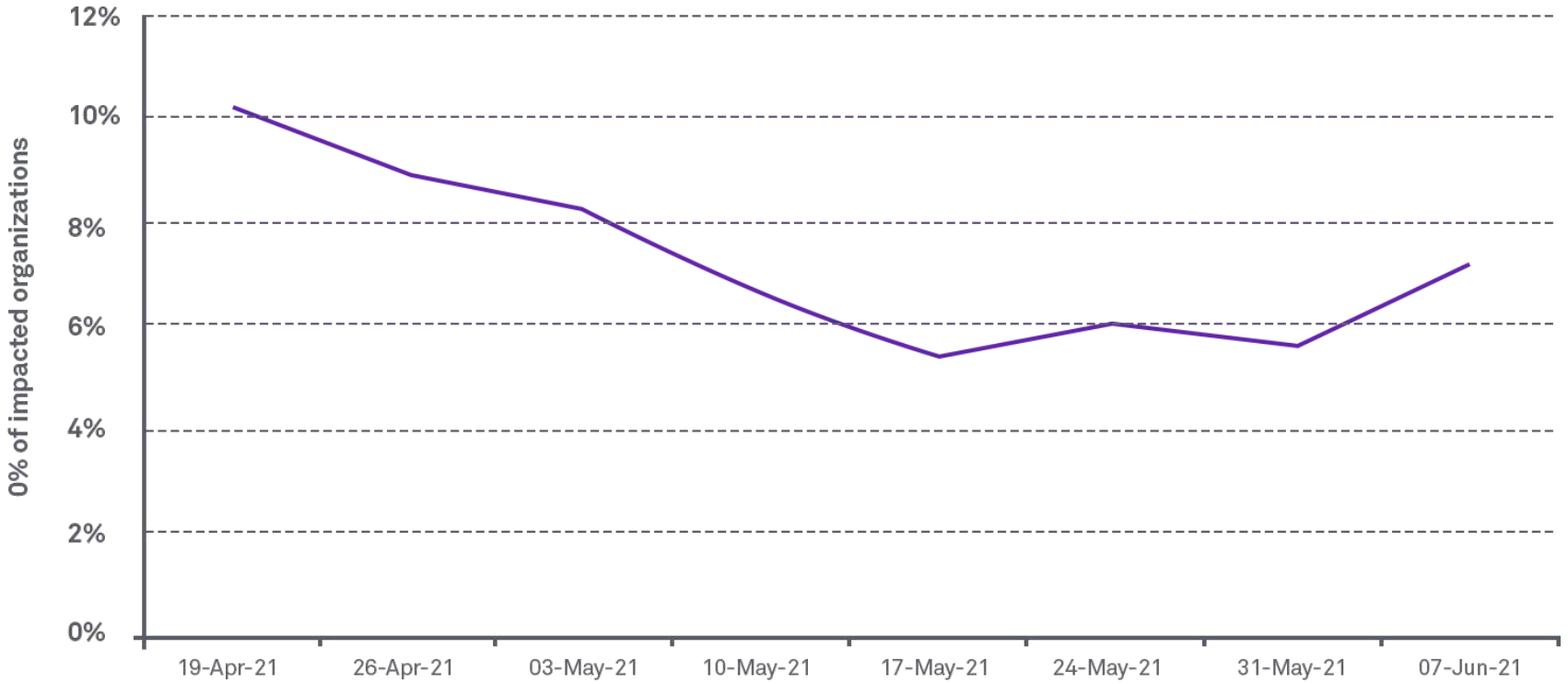
# Attacks per Organization



# Top Mobile Malwares

| MALWARE FAMILY | DESCRIPTION |
| --- | --- |
| **xHelper** | xHelper is an Android malware which mainly shows intrusive popup ads and notification spam. It is very hard to remove once installed due to its reinstallation capabilities. First observed in March 2019, xHelper has now infected more than 45,000 devices. |
| **Triada** | Triada is a modular backdoor for Android which grants super-user privileges to download a malware. Triada has also been seen spoofing URLs loaded in the browser. |
| **Hiddad** | Hiddad is an Android malware which repackages legitimate apps and then releases them to a third-party store. Its main function is to display ads, but it can also gain access to key security details built into the OS. |

# Phishing Impact on Organizations



# Attack Vectors Impact on Organizations