More than 200 apps containing malicious code were discovered and downloaded millions of times on the Google Play Store.

A cybersecurity firm has discovered a huge number of Android apps containing malicious code (adware), a discovery that also raises big questions about how Google monitors its online store.

Over the past few years, Google has invested heavily in developing advanced security algorithms for the Play Store, but preventing threats early and thoroughly is not easy.

Data collected between June 2023 and April 2024 by cybersecurity researchers from Zscaler security organization discovered more than 200 malicious apps, with millions of downloads, publicly distributed on the Google Play Store. The most common threats that researchers found on the official Android app store include:

1. **Joker** (38.2%): Software that steals information and collects SMS messages, enrolls victims in premium services.
2. **Adware** (35.9%): Apps that consume internet bandwidth and battery to load foreground or hidden ads in the background, creating fraudulent ad impressions.
3. **Facestealer** (14.7%): Software that steals Facebook account information, overlaying phishing forms on legitimate social networking applications.
4. **Coper** (3.7%): Information stealing and SMS interception software, can also perform keylogging and overlay phishing sites.
5. **Loanly Installer** (2.3%).
6. **Harly** (1.4%): Trojan applications subscribe victims to premium services.
7. **Anatsa** (0.9%): Anatsa (or Teabot) is a banking trojan that targets over 650 banking applications worldwide.

Earlier in May this year, Zscaler researchers also warned about more than 90 malicious apps on Google Play, with a total of 5.5 million downloads.

While Google has security mechanisms in place to detect malicious apps, threat actors still have a number of tricks up their sleeves to bypass the verification process. In a report last year, the Google Cloud security team described a method of distributing malware through app updates, or by downloading malware from attacker-controlled servers.

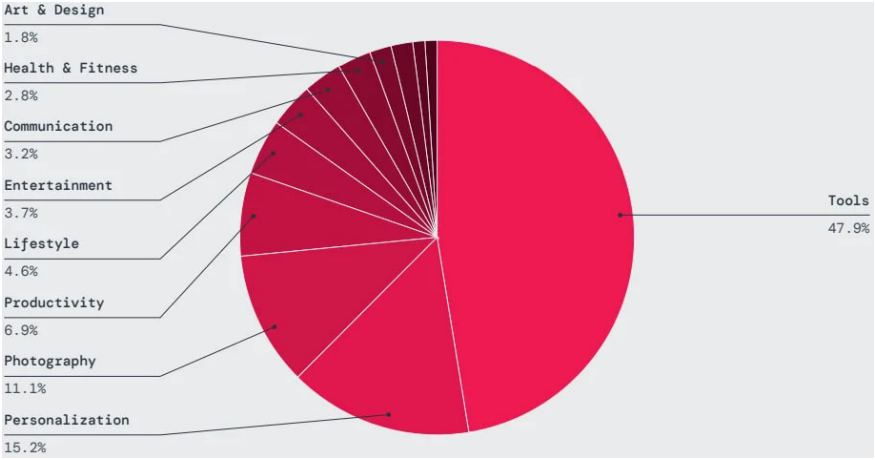
While Zscaler's report focuses on popular Android malware, other researchers have discovered a number of campaigns that also abuse Google Play to distribute malware to millions of people.

A typical example is the Necro malware downloader for Android, which was downloaded 11 million times through just two apps released on the Google Play Store.

In another case, the Goldoson Android malware was detected in 60 legitimate apps with a total of 100 million downloads also on the Play Store.

Last year, SpyLoan malware was found in apps on Google Play that were downloaded more than 12 million times.

Nearly half of the malicious apps detected by Zscaler ThreatLabz were published on Google Play in the tools, personalization, photography, productivity, and lifestyle categories.



Zscaler's mobile threat report also shows a significant increase in spyware infections, primarily caused by the SpyLoan, SpinOK, and SpyNote groups. Over the past year, the company recorded 232,000 blocks of spyware activity.

The countries most targeted by mobile malware over the past year were India and the United States, followed by Canada, South Africa and the Netherlands.

According to the report, mobile malware was primarily targeted at the education sector, with a 136.8% increase in blocked transactions. The services sector saw a 40.9% increase, and chemicals and mining increased by 24%. All other sectors saw a general decline.

To minimize the chance of being infected with malware from Google Play, users should carefully read reviews from others to see what issues have been reported, then thoroughly check information about the app publisher.

You finished reading the article "**More than 200 apps containing malicious code were discovered and downloaded millions of times on the Google Play Store.**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.