“Sharkbot” found on Google Play store - Check Point Blog

By etal

Published: 2022-04-07 · Archived: 2026-04-06 02:10:24 UTC

Highlights:

- Check Point Research (CPR) found anti-virus apps on the Google Play store disguised as legitimate which downloaded and installed android malware
- At least six different apps with over 15,000 total downloads were spreading the malware, which were consequently all taken down from the Google Play store after CPR’s disclosure
- Dubbed “Sharkbot” the malware steals credentials and banking information

When searching for an anti-virus (AV) solution to protect your mobile, the last thing one would expect is for it to make your device *vulnerable* to malware.
This is what the CPR team encountered while analyzing suspicious applications found on the Google Play store. These applications were disguised as genuine AV solutions, but in reality, users downloaded and installed an android stealer called ‘Sharkbot’.
Sharkbot steals credentials and banking information. This malware implements a geofencing feature and evasion techniques, which makes it stand out from the rest of malwares. It also makes use of something called domain generation algorithm (DGA), an aspect rarely used in the world of Android malware.
CPR identified approximately *1000 unique IP addresses* of infected devices during the time of analysis.

Most of the victims were from Italy and the UK as per the chart below.

Regional statistics

Sharkbot lures victims to enter their credentials in windows that mimics benign credential input forms. When the user enters credentials in these windows, the compromised data is sent to a malicious server. Sharkbot doesn't target every potential victim it encounters, but only select ones, using the geofencing feature to identify and ignore users from China, India, Romania, Russia, Ukraine or Belarus.

Disguised as legitimate anti-virus apps on Google Play store

CPR researchers spotted a total of six different applications in the Google Play store that were spreading Sharkbot.

Four applications came from three developer accounts, Zbynek Adamcik, Adelmio Pagnotto and Bingo Like Inc. When CPR checked the history of these accounts, we saw that two of them were active in the fall of 2021. Some of the applications linked to these accounts were removed from Google Play, but still exist in unofficial markets. This could mean that the threat actor behind these applications is trying to stay under the radar, while still involved in malicious activity. Overall, we saw over 15,000 downloads of these apps from Google Play.

Applications found on Google Play store

Responsible disclosure to Google

Immediately after identifying these applications that spread Sharkbot, CPR reported these finding to Google**.** Quickly after examining the apps, Google proceeded to permanently remove these applications on Google Play store.

On the same day CPR reported the finding to Google, the NCC group published a separate research about Sharkbot, mentioning one of the malicious apps.

Timeline

- February 25, 2022 – CPR discovered 4 applications of SharkBot Dropper on Google Play, with a total of 11K installations.
- March 03, 2022 – CPR reported to Google the malicious applications found on Google Play.
- March 03, 2022 – NCC Group published their research on Sharkbot Dropper.
- March 09, 2022 – Reported applications removed from Google Play.
- March 15, 2022 – CPR found one more SharkBot dropper on Google Play with0+ installs. CPR reported it to Google.
- March 22, 2022 – An additional SharkBot dropper was discovered on Google Play, 0+ installs. CPR reported it to Google.
- March 27, 2022 – Newly found SharkBot dropper’s removed from Google Play.

Beware of malicious apps

Threat actors are evolving and constantly seeking ways to inject and drop malware at any means possible, including disguising as legitimate “official” apps.

We advise Android users to:

- Install applications only from trusted and verified publishers
- If you see an application from a new publisher, search for equivalents from trusted publishers.
- Report to Google any seemingly suspicious applications you encounter

Protections

Check Point's Harmony Mobile prevents malware from infiltrating mobile devices by detecting and blocking the download of malicious apps in real-time. Harmony Mobile's unique network security infrastructure – on-device network protection – allows you to stay ahead of emerging threats by extending Check Point's industry-leading network security technologies to mobile devices.

Threat Emulation protections:

Sharkbot.TC.*

The full technical analysis can be read on research.checkpoint.com

---