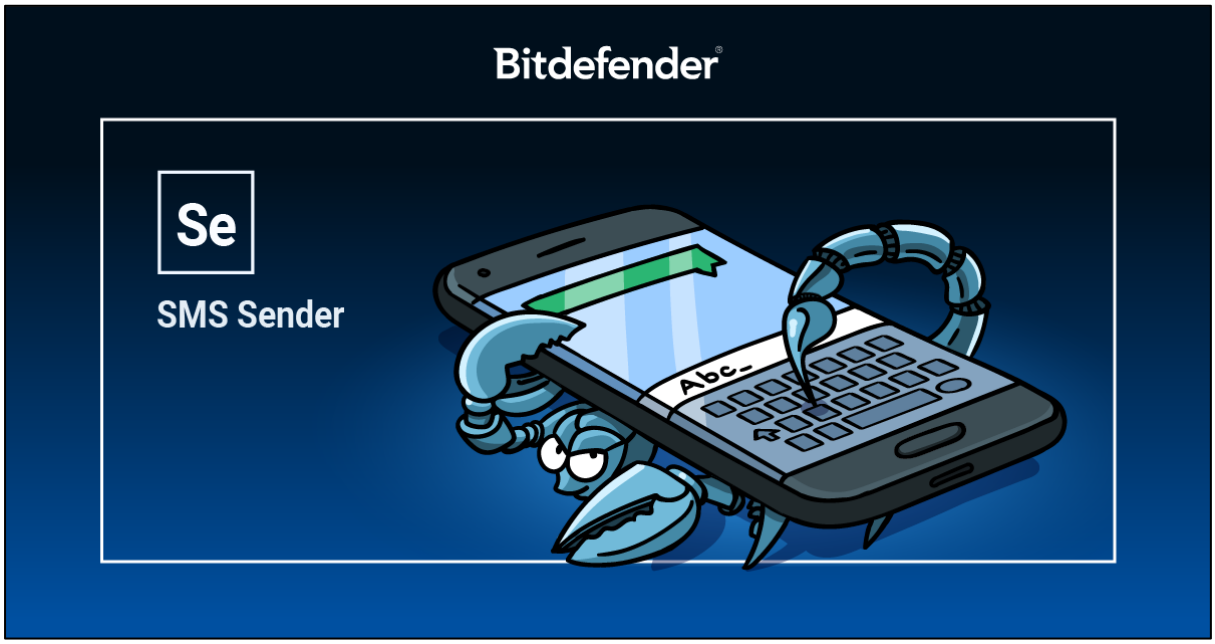
What is an SMS Sender? Prevention & Removal

SMS Sender threats have been around ever since mobile devices became widely adopted, and they've been responsible for a huge number of racked up phone bills and premium number subscriptions, generating significant financial losses around the world.

What is an SMS Sender?

SMS Sender is a type of Trojan designed for Android devices with a single purpose: to generate profit for cybercriminals by covertly infiltrating smartphones and taking control of SMS sending and receiving functions. This is a very effective and easy way of making money, as it's completely untraceable until the damage is already done. Because users are unaware of sent text messages, the malicious behavior is usually discovered when very large phone bills show up or when credit disappears in a matter of days.



As soon as an application infected with an SMS-sending Trojan reaches a smartphone, it seizes SMS sending and receiving capabilities. This means that it can send and receive text messages without users knowing about it, while also hiding notifications.

These Trojans usually try to contact more than one premium-rated number, with services per text messaging sometimes reaching a couple of dollars or euros. These are usually adult services to which the attacker has some sort of affiliation, meaning that for each subscribed user the attacker receives money. Some of these services have begun incorporating features meant to prevent automatic subscription, such as two-factor authentication or CAPTCHA. But the SMS-sending Trojan can also read incoming emails, so it can intercept these one-time authentication passwords and make the process look legitimate.

How does an SMS Sender get into my smartphone?

One of the most common infection methods with SMS-sending Trojans is through Android applications downloaded and installed from third-party marketplaces that don't usually sanitize apps with the same level of scrutiny as official marketplaces. This allows hackers to inject malicious code into legitimate – usually paid applications, with the promise that the downloaded app will contain the full version, without having to purchase it. This method is quite effective at getting users to sideload (install from unofficial stores) applications, as some users do not want to actually buy apps.

Moreover, even apps in official stores have on occasion been known to behave maliciously and exhibit malicious SMS-sending abilities. In fact, these apps were so sophisticated at the time that they even had CAPTCHA bypassing mechanisms, specifically for skirting validation from premium-rated numbers.

Other infection methods that are usually a bit more complex involve the use of zero-day exploits (vulnerabilities that were previously unknown) usually in browsers triggered by malicious URLs. Whenever a user opens an attacker-crafted link, he could be redirected to a webpage that might enable an attacker to remotely exploit and control an Android device. Of course, this involves a high degree of sophistication from the attacker, and such Android vulnerabilities are usually exploited to deliver other types of threats, such as remote access Trojans (RATs), rather than SMS-sending malware.

How to avoid SMS-sending Trojans

Users should avoid downloading and installing Android applications from untrusted or third-party marketplaces, especially apps that promise fully unlocked features for otherwise paid apps. These apps are usually injected with SMS-sending Trojans and other malware and lure victims with the promise of fully unlocked features to popular apps. Sometimes cybercriminals leverage the name of popular applications, such as Angry Birds or Pokemon Go, to create malicious apps that have nothing to do with the original application. The best way to keep your device safe from SMS-sending Trojans is to use a mobile security solution that can scan apps before installing them. Even if you're downloading apps from official stores such as Google Play or third-party stores, an antivirus can assess whether an app is dangerous and prevent it from installing on your device.

Disinfection

Removing an SMS Sender is sometimes as simple as using the built-in uninstall feature in Android. However, these malicious apps usually hide their names under aliases designed to trick users into believing they are system apps. For example, one such malicious application could use an alias like "com.android.system.service" or "com.android.system.manager" when users would look it up in the Uninstall manager, but use a different name, such as "Download Manager" on the start screen.

It’s also important to go through permissions whenever you install new applications, as sometimes they are dead giveaways that the app will perform activities it shouldn’t. For example, a racing simulator asking for permission to send text messages should raise an eyebrow, as this feature is not likely needed in the game. Consequently, any application that tries to access SMS-sending permissions should have legitimate rights to do so, or it may not be the real deal.