Android users warned of malware attack spreading via SMS | Tripwire

By Graham Cluley

Published: 2016-02-16 · Archived: 2026-04-06 01:34:18 UTC

Security researchers are warning owners of Android smartphones about a new malware attack, spreading via SMS text messages. As the team at Scandinavian security group CSIS describes, malware known as MazarBOT is being distributed via SMS in Denmark and is likely to also be encountered in other countries. Victims' first encounter with the malware reportedly comes via an unsolicited text message that their Android smartphone receives. The txt message uses social engineering to dupe unsuspecting users into clicking on a link to a downloadable Android application. CSIS provided a (sanitised) version of a typical message to warn users what to look out for:

> "You have received a multimedia message from +[country code] [sender number] Follow the link http://www.mmsforyou[.]net/mms.apk to view the message"

Once the APK package is downloaded, potential victims are urged to grant the malicious app a wide range of permissions on their Android device:

- SEND_SMS
- RECEIVE_BOOT_COMPLETED
- INTERNET
- SYSTEM_ALERT_WINDOW
- WRITE_SMS
- ACCESS_NETWORK_STATE
- WAKE_LOCK
- GET_TASKS
- CALL_PHONE
- RECEIVE_SMS
- READ_PHONE_STATE
- READ_SMS
- ERASE_PHONE

Once installed, MazarBOT downloads a copy of Tor onto users' Android smartphones and uses it to connect anonymously to the net before sending a text message containing the victim's location to an Iranian mobile phone number. With the malware now in place, a number of actions can be performed, including allowing attackers to secretly monitor and control smartphones via a backdoor, send messages to premium-rate numbers, and intercept two-factor authentication codes sent by online banking apps and the like. In fact, with full access to the compromised Android smartphone, the opportunities for criminals to wreak havoc are significant – such as erasing infected phones or launching man-in-the-middle (MITM) attacks. In its analysis, CSIS notes that MazarBOT was reported by Recorded Future last November as being actively sold in Russian underground forums and

intriguingly, the malware will not activate on Android devices configured with Russian language settings. This, in itself, does not prove that the perpetrators of the malware campaign are based in Russia, but it certainly sounds as if that is a strong possibility. Malware authors in the past have often coded a "safety net" into their malware to prevent them from accidentally infecting their own computers and devices. For more detailed information about the threat, check out the blog post from CSIS. And, of course, remember to always be wary of unsolicited, unusual text messages and installing apps from third-party sources on your Android smartphone. **Editor's Note:** *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
