Source : www.thehindu.com Date : 2019-12-18

EXPLAINED: WHAT IS THE 'STRANDHOGG' BUG?

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

All versions of Android, including Android 10, are vulnerable to this bug

The Union Home Ministry has sent an alert to all States warning them about the vulnerability in the Android operating system that allows malware applications to pose as legitimate apps and access user data of all kind.

Promon, a Norwegian firm specialising in In-App protection, found proof of this dangerous Android vulnerability, which they call 'StrandHogg', Old Norse for the Viking tactic of raiding coastal areas to plunder and hold people for ransom.

“Vikings were known to set up spy networks, with information on religious feasts and events, local customs and high-value personalities who could be ransomed being used when choosing the next area to attack," Gustaf Sahlman, CEO of Promon wrote in his company blog. "Cybercriminals are the modern-day Vikings, and we encourage individuals to be extra vigilant, and for companies, to ensure they have robust app protection in place.”

The vulnerability allows sophisticated malware attacks without the need for a device to be rooted to the Android operating system. Attackers exploit Android's control setting called 'taskAffinity', which enables any app to freely assume any identity in Android's multi-tasking system.

According to a research by Penn State University in 2015, which theoretically described some aspects of the weakness, the Android task management mechanism was plagued by 'severe security risks'.

"When abused, these convenient multi-tasking features can backfire and trigger a wide spectrum of 'task hijacking attacks'," researchers wrote.

They explained that when a user launches an app, an attacker can condition the system to display to the user a spoofed User Interface (UI) under attacker’s control instead of the real UI from the original app, without the user’s awareness. All apps on the user’s device are vulnerable, including the privileged system apps.

Google, at that time, dismissed the vulnerability's severity.

Promon expanded the study and conducted research of real-life malware that exploits this serious flaw. It found that all of the top 500 most popular app (as ranked by 42Matters, an app intelligence company) are at risk.

According to Promon, the specific malware sample did not reside on Google Play, but was installed through several dropper apps/hostile downloaders distributed by Google Play. These apps have now been removed, but in spite of Google’s Play Protect security suite, dropper apps continue to be published and frequently slip under the radar, with some being downloaded millions of times before being spotted and deleted.

Dropper apps are those that either have or pretend to have functionality of popular apps, but they also install additional apps to a device that can be malicious, or steal data.

Currently, there is no effective block or even detection method against StrandHogg on the

device itself. However, as an user, you should be alert to the following discrepancies in your device:

Twitter’s new account named @TwitterRetweets has been launched with an aim to highlight the best of the micro-blogging platform and will provide followers with ‘Your best Tweets Retweeted

The news comes close to the heels of Facebook-owned Whatsapp disclosing that an Israeli spyware was used to spy on people in India.