New Android vulnerability Strandhogg 2.0 exploits user trust

Enlarge / Strandhogg 2.0 can be thought of as the ultimate phishing attack. When the user taps a legitimate icon—which could be for email, camera, etc—the malware intercepts the tap and can present a copycat dialog instead.

reader comments

6 with 5 posters participating, including story author

Share this story

A Norwegian infosec firm discovered a new Android vulnerability, which they've dubbed Strandhogg 2.0. Security firm Promon says "Strandhogg" is an old Norse strategy for coastline raids and abductions, and today's vulnerability is the "evil twin" of a similar one discovered in 2019.

The original Strandhogg used an Android feature called taskAffinity to hijack applications—by setting the taskAffinity of one of its activities to match the packageName of any other app, then setting allowTaskReparenting="true" in its own manifest, the Strandhogg app would be launched in place of the target app.

Imagine tapping the legitimate Gmail icon on your phone and getting what appears to be a legitimate login prompt, pixel-for-pixel identical with the one you'd see if your account had been logged off. Would you enter your credentials? If one of the free games or apps you or a child might have installed was a Strandhogg vessel, you just gave your credentials to an

attacker—which might even launch the Gmail application itself immediately after testing your credentials, leaving no obvious sign you had been compromised.

[embedded content]
Impatient users should skip ahead to 1:00—the first minute of the video is spent simply demonstrating that the Camera, Facebook, Messages, Files, and Gmail apps are legitimate.
Strandhogg's 1.0 major weakness was the need to declare taskAffinity in the Android Manifest. The Manifest is a plain XML file and must be included in the package hosted at the Play Store itself—it can't simply be downloaded later, after the app is installed. This made it relatively simple to scan the Play store for apps with sketchy-looking taskAffinity declarations.

Strandhogg 2.0 doesn't require any special settings in a package's Android Manifest—meaning the attacking code doesn't need to be present on the Play Store to be scanned at all. Instead, the attacker can download the attack code later, once the trojan app or game is already installed on a user's device.

Enlarge / Any Android application can be targeted by Strandhogg's overlay-phishing technique—including banking apps.
In addition to the obvious credential-stealing attacks, Strandhogg can be used to trick users into escalating its privileges based on the trust they have for the apps it

hijacks. For example, a user tapping Camera is asked if they want to grant it permission to access the camera and microphone—if the user taps Yes, they've actually given those privileges to the malware app, not the Camera app it covered up on the screen.

Strandhogg 2.0 affects all versions of Android prior to 10—which translates to roughly 90 percent of the Android userbase. Google rolled out a patch to close the Strandhogg 2.0 vulnerability, CVE-2020-0096, in May's Android Security Update. This is good news for Pixel users—but as always, carriers and OEMs may delay those upgrades significantly.

The older Strandhogg 1.0 vulnerability is not patched and likely will not be—it appears that Google prefers to play whack-a-mole with dodgy apps as they are uploaded to the Play store, since it can scan for exploits of that vulnerability directly in the Manifests of potential malware applications.

https://arstechnica.com/?p=1678835