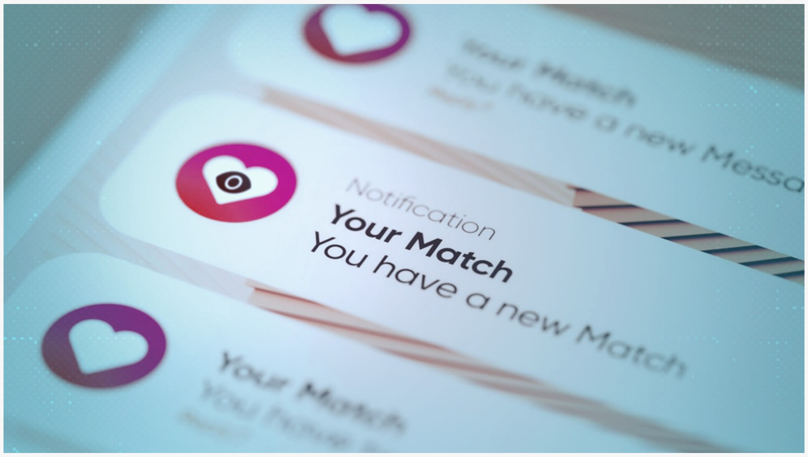
EINPRESSWIRE

Fake dating app used as lure in spyware campaign targeting Pakistan, ESET Research discovers



DUBAI , DUBAI, UNITED ARAB EMIRATES, February 3, 2026 /EINPresswire.com/ -- ESET researchers have uncovered an Android spyware campaign leveraging romance scam tactics to target individuals in Pakistan. The campaign uses a malicious app posing as a chat platform that allows users to initiate conversations operated via WhatsApp. Underneath the romance charade, the real purpose of the malicious app, which ESET named GhostChat, is exfiltration of the victim’s data. The same threat actor appears to be running a broader spy operation – including a ClickFix attack leading to the compromise of victims’ computers, and a WhatsApp device-linking attack gaining access to victims’ WhatsApp accounts – thus expanding the scope of surveillance. These related attacks used websites impersonating Pakistani governmental organizations as lures. Victims obtained GhostChat from unknown sources, and it requires manual installation; it was never available on Google Play, and Google Play Protect, which is enabled by default, protects against it.

“This campaign employs a method of deception that we have not previously seen in similar schemes – fake female profiles in GhostChat are presented to potential victims as locked, with passcodes required to access them. However, as the codes are hardcoded in the app, this is just a social engineering tactic likely aimed to create the impression of exclusive access for the potential victims,” says ESET researcher Lukáš Štefanko, who discovered the campaign. “Our investigation reveals a highly targeted and multifaceted espionage campaign aimed at users in Pakistan,” he adds.

The app uses the icon of a legitimate dating app but lacks the original app’s functionality and instead serves as a lure – and tool – for espionage on mobile devices. Once logged in, victims are presented with a selection of 14 female profiles; each profile is linked to a specific WhatsApp number with a Pakistani (+92) country code. The use of local numbers reinforces the illusion that the profiles are real individuals based in Pakistan, increasing the credibility of the scam. Upon entering the correct code, the app redirects the user to WhatsApp to initiate a conversation with the assigned number – presumably operated by the threat actor.

While the victim engages with the app, and even prior to logging in, GhostChat spyware has already begun running in the background, silently monitoring device activity and exfiltrating sensitive data to a C&C server. Beyond initial exfiltration, GhostChat engages in active espionage: It sets up a content observer to monitor newly created images and uploads them as they appear. Additionally, it schedules a periodic task that scans for new documents every five minutes, ensuring continual surveillance and data harvesting.

The campaign is also connected to broader infrastructure involving ClickFix-based malware delivery and WhatsApp account hijacking techniques. These operations leverage fake websites, impersonation of national authorities, and deceptive, QR-code-based device-linking to compromise both desktop and mobile platforms. ClickFix is a social engineering technique that tricks users into manually executing malicious code on their devices by following seemingly legitimate instructions.

In addition to desktop targeting via the ClickFix attack, a malicious domain was used in a mobile-focused operation aimed at WhatsApp users. Victims were lured into joining a supposed community – posing as a channel of the Pakistan Ministry of Defence – by scanning a QR code to link their Android device or iPhone to WhatsApp Web or Desktop. Known as GhostPairing, this technique allows an adversary to gain access to the victims' chat history and contacts, acquiring the same level of visibility and control over the account as the owners, effectively compromising their private communications.

For a more detailed analysis of GhostChat, check out the latest ESET Research blog post, "Love? Actually: Fake dating app used as lure in targeted spyware campaign in Pakistan" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research..

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here