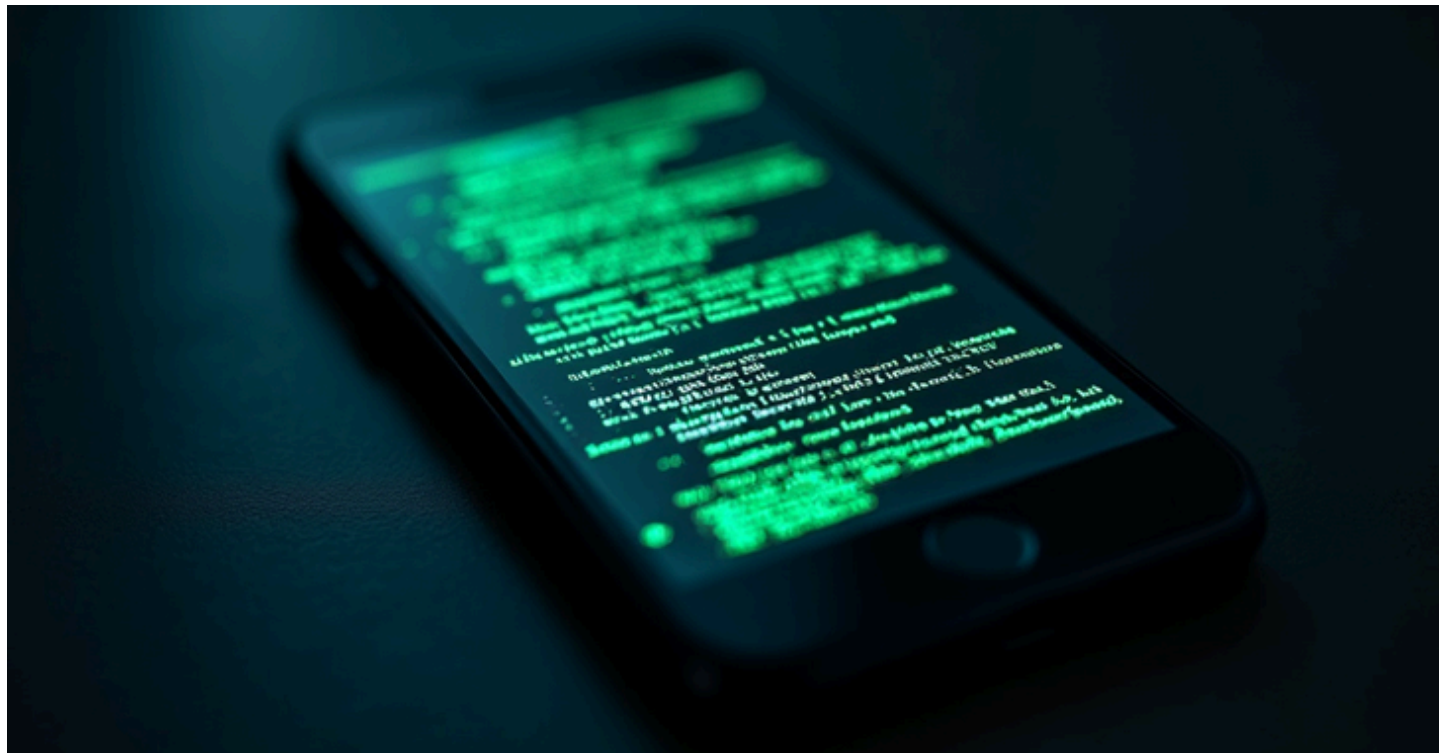


# Watering Hole Attack on Kurdish Sites Distributing Malicious APKs and Spyware

The Hacker News : 4-5 minutes

Cyber Espionage / Mobile Security



As many as 25 websites linked to the Kurdish minority have been compromised as part of a watering hole attack designed to harvest sensitive information for over a year and a half.

French cybersecurity firm Sekoia, which disclosed details of the campaign dubbed SilentSelfie, described the intrusion set as long-running, with first signs of infection detected as far back as December 2022.

The strategic web compromises are designed to deliver four different variants of an information-stealing framework, it added.

## Top 2024 SaaS Security Risks

[READ THE REPORT](#)



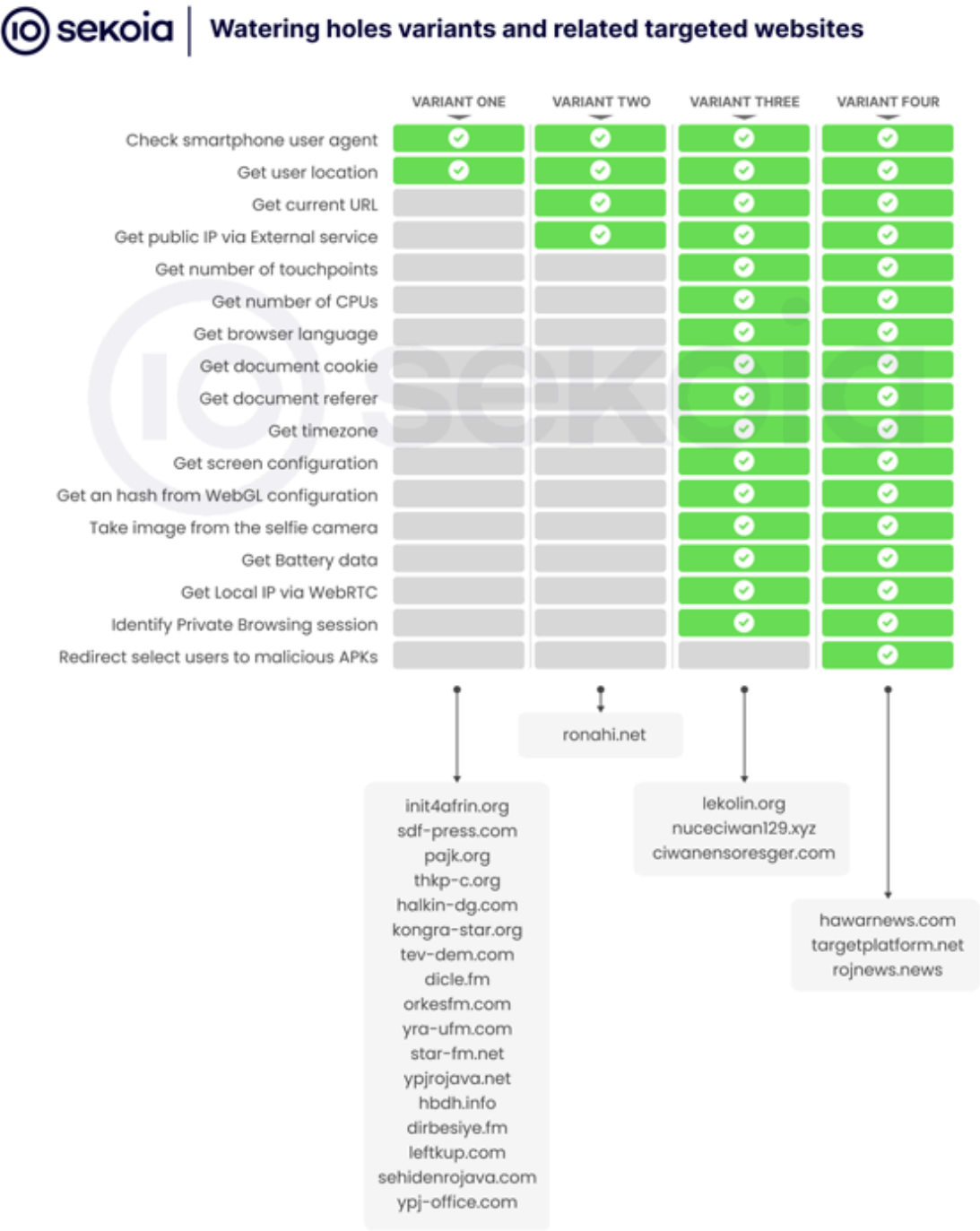
"These ranged from the simplest, which merely stole the user's location, to more complex ones that recorded images from the selfie camera and led selected users to install a malicious APK, i.e an application used on Android," security researchers Felix Aimé and Maxime A [said](#) in a Wednesday report.

Targeted websites include Kurdish press and media, Rojava administration and its armed forces, those related to revolutionary far-left political parties, and organizations in Türkiye and Kurdish regions. Sekoia told The Hacker News that the exact method by which these websites were breached in the first place remains uncertain.

The attacks have not been attributed to any known threat actor or entity, indicating the emergence of a new threat cluster targeting the Kurdish community, which has been previously singled out by groups like [StrongPity](#) and [BladeHawk](#).

Earlier this year, Dutch security firm Hunt & Hackett also revealed that Kurdish websites in the Netherlands were singled out by a Türkiye-nexus threat actor known as [Sea Turtle](#).

The watering hole attacks are characterized by the deployment of a malicious JavaScript that's responsible for gathering various kinds of information from site visitors, including their location, device data (e.g., number of CPUs, battery status, browser language, etc.), and public IP address, among others.

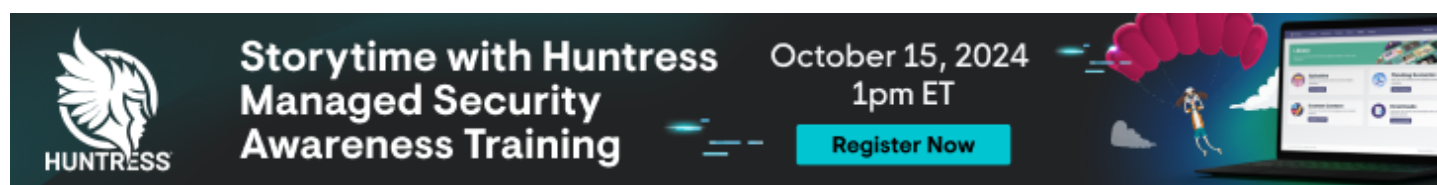


One variant of the reconnaissance script found on three websites (rojnews[.]news, hawarnews[.]com, and targetplatform[.]net.) has also been observed redirecting users to rogue Android APK files, while some others include the ability for user tracking via a cookie named "sessionIdVal."

The Android app, per Sekoia's analysis, embeds the website itself as a WebView, while also clandestinely hoovering system information, contact lists, location, and files present in the external

storage based on the permissions granted to it.


"It is worth noting that this malicious code doesn't have any persistence mechanism but is only executed when the user opens the RojNews application," the researchers pointed out.



"Once the user opens the application, and after 10 seconds, the LocationHelper service starts beaconing the background to the URL rojnews[.]news/wp-includes/sitemaps/ via HTTP POST requests, sharing the current location of the user and waiting for commands to execute."

Not much is known about who is behind SilentSelfie, but Sekoia has assessed that it could be the handiwork of the [Kurdistan Regional Government](#) of Iraq based on the arrest of RojNews journalist Silêman Ehmed by KDP forces in October 2023. He was [sentenced](#) to three years in prison in July 2024.

"Even though this watering hole campaign is of low sophistication, it is notable for the number of kurdish websites affected and its duration," the researchers said. "The campaign's low level of sophistication suggests it might be the work of an uncovered threat actor with limited capabilities and relatively new to the field."

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.