SpyNote Android malware spreads via fake volcano eruption alerts

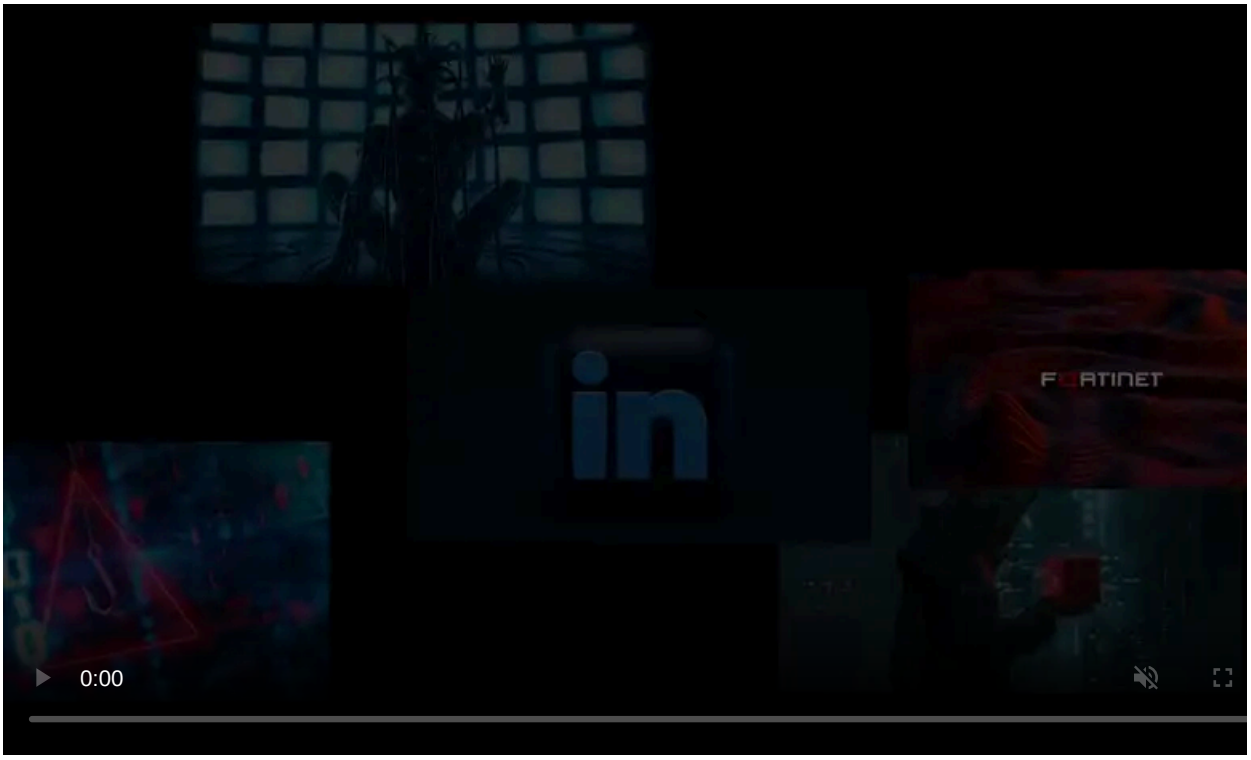
By Bill Toulas

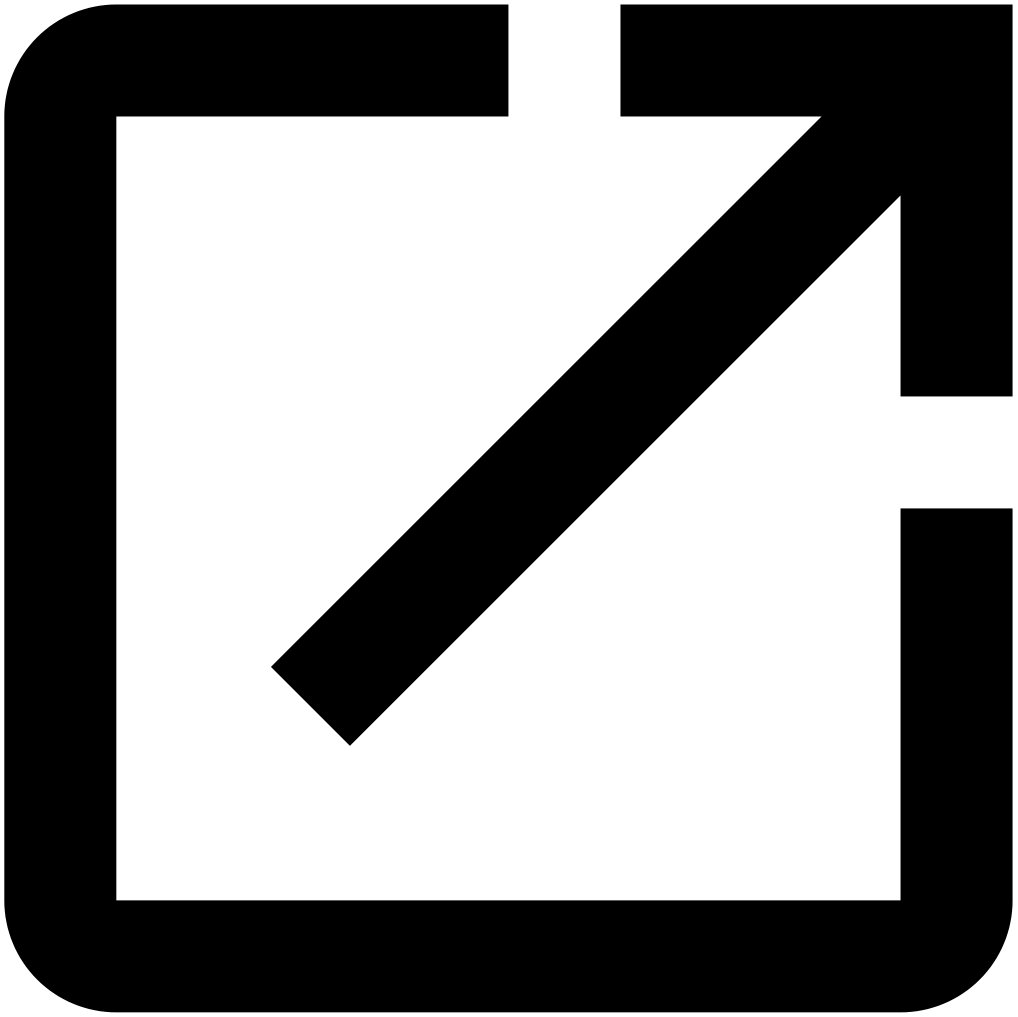
Published: 2023-10-17 · Archived: 2026-04-05 19:41:46 UTC

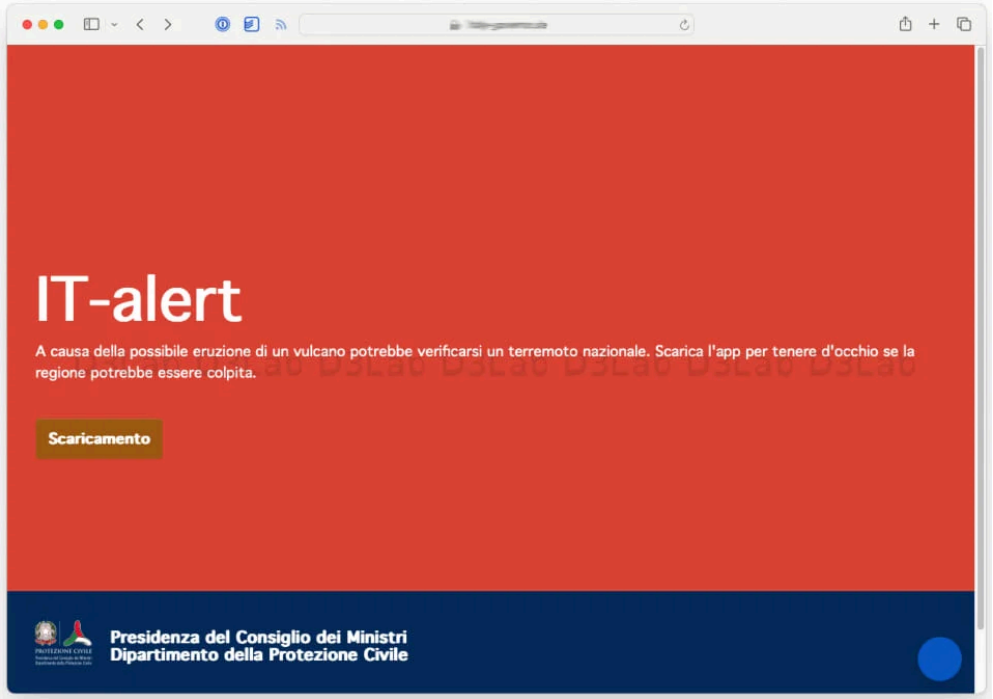
The Android 'SpyNote' malware was observed in attacks targeting Italy using a fake 'IT-alert' public alert service that infected visitors with the information-stealing malware.

IT-alert is a legitimate public service operated by the Italian government, specifically the Department of Civil Protection, to provide emergency alerts and guidance to the population during imminent or ongoing disasters such as wildfires, floods, earthquakes, etc.

Italian researchers at the D3Lab first spotted the fake IT-alert site, which is warning of an elevated possibility of an upcoming volcano eruption, urging visitors to install the app to remain informed.


0:00

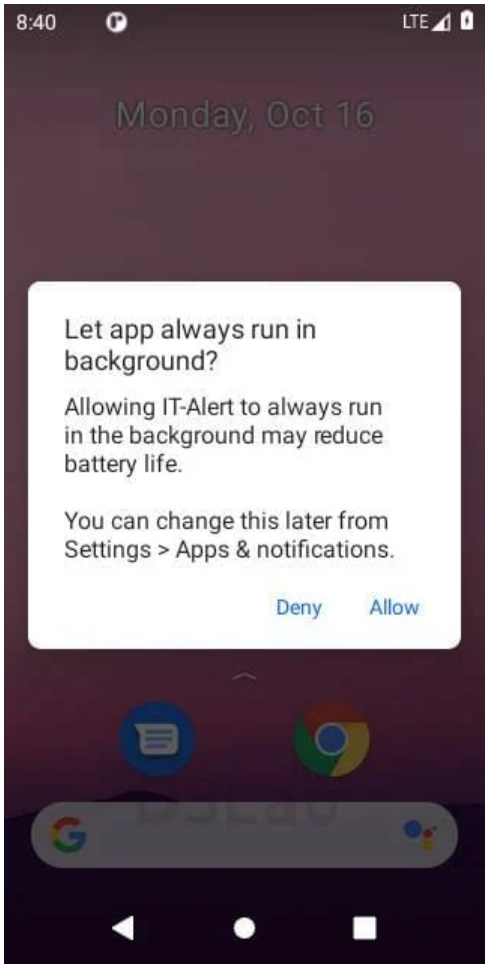




Fake IT-alert website pushing SpyNote *(D3 Labs)*

If the download button is clicked from an iOS device, the user is redirected to the real IT-alert site, but Android users attempting to download the app directly receive 'IT-Alert.apk.'

The APK (Android package) file installs SpyNote malware on the device, granting it permission to use Accessibility services, which enable the attackers to perform a wide range of dangerous and invasive actions on the compromised device.



App requesting to run in the background
(D3Lab)

SpyNote can also perform overlay injection attacks to steal user credentials when the victim opens banking, cryptocurrency wallet, and social media applications.

Other documented capabilities of the particular malware include camera recording, GPS and network location tracking, standard keylogging, screenshot capturing, phone call recording, and targeting Google and Facebook accounts.

SpyNote spikes after source code leak

The SpyNote Android malware was first documented in 2022 and is now in its third major version, which is sold to cybercriminals through Telegram.

In January 2023, a ThreatFabric report warned that SpyNote detections spiked following the source code leak of one of its variants, codenamed 'CypherRat.'

Some of those who got their hands on the leaked source code created custom variants targeting specific banks, while others opted to masquerade it as Google's Play Store, Play Protect, WhatsApp, and Facebook.

Late last week, a report from F-Secure highlighted the rising prominence of SpyNote, providing a detailed analysis of its features and capabilities.

To defend from these threats, avoid downloading and installing APKs from outside the Play Store unless you specifically trust the publisher.

Update 10/18 - A Google spokesperson confirmed via a comment sent to BleepingComputer that SpyNote is not present on any apps available on Google Play, Android's official app store.

> Based on our current detection, no apps containing this spyware are found on Google Play. Google implemented user protections for this spyware ahead of this report's publication.
>
> Users are protected by Google Play Protect, which can warn users or block apps known to exhibit malicious behavior on Android devices with Google Play Services. - Google

---

Source: https://www.bleepingcomputer.com/news/security/spynote-android-malware-spreads-via-fake-volcano-eruption-alerts/