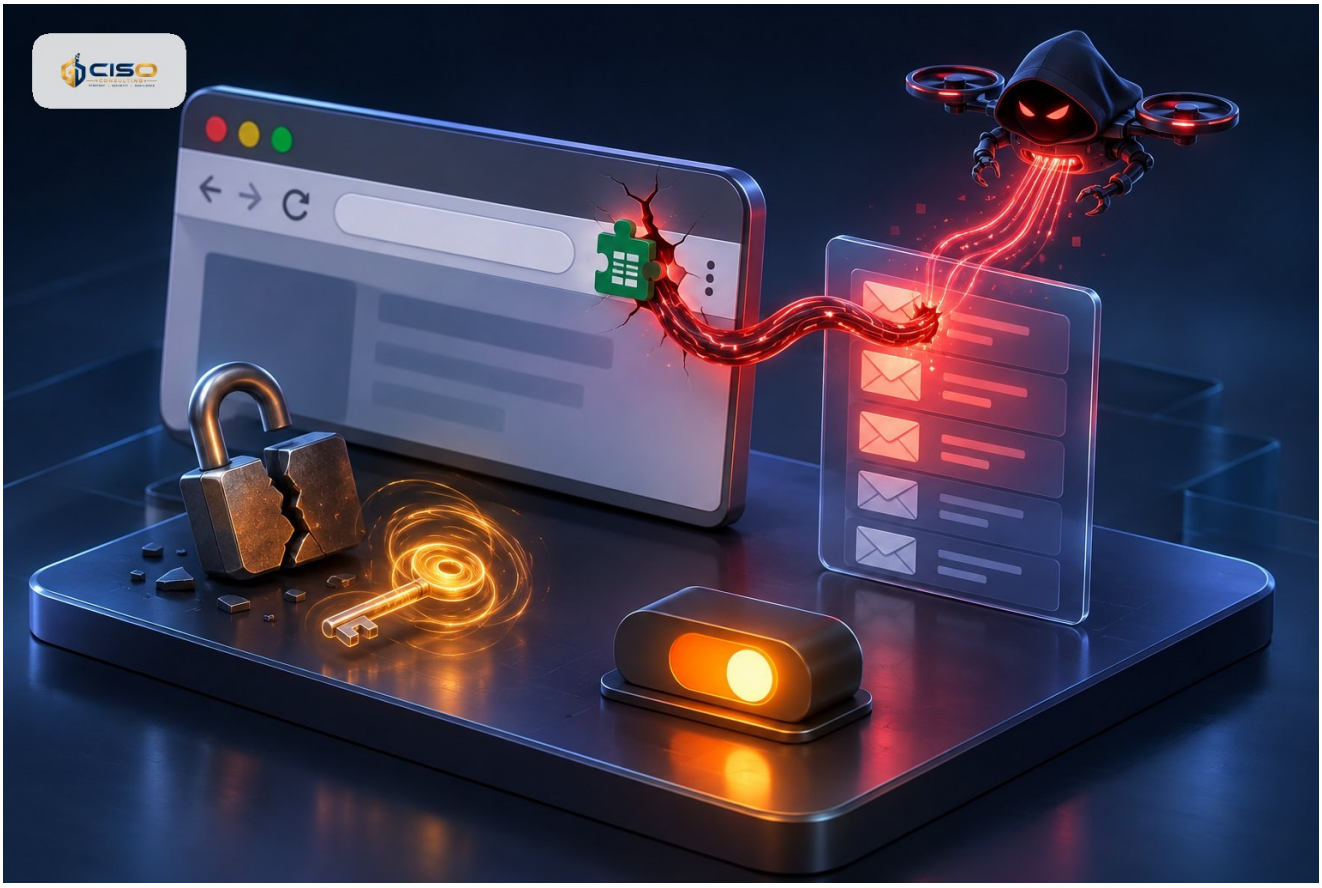
Remus infostealer uses fake Google Sheets Chrome extension to read Gmail



Researchers found that the Remus infostealer's advertised Gmail "zero-day" is a malicious Chrome extension that keeps reading unread emails after password changes. Defenders should review browser extensions and Developer Mode.

- Remus operators advertised a Gmail zero-day from November 8; researchers found it was a malicious Chrome extension, not a Google flaw.
- The extension survives password changes and session revocation because it stays installed; it only reads mail while the user is signed in.
- It is named "Google Sheets", copies the Google Docs Offline description and requests access to all websites.
- It checks for unread emails every minute across up to 10 account slots and sends subject, body,

> sender and victim address to a command-and-control server.
>
> - Remus enables Developer Mode and edits the Chrome profile to get around the removal of a command-line option in Chrome 137 and later.

Researchers at GenDigital and Invoke RE have explained how the Remus infostealer reads Gmail messages. The malware's developer began advertising a Gmail zero-day on November 8, claiming emails could be collected even after victims changed passwords and revoked sessions. Hudson Rock looked into the claim and could not confirm it, finding no technical proof of a zero-day.

How the technique works

According to the independent analysis, no vulnerability is involved. The malware drops a native DLL whose only job is to install a malicious extension in Google Chrome, the only browser it targets. The extension is bundled inside the DLL as an unencrypted ZIP archive.

Chrome 137 and later removed a command-line option that malware used to load extensions. Remus works around this by editing the victim's Chrome profile to register the extension and then turning on Developer Mode, which unpacked extensions require.

The extension presents itself as "Google Sheets", copies the description of Google Docs Offline and asks for access to all websites. Once running, it checks for unread emails every minute across up to 10 account slots and retrieves them in full. It sends the subject, body, sender and the victim's address to its command-and-control server with a campaign identifier. Failed uploads are retried, and a local record avoids duplicates.

What this means for defenders

Because the extension remains in the browser, changing a password or revoking sessions does not remove it. Its access pauses when the session ends and resumes when the user signs in again. Incident response for a suspected infection therefore has to include cleaning the endpoint, not only resetting credentials. The source advises downloading software from trusted sources only and checking chrome://extensions for rogue entries or unexpected Developer Mode.

What to do now

1. Audit Chrome extensions on managed endpoints and remove any unapproved ones, especially those named "Google Sheets" that are not from the official store.
2. Detect and alert on Developer Mode being enabled in Chrome, and restrict it through browser policy where possible.
3. When a Gmail compromise is suspected, reimage or clean the endpoint as well as resetting passwords and revoking sessions.
4. Restrict software installation to trusted, approved sources and remind staff not to download tools from

unverified sites.

5. Review outbound traffic from endpoints for unexpected connections that may indicate extension-based exfiltration.