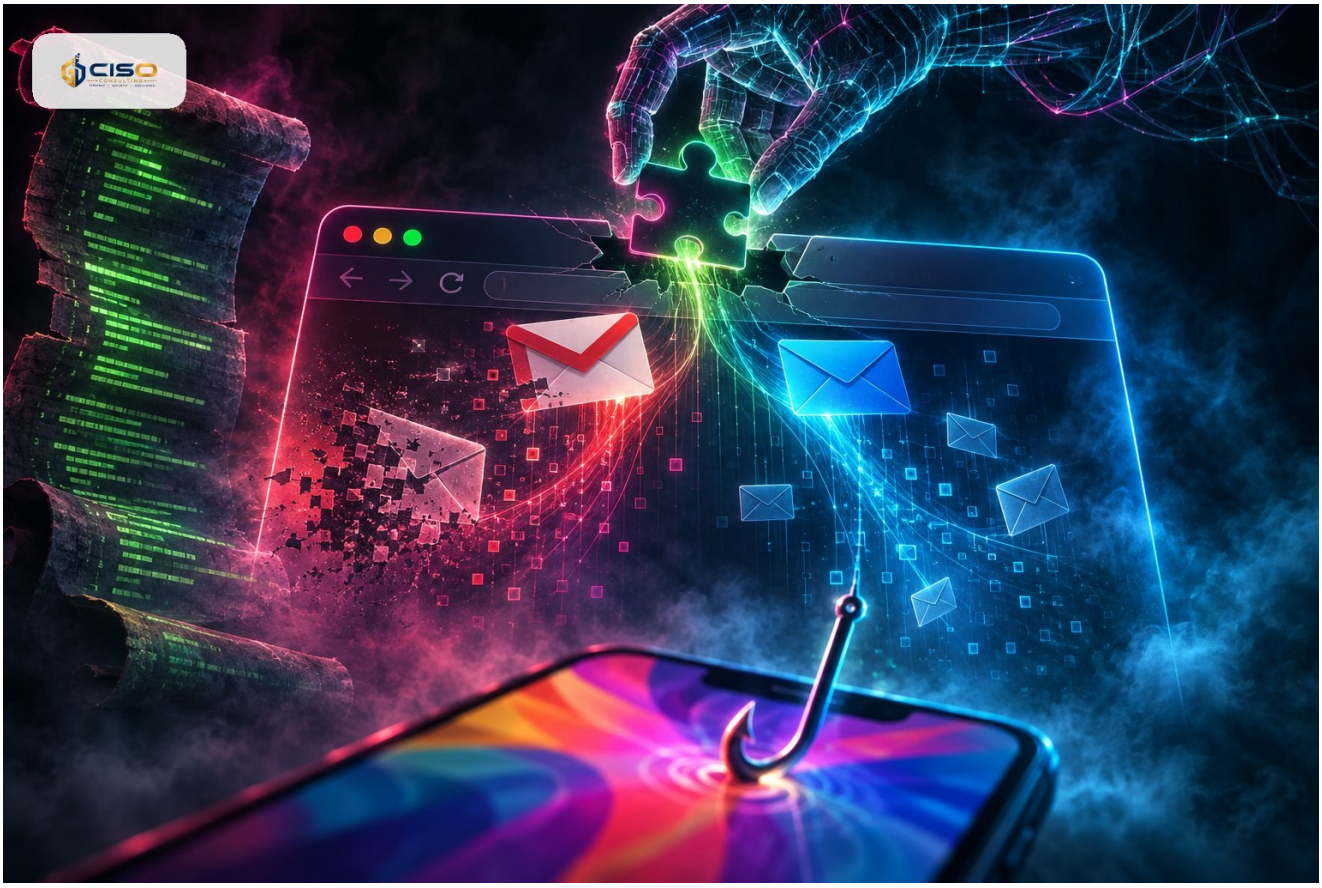
SYS010 infostealer uses browser management policies to spy on Gmail and Outlook



Bitdefender reports a new SYS01 variant, SYS010, spread through Meta ads for fake wallpaper apps. It force-installs browser extensions via management policies to steal sessions and read or delete Gmail and Outlook email.

- Malicious Meta ads promote fake Wallpaper Engine and Lively Wallpapers apps for Windows; the wallpapers work while malware installs in the background.
- The malware enrols Chrome in an attacker-controlled Google admin console, uses an ExtensionSettings policy in Firefox, and can enrol Edge devices in an attacker-controlled MDM server.
- It repeats the UAC prompt every three seconds, up to 99 times, until the user approves.
- The extensions steal session cookies, bypassing passwords and two-factor checks, and the Chrome

one can read and permanently delete Gmail and Outlook messages.

- Bitdefender notes that request counts by country do not reflect confirmed infections.

Bitdefender Labs has described a campaign it tracks as SYS010, likely a new version of the SYS01 infostealer seen in Facebook malvertising since at least 2022. The researchers identified a malicious ad on October 16 and found the campaign still running, with hundreds of ads created.

How the attack works

The ads impersonate Wallpaper Engine and Lively Wallpapers and send Windows users to malicious download sites, some with domains made to look official. The installed app delivers the promised animated wallpapers, which masks the malicious activity.

A script then changes browser management policies to force-install extensions in Chrome, Edge and Firefox. These changes need administrator rights, so the malware shows the UAC prompt every three seconds, up to 99 times, until the user approves. Once installed, the extensions cannot be disabled or removed by the user.

What is exposed

The extensions pose as document tools and are distributed outside the Chrome Web Store. They steal session cookies, which gives the operator access to signed-in accounts without passwords or two-factor challenges. They also collect details of Facebook Pages, advertising and business accounts, including spending and payment data. The Chrome extension can read recent Gmail and Outlook messages and permanently delete selected ones, which could let attackers intercept login codes and remove security alerts.

Bitdefender stresses that the country-level request figures it observed are not confirmed infections. For businesses, stolen advertising accounts can mean unauthorized charges, lost access to social media accounts and exposed customer conversations.

What to do now

1. Check managed and unmanaged Windows endpoints for unexpected browser management enrolment, such as a "managed by your organization" notice that IT did not configure.
2. Review Chrome, Edge and Firefox policies for force-installed extensions you did not approve, especially document-tool add-ons installed outside official stores.
3. Restrict software installation from social-media ads and train staff to refuse UAC prompts with no clear purpose.
4. Review who has access to corporate Meta business and advertising accounts, remove unneeded permissions, and check for unfamiliar ads, payment changes or spending.
5. If infection is suspected, revoke active sessions and reset credentials for email and business accounts from

a clean device, and review mailboxes for deleted security alerts.