Can ransomware still reach data stored in cloud services like OneDrive or Google Drive?

Short answer: Yes. While cloud storage was once out of reach for ransomware, attackers have adapted their methods and can now target cloud-stored data through techniques like drive mapping and, more commonly today, theft of API keys and session tokens.

How ransomware's approach to cloud data has changed

When remote work drove a rapid shift toward cloud storage, both businesses and cybercriminals were adjusting to the new environment at the same time. In the early stages of this shift, ransomware typically could not touch files stored in cloud platforms — if data lived in the cloud rather than on a local server, attackers generally left it alone because they lacked a direct path to it.

That changed as attackers learned to manually connect cloud storage, such as an Amazon, OneDrive, or Google Drive account, to an infected system. They did this by mounting the cloud storage as a local drive letter, similar to how a USB device appears as its own drive on a computer. Once mounted this way, the cloud-based files became just as exposed to encryption as files on a local hard drive.

Today's bigger threat: stolen keys and tokens

As cloud usage matured, attacker tactics shifted again. Rather than manually mounting drives, many now go after API keys and session tokens — credentials that grant direct, program-level access to cloud accounts and data. Gaining one of these is comparable to stealing a password, except it often provides broader and faster access to cloud resources than a stolen password alone.

This shift matters because the same speed and scalability that make cloud computing valuable for legitimate IT teams are now available to attackers as well. Among Cyber Crucible clients last year,

more than half experienced an attempted theft of a cloud session token aimed at hijacking a user's active session, while fewer than 9% saw any actual data compromise. This suggests attackers are prioritizing credential and token theft as their primary entry point, with data theft as a secondary goal.

Is cloud data automatically safe?

Cloud storage does not guarantee protection from ransomware or data theft. It simply changes the method attackers must use to reach that data — shifting the primary risk toward credential and session token compromise rather than direct file encryption.

https://player.vimeo.com/video/1047006345

Watch on Vimeo · Captions: English, Français, Español, العربية

Revision #4
Created 2026-07-23 23:17:36 UTC by Dennis Underwood
Updated 2026-07-24 00:31:00 UTC by Dennis Underwood