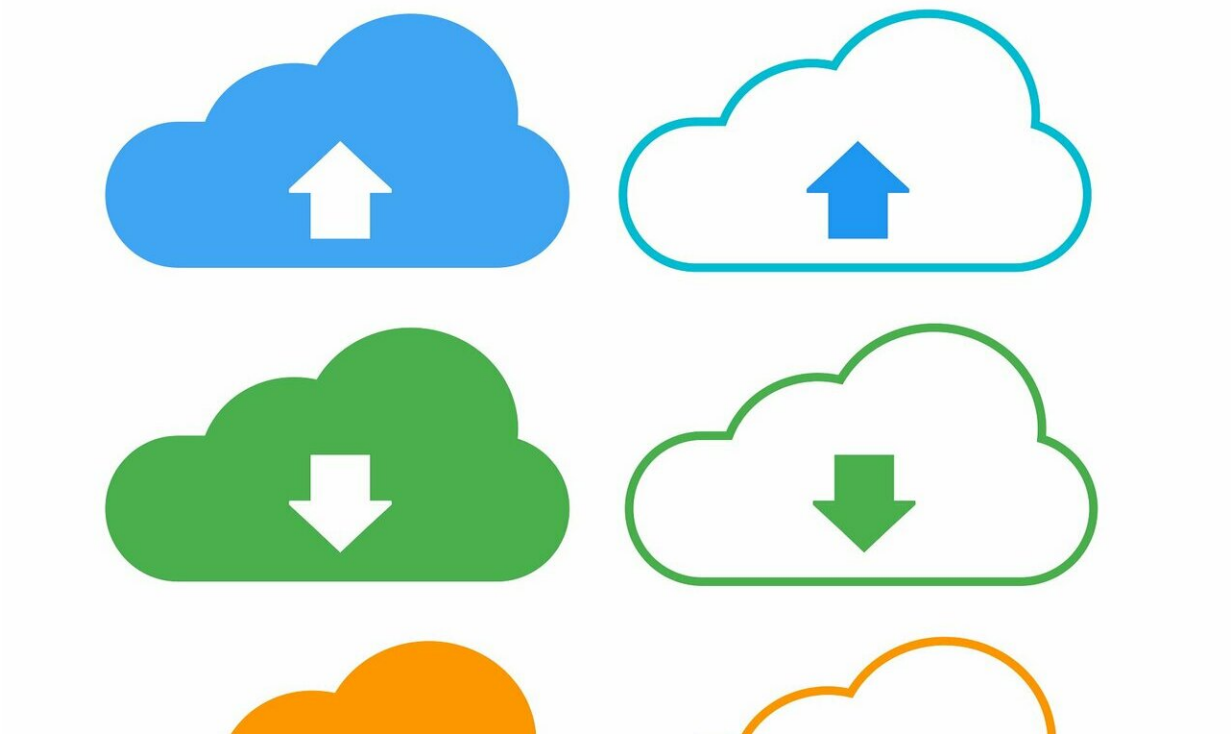
Mismanaged cloud services put user data at risk

April 11 2022, by Eric Pauley



Credit: CC0 Public Domain

Organizations' failure to properly manage the servers they lease from cloud service providers can allow attackers to receive private data, research my colleagues and I conducted has shown.

Cloud computing allows businesses to lease servers the same way they

lease office space. It's easier for companies to build and maintain mobile apps and websites when they don't have to worry about owning and managing servers. But this way of hosting services raises security concerns.

Each cloud server has a unique IP address that allows users to connect and send data. After an organization no longer needs this address, it is given to another customer of the service provider, perhaps one with malicious intent. IP addresses change hands as often as every 30 minutes as organizations change the services they use.

When organizations stop using a cloud server but fail to remove references to the IP address from their systems, users can continue to send data to this address, thinking they are talking to the original service. Because they trust the service that previously used the address, user devices automatically send sensitive information such as GPS location, financial data and browsing history.

An attacker can take advantage of this by "squatting" on the cloud: claiming IP addresses to try to receive traffic intended for other organizations. The rapid turnover of IP addresses leaves little time to identify and correct the issue before attackers start receiving data. Once the attacker controls the address, they can continue to receive data until the organization discovers and corrects the issue.

Our study of a small fraction of cloud IP addresses found thousands of businesses that were potentially leaking user data, including data from mobile apps and advertising trackers. These apps initially intended to share personal data with businesses and advertisers, but instead leaked data to whoever controlled the IP address. Anyone with a cloud account could collect the same data from vulnerable organizations.

Why it matters

Smartphone users share personal data with businesses through the apps they install. In a recent survey, researchers found that half of smartphone users were comfortable sharing their locations through smartphone apps. But the personal information users share through these apps could be used to steal their identity or hurt their reputation.

Personal data has seen increasing regulation in recent years, and users may be content to trust the businesses they interact with to follow those regulations and respect their privacy. But these regulations may not sufficiently protect users. Our research shows that even when companies intend to use data responsibly, poor security practices can leave that data up for grabs.

Users should know that when they share their private or personal data with companies, they are also exposed to the security practices of those companies. They can take steps to reduce this exposure by reducing how much data they share and with how many organizations they share it.

What other research is being done in this field

Academics and industry are focusing on responsible collection of user data. A recent push by Google aims to reduce collection of users' personal data by mobile advertisements, ensuring that their security and privacy is protected.

At the same time, researchers are working to better explain what applications do with the data they collect. This work aims to ensure that the data users share with applications is used how they expect by matching permission prompts with how the apps actually behave.

What's next

We're conducting research into new technologies on smartphones and devices to ensure they protect user data. For instance, research led by a colleague of mine describes an approach to protect personal data collected by smart cameras. Our vantage point on traffic in the public cloud is also enabling new studies of the internet as a whole. We are continuing to work with cloud providers to ensure that user data stored on the cloud is secure, and are introducing techniques to prevent businesses and their customers from being victimized on the cloud.

Provided by The Conversation