Cloud server leasing can leave sensitive data up for grabs

April 11 2022

Credit: Pixabay/CC0 Public Domain

Renting space and IP addresses on a public server has become standard business practice, but according to a team of Penn State computer scientists, current industry practices can lead to "cloud squatting," which

can create a security risk, endangering sensitive customer and organization data intended to remain private.

Cloud squatting occurs when a company, such as your bank, leases space and IP addresses—unique addresses that identify individual computers or computer networks—on a public server, uses them, and then releases the space and addresses back to the public server company, a standard pattern seen every day. The public server company, such as Amazon, Google, or Microsoft, then assigns the same addresses to a second company. If this second company is a bad actor, it can receive information coming into the address intended for the original company—for example, when you as a customer unknowingly use an outdated link when interacting with your bank—and use it to its advantage—cloud squatting.

"There are two advantages to leasing server space," said Eric Pauley, doctoral candidate in computer science and engineering. "One is a cost advantage, saving on equipment and management. The other is scalability. Leasing server space offers an unlimited pool of computing resources so, as workload changes, companies can quickly adapt." As a result, the use of clouds has grown exponentially, meaning almost every website a user visits takes advantage of cloud computing.

While the Penn State researchers suspected cloud squatting was possible, they designed an experiment to determine if cloud tenants were vulnerable and to quantify the extent of the problem. The researchers set up a series of cloud server rentals from Amazon Web Services' in its us east 1 region, the region that serves the East Coast of the U.S. They rented server space for 10-minute intervals, received information sent to the address intended for previous tenants and then moved to another server location, repeating the process. They did not ask for any data, nor did they send out any data. Whatever unsolicited data they received was potentially intended for previous tenants.

For example, if a mobile banking company rented server space, they would receive an IP address from the public cloud-services company. After they relinquished that server space and IP address, the next tenant of that space could receive any personal financial data sent by the bank's customer to the IP address.

The researchers note in the Proceedings of the 43rd IEEE Symposium on Security and Privacy that they "deployed over 3 million servers receiving 1.5 million unique IP addresses over 101 days." They identified cloud servers, third-party services and Domain Name Servers (DNS) as sources of potentially serious security breaches.

"The previous perception was that DNS was the sole risk," said Pauley. "So, if DNS was secure, it was fine. Unfortunately, this was not a panacea."

In the 5 million pieces of data they received, many contained sensitive information including financial transactions, GPS locations and personal identifiable information.

"We did not knowingly receive health data but did confirm that an adversary could receive that data," said Patrick McDaniel, holder of the William L. Weiss Chair in Information and Communications Technology in the School of Electrical Engineering and Computer Science, Penn State. "For example, requests received by one of our IP addresses were to the web site for Health and Human Services, HHS.gov. We did not further interact, but others could pretend to be an HHS service and get people to interact." In this case, from the user's perspective, they would believe they were talking to a legitimate government agency, exposing sensitive personal and health data.

If companies use cloud messaging internally or cloud print services, then when those IP addresses are let go, information requests sent to those

services by company staff who mistakenly attempt to use the old addresses or who are unaware that the addresses have changed can get into the wrong hands.

"Our experiment collected, encrypted and sent anything we got off to a secure location for analyses," said McDaniel. "We also took additional steps to ensure that any detected user data was protected."

McDaniel notes that the research was performed in compliance with Amazon's Vulnerability Reporting program, which allows security researchers who are acting in good faith to conduct their research.

The researchers immediately contacted the three major cloud server companies, AWS, Microsoft and Google, as well as vulnerable US Government agencies, to inform them of the vulnerabilities in their server practices. Amazon, after reviewing the information and an internal audit, is implementing a series of practices to try to contain cloud squatting on their servers.

To resolve cloud squatting concerns, the researchers believe that there are mitigation efforts that should be made by both the cloud server companies and the clients who rent server space. From the cloud server side, one of the ways to thwart cloud squatting is to prevent IP address reuse. However, this is limited by the number of available IP addresses.

Second, "server companies can create reserved IP address blocks," said McDaniel. "A large client organization could be assigned a fixed range of addresses that are recyclable within the company."

Third, server companies can delay recycling of IP addresses, but the longer IP addresses are idle, the more it will cost the server company.

From the client side, users can avoid producing IP address

configurations that linger after cloud server IP addresses are let go. However, the researchers found that this rarely happens because there is often limited central control and oversight of IP address configurations within an organization. During interviews with affected cloud server users, the researchers found that many organizations have little visibility into how the dozens or hundreds of different accounts using cloud computing capabilities are being used and, most importantly, decommissioned, by departments and employees.

"Generally speaking, the users fail to remove configurations that point to IP addresses on cloud servers," said McDaniel. "It could be a decommissioned printer that is still in the menu or a domain name or a sticky note saying connect to a specific address. Because the problems are very broad and dispersed across many, many users, it can be very difficult to have overall methods to fix them. However, the common threads are a failure to monitor and decommission outdated configurations."

IP addresses used to be long-lived or static, but now they are dynamic, changing in hours or minutes. This introduces a large class of vulnerability, according to the researchers.

"I would heed the conclusion that despite the overwhelming attraction of cloud servers, cloud computing is not without risk," said Pauley. "However, by managing and watching their use, we can mitigate a lot of that danger. The free lunch that people thought the clouds were is not free. Companies have to weigh the risk to benefit."

More information: Measuring and Mitigating the Risk of IP Reuse on Public Clouds, Proceedings of the 43rd IEEE Symposium on Security and Privacy, 2022.

Provided by Pennsylvania State University