Attackers Scrape GitHub For Cloud Service Credentials, Hijack Account To Mine Virtual Currency

By Runa A. Sandvik

Published: 2014-01-14 · Archived: 2026-04-29 07:18:28 UTC

Rich Mogull, CEO at information security research and advisory firm Securosis, was working on a piece of code to accompany his presentation at the upcoming RSA Conference when he accidentally published the credentials for his AWS account--Amazon's cloud computing service--online. A mistake that would later cost him $500.

Official Litecoin logo (from http://commons.wikimedia.org/)

In a blog post titled "My $500 Cloud Security Screwup", Mogull writes that he only learned about the issue when he received an email from Amazon's AWS team one evening. The email said that both his access and secret key were publicly available on GitHub, a web-based hosting service for software development projects. In addition, the AWS team had reason to believe someone used the credentials to set up a number of unauthorized servers in the Amazon cloud.

As soon as he had read the email, Mogull logged on to his AWS account and found that the perpetrators had set up no fewer than ten extra large cloud instances; five on the U.S. west coast, another five in Ireland. All instances had been running for 72 hours, which, Mogull writes, "means the bad guys found the credentials within about 36 hours of creating the project and loading the files" on GitHub.

"The attackers didn’t mess with anything active I was running," Mogull writes in the blog post. "That got me curious, because 10 extra large instances racking up $500 in 3 days initially made me think they were out to hurt me." As it turns out, the attackers were using his Amazon account to mine Litecoin, an alternative cryptocurrency created two years ago with a $600 million market cap.

Though the attackers did try to clean up their tracks, further analysis of one cloud instance revealed that not only were they using Tor to connect to the server, they also used Tor to connect to a Litecoin mining pool running as a previously unknown Tor Hidden Service. While most connections to the server appear to be coming from the Tor network, there are successful login connections from one host in Latvia and another in China.

In the blog post, Mogull concludes that attackers "are scraping GitHub for AWS credentials embedded in code (and probably other cloud services)," and use these to launch instances and mine virtual currencies, such as Bitcoin and Litecoin.

Mogull has since updated the post to say that Amazon has reached out and reversed the charges.

Mary Camarata, Amazon's Global Director of Public Relations, confirmed in an email that they monitor GitHub and similar sites as part of their operating procedures. "What the blogger experienced is basic fraud," she wrote. "To help protect our customers, we operate continuous fraud monitoring processes and alert customers if we find unusual activity."

Mogull says he considers himself lucky and writes that he is only out "45 minutes of investigation and containment effort." While the attackers would not have been able to lock him out of his own account, they could have cost him considerably more time and money.

-

You can follow me on Twitter and email me (GPG public key).
