Google’s Vertex AI Platform Gets Freejacked

By Michael Clark

Published: 2023-08-14 · Archived: 2026-04-05 20:25:17 UTC

The Sysdig Threat Research Team (Sysdig TRT) recently discovered a new Freejacking campaign abusing Google's Vertex AI platform for cryptomining. Vertex AI is a SaaS, which makes it vulnerable to a number of attacks, such as Freejacking and account takeovers. Freejacking is the act of abusing free services, such as free trials, for financial gain. This freejacking campaign leverages free Coursera courses that provide the attacker with no-cost access to GCP and Vertex AI. The attacker is able to generate free money while the service provider ends up footing the bill.

Using trial accounts seems inefficient on the surface, as many services require credit card checks and have other limiting features. However, we have observed attackers heavily automate the process and use sites which generate temporary email addresses, phone numbers, and even credit cards. CAPTCHAs are also a common defense, but we have seen attackers automate their resolution too. If scaled up, Freejacking can be an effective way to earn money.

In this attack, we observed dozens of instances being created per fake account. Each fake account was created with automation, so the attacker could have quite a few instances running. The trials themselves are often limited by time and resources, so the amount of money per instance is probably only a dollar or two for its lifetime. But with enough scale it can be worth the effort considering the cost of living where the attacker lives. We currently believe the attacker in this example is from Indonesia. Importantly, as we learned with PURPLEURCHIN, $1 of profit for an attacker can mean a $53 loss for the provider.

With AI being all the rage right now, these platforms are popping up all over the place. They are used to make machine learning/AI easier by providing pipelines and computing infrastructure, among a lot of other niceties. Part of the offering is compute infrastructure to train the models in a scalable and high-performance manner. With the AI gold rush occurring, teams all over the world are racing to field products, which means results first, and then "doing" security somewhere down the line.

These computing resources are what attackers are after and the graphics cards (GPU's) that come with them are ideal for mining cryptocurrency. GPU's have special chipsets which allow them to make calculations in a much more parallel way compared to CPU's. This parallelism allows the cryptomining program to perform roughly 6x better than a similar CPU. With this kind of hardware, attackers can earn more money, more quickly.

In this attack, the attacker leverages Jupyter Notebooks provided by the Vertex AI platform in order to run their miner. It's a rather simple, but effective tactic. A Jupyter Notebook is an interactive Python-based form which allows you to easily run code and commands while formatting the output. Since it provides such easy access to the command line, attackers are always happy to find them.

They run a script which creates three tensorflow instances in multiple regions. Tensorflow is a popular machine learning platform that can leverage GPU's and other specialized hardware. Next they use a custom GCP machine

type which launches a Tensorflow instance with 6 CPU's and 12GB of RAM. Tensorflow is the important aspect of the instances they are creating, as these images come with GPU's which can maximize cryptomining results.

```
 gcloud notebooks instances create tensorflow-1 --vm-image-project deeplearning-platform-release --vm-image-name

sleep 5

gcloud notebooks instances create tensorflow-2 --vm-image-project deeplearning-platform-release --vm-image-name

sleep 5

gcloud notebooks instances create tensorflow-3 --vm-image-project deeplearning-platform-release --vm-image-name

sleep 5
```

Once the Tensorflow instances are created, the attacker pulls down their miner from a public repository and runs it as long as they can. The cryptocurrency used in this attack is called Dero, another privacy focused coin similar to Monero. These coins are designed so it is difficult to track their transactions, making it a less risky choice for the attacker. The attacker launches their miner with a command like the one below.

```
 ./nodes -w deroi1qyzlxxgq2weyqlxg5u4tkng2lf5rktwanqhse2hwm577ps22zv2x2q9pvfz92xm369mdkp06lgvqf4y5cm.$(echo J6c
```

The IP Address in the "nodes" command, 149.129.237.206, is a mining pool controlled by the attacker hosted on an Alibaba server. The Dero wallet is a long unique string which is appended with an identifier (e.g. the date) which allows this mining instance to be considered a separate worker in the mining pool mainly for metrics. This miner will run until the users trial resources are expired.

Google's Vertex AI is not the only AI platform vulnerable to this type of attack, any service which offers free/trial compute can and will be used for freejacking. Either their free trials will be abused or their customers will be compromised and used to mine cryptocurrency. The shared responsibility model of security is important here as both the service providers and the customers need to ensure their ends are properly protected. Threat Detection and Response tools are very effective at countering cryptominers and should be used by both parties for runtime monitoring and suspicious account logins.

Source: https://sysdig.com/blog/googles-vertex-ai-platform-freejacked/