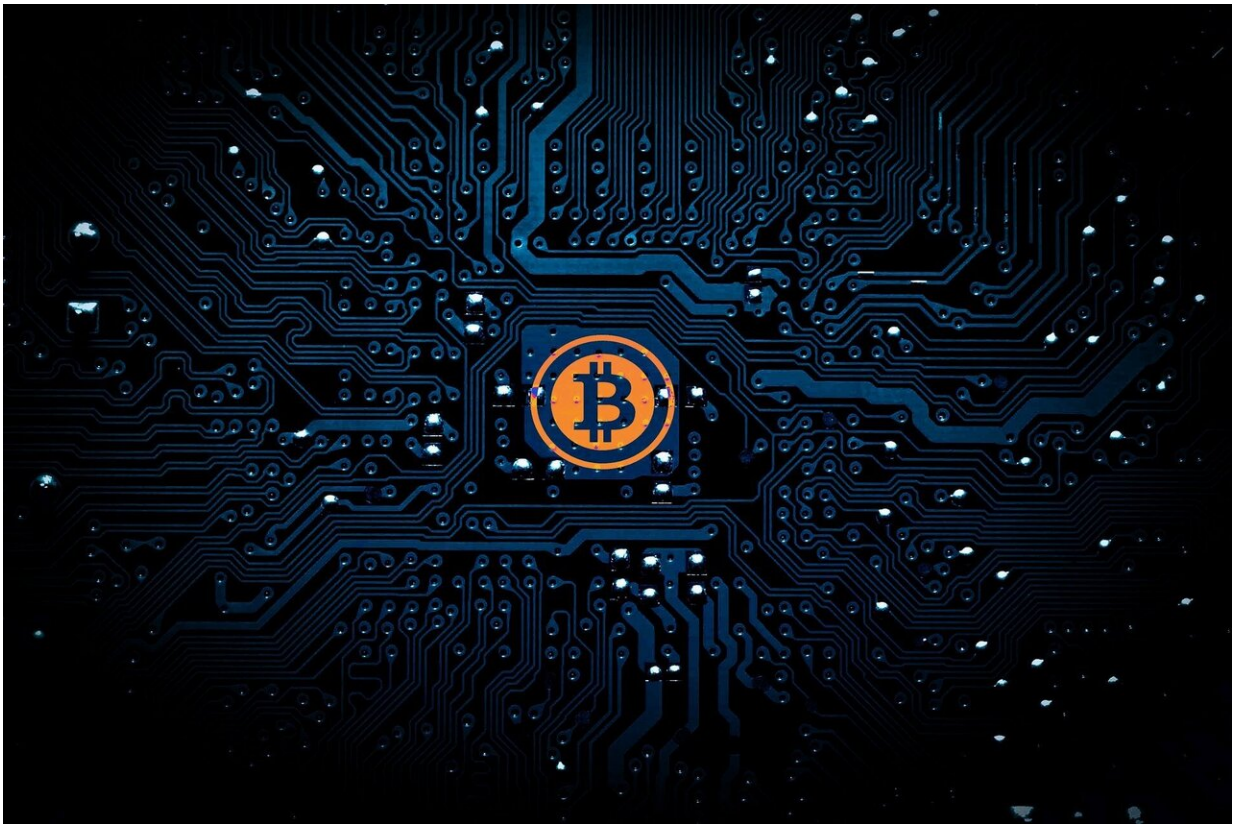
GitHub is investigating a crypto-mining campaign exploiting its server infrastructure

April 6 2021, by Sarah Katz



Credit: Pixabay/CC0 Public Domain

The Record, the news branch of the threat intelligence company Recorded Future, has reported that GitHub is currently looking into multiple attacks against its cloud infrastructure. These attacks have

enabled cybercriminals to exploit and implant the company's servers for use in illegal crypto-mining operations.

In progress since Fall of 2020, these attacks utilize a GitHub feature called GitHub Actions which allow users to automatically initiate tasks and workflows following a certain triggering event within one of their GitHub repositories.

Attackers perform this exploit by hijacking a legitimate repository, installing malicious GitHub Actions to the original code and then executing a Pull Request with the original repository in order to fuse the evil code and the legitimate code.

However, unlike some other GitHub attacks which depend on the project owner to first approve the malicious Pull Request, this attack runs off of simply filing that evil Pull Request. In fact, security research has shown that this attack specifically targets GitHub project owners who use automated workflows and automated jobs to test incoming Pull Requests. Therefore, as soon as a project owner runs a malicious Pull Request, GitHub's systems will process the attacker's code and open a virtual machine to download, install and run cryptocurrency-mining software on GitHub's infrastructure.

Indeed, security researchers have reported observing attackers initiate as many as 100 crypto-miners with a single attack, placing massive computational pressure for GitHub's infrastructure. So far, these attackers seem to be striking at random and at scale. Thus far, research has revealed at least one account running hundreds of Pull Requests containing malicious code.

The first instance of this attack was reported by a software engineer in France back in November of 2020. Similar to its reaction to the first incident, GitHub has reportedly claimed to be actively investigating this

ongoing attack. However, for now, GitHub seems to be going back and forth a lot with the attackers, as the hackers simply create new accounts once the company detects and deactivates infected accounts. Based on the attack visuals gathered so far, some of these attacks appear to initiate from a string of Chinese characters.

At present, the attackers do not seem to be actively targeting GitHub users at all, instead focusing on using GitHub's cloud infrastructure to host crypto-mining activities.

More information: Cimpanu, C. "GitHub Investigating Crypto-Mining Campaign Abusing Its Server Infrastructure." The Record by Recorded Future, The Record, 3 Apr. 2021, therecord.media/github-investi … rver-infrastructure/