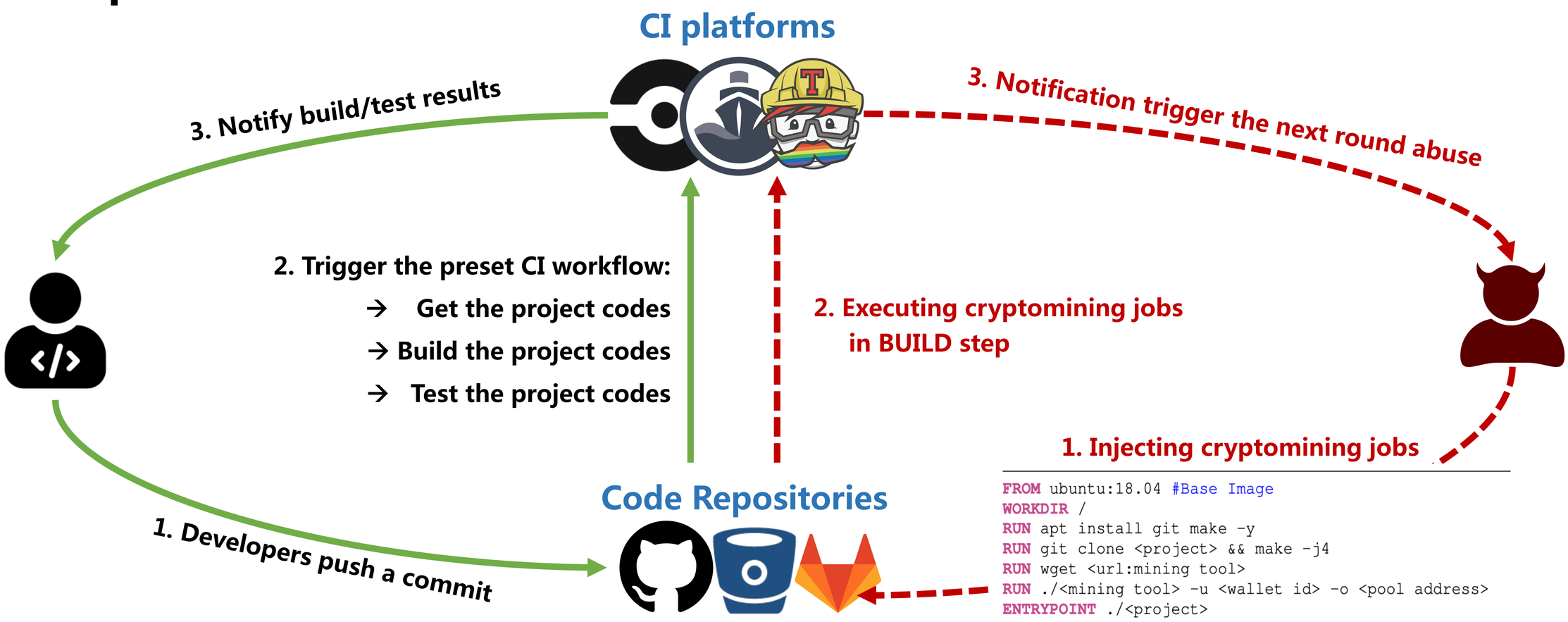
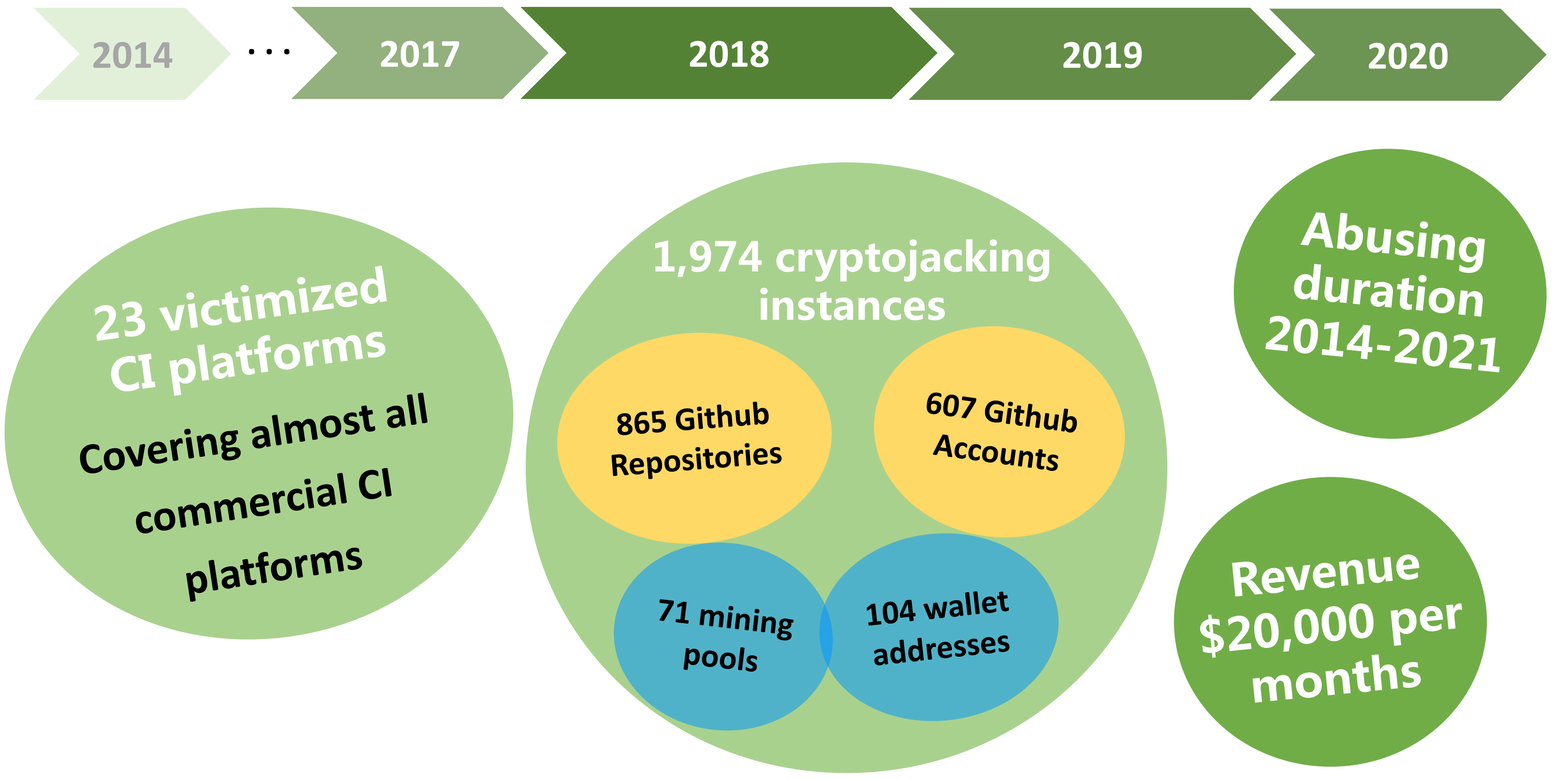
Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms

Zhi Li, Weijie Liu, Hongbo Chen, XiaoFeng Wang, Luyi Xing, Mingming Zha, Hai Jin, Deqing Zou
Huazhong University of Science and Technology & Indiana University Bloomington

How CI platforms work?

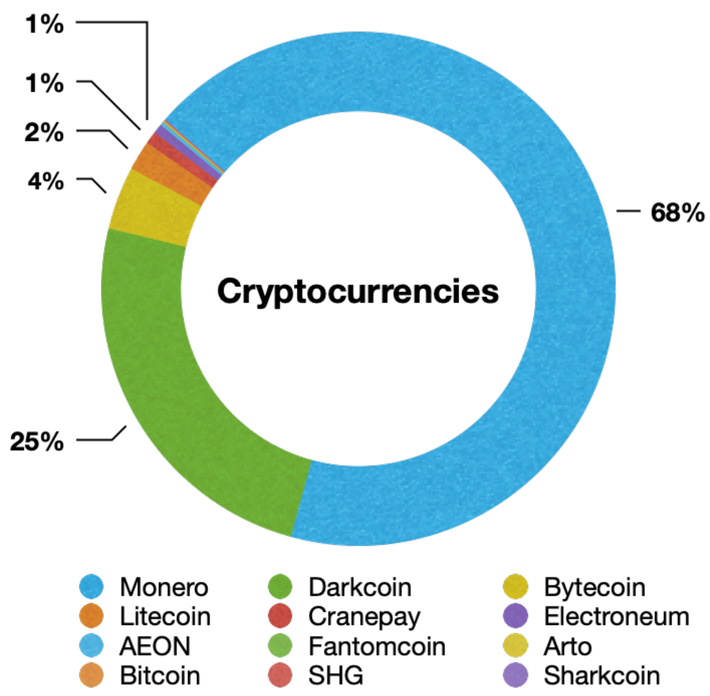


Cryptojacking on DevOps Platforms



Cryptocurrency Choices

The **Monero** is the most popular cryptocurrency (with the highest revenue)



Mitigation

Step-1

Detect consistency & High-frequency memory accesses

Step-2

Penalize access behaviors

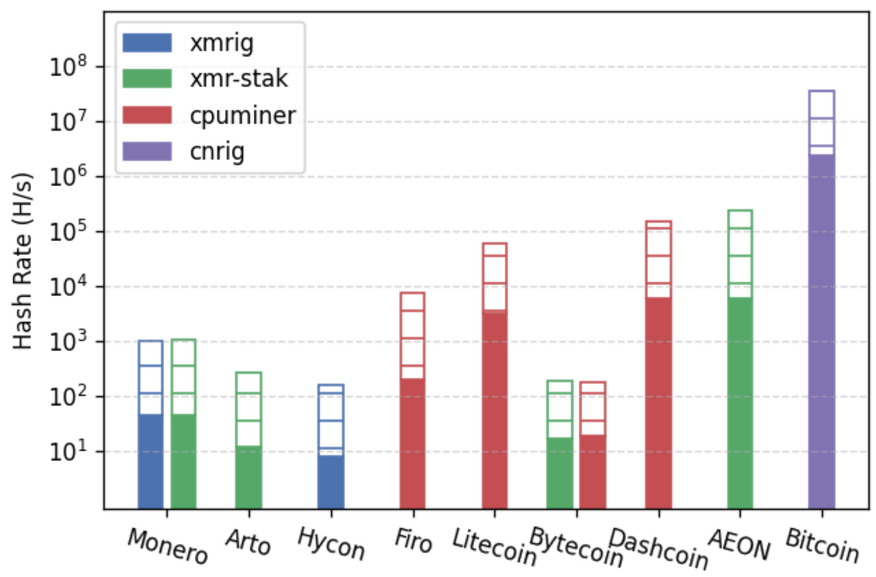
Step-3

Suppress mining jobs performance

Step-4

Make mining jobs unprofitable

Mitigation Results



Average Delay Ratio: 95.3%

Highest Delay Rate: 97.3%

AEON

lowest Delay Rate: 93.1%

Bitcoin

Poster: Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms

PUBLISHED PAPER

Title: Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms
Authors: Zhi Li, Weijie Liu, Hongbo Chen, XiaoFeng Wang, Xiaojing Liao, Luyi Xing, Mingming Zha, Hai Jin, Deqing Zou
Email: lizhi16@hust.edu.cn, {weijliu, hc50, xw7, xliao, luyixing, mzha}@iu.edu, {hjin, deqingzou}@hust.edu.cn
Date: MAY 22-26, 2022
Venue: Proceeding of the 43rd IEEE Symposium on Security and Privacy (SP'22)
DOI: https://doi.ieeecomputersociety.org/10.1109/SP46214.2022.00022

ABSTRACT

The recent wave of in-browser cryptojacking has ebbed away, due to the new updates of mainstream cryptocurrrencies, which demand the level of mining resources browsers cannot afford. As replacements, resource-rich, loosely protected free Internet services, such as *Continuous Integration* (CI) platforms, have become attractive targets. In this paper, we report a systematic study on real-world illicit cryptomining on public CI platforms (called *Cijacking*). Unlike in-browser cryptojacking, Cijacks masquerade as CI jobs and are therefore more difficult to detect, since legitimate CI workflows such as container image building and testing also entail intensive computing. In our research, we leveraged the critical mining information the adversary has to specify, such as wallet addresses and mining pool domains, to recover the attack traces from GitHub repositories and the log files on CI platforms, leading to the discovery of 1,974 Cijacking instances, 30 campaigns across 12 different cryptocurrencies on 11 mainstream CI platforms. Further, our study unveils the evolution of attack strategies, in response to the protection put in place by the platforms, the duration of the mining jobs (as long as 33 months), and their lifecycle. Further discovered is the revenue of the attack, over $20,000 per month.

Since robust detection of cryptojacking is known to be hard, we developed a novel technique, called Cijitter, to strategically inject delays to the execution of a CI workflow to disproportionally penalize the mining jobs that need to work on a series of tasks under time constraints. Our analysis and evaluation, as conducted on both benchmarks and common CI jobs, show that our approach substantially suppresses the miner's revenues, rendering them unprofitable, but only has small impacts on the performance of CI jobs and developer productivity (94.3% of CI jobs see a less than 10% delay).