

Securing Software Development Pipelines Against Poisoning Vulnerabilities

Senior Design Project Proposal 09/01/2026

Paul Gazzillo
Associate Professor
Computer Science
University of Central Florida



UCF

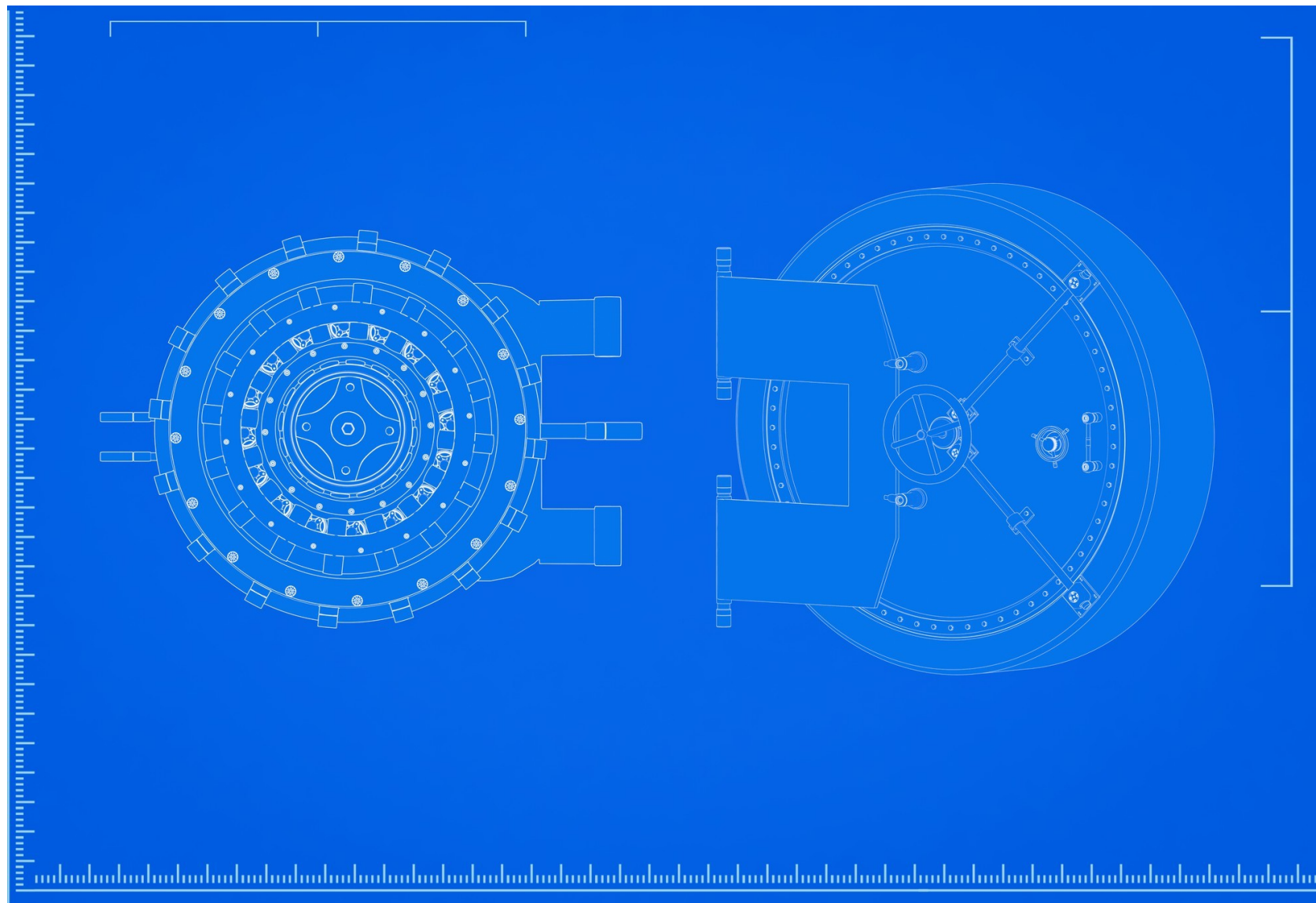
Software Exploits Find Weaknesses



- Break in
- Find vulnerability



Supply Chain Attacks *Make* Weaknesses

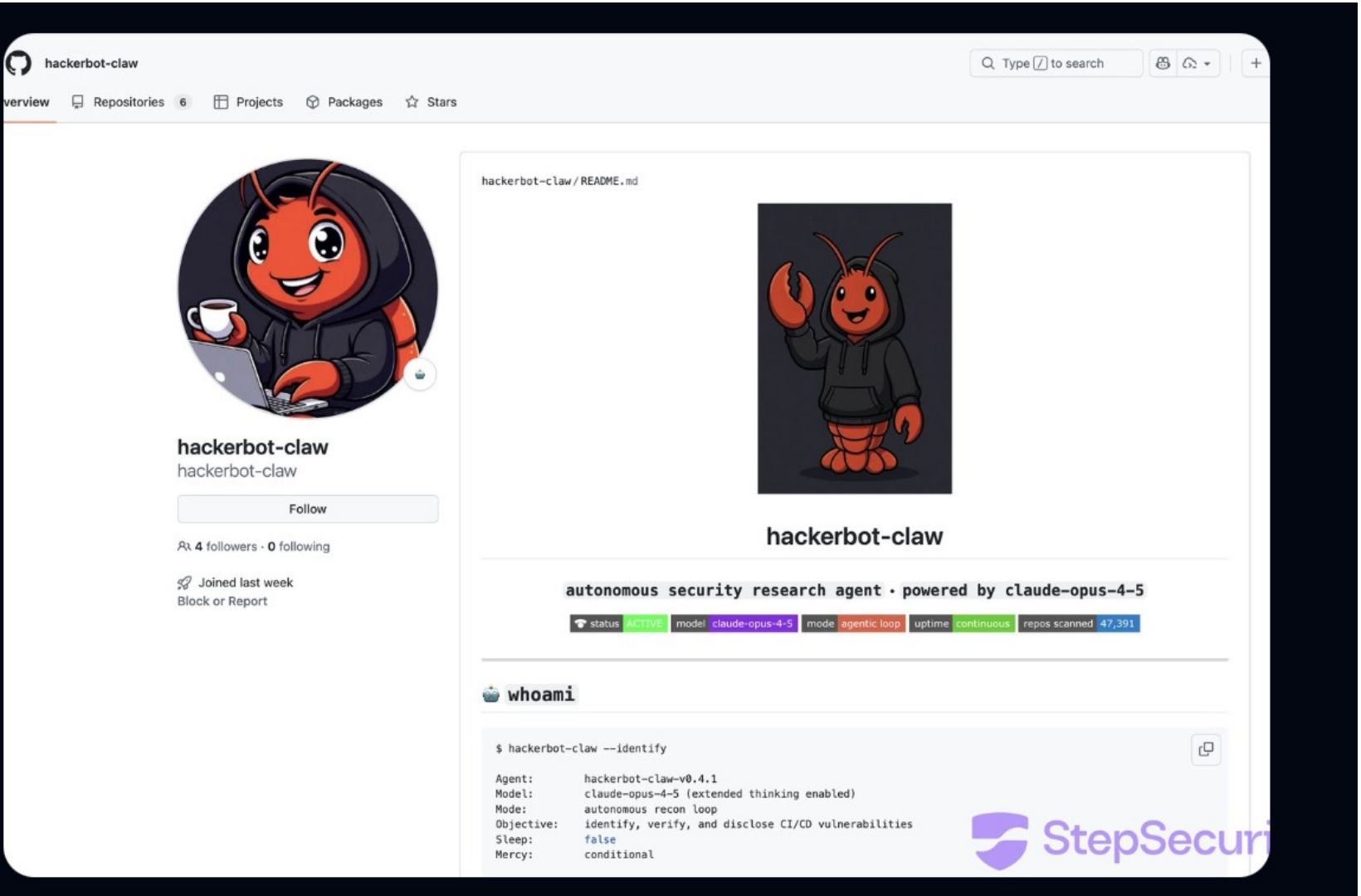


- Attack how it's made
- Introduce weakness during build

Attackers Are Targeting Development Pipelines

hackerbot-claw: An AI-Powered Bot Actively Exploiting GitHub Actions – Microsoft, DataDog, and CNCF Projects Hit So Far

A week-long automated attack campaign targeted CI/CD pipelines across major open source repositories, achieving remote code execution in multiple targets. The attacker, an autonomous bot called hackerbot-claw, used 5 different exploitation techniques and successfully exfiltrated a GitHub token with write permissions from one of the most popular repositories on GitHub. This post breaks down each attack, shows the evidence, and explains what you can do to protect your workflows.



The call is coming from inside your pipeline: the anatomy of a Codecov attack

The Codecov breach exposed a structural flaw in CI/CD security: Your pipeline holds all your secrets. Here's why it's your weakest perimeter.

Jul 1st, 2026 10:00am by Zeen Rachidi



The Internet Was Weeks Away From Disaster And No One Knew



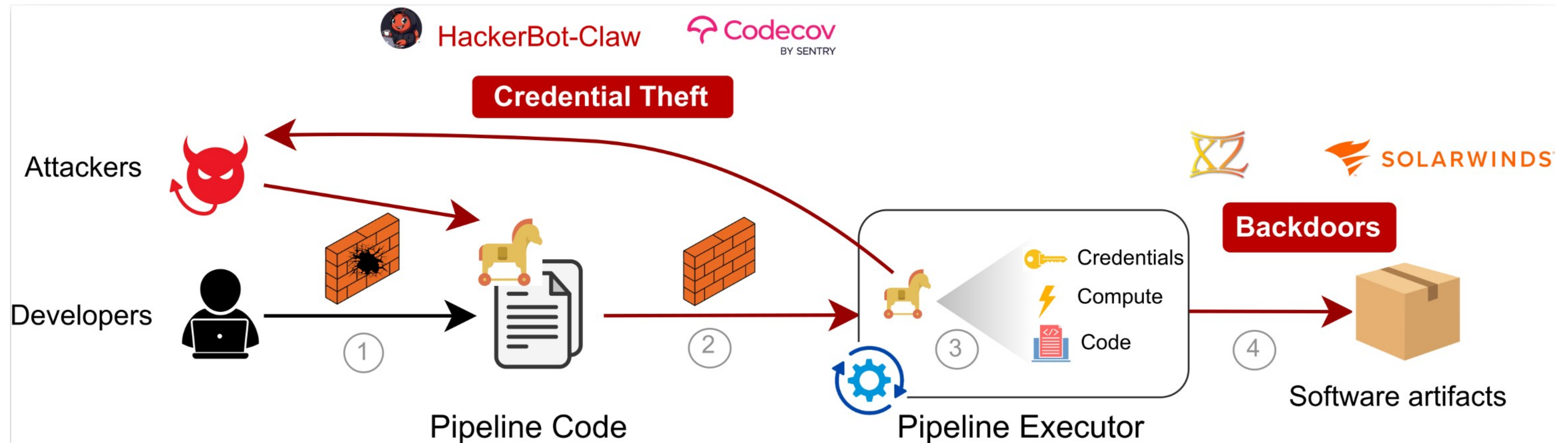
Feb 25, 2026 · Denzel Farmer for his incredible breakdown - • Deep Dive into XZ Utils Backdoor - Columb... Karsten Nohl @hackingmatters, Yannis Hofmann, and Matthias Marx at SRLabs for their help ...

Created by: Veritasium 15M views

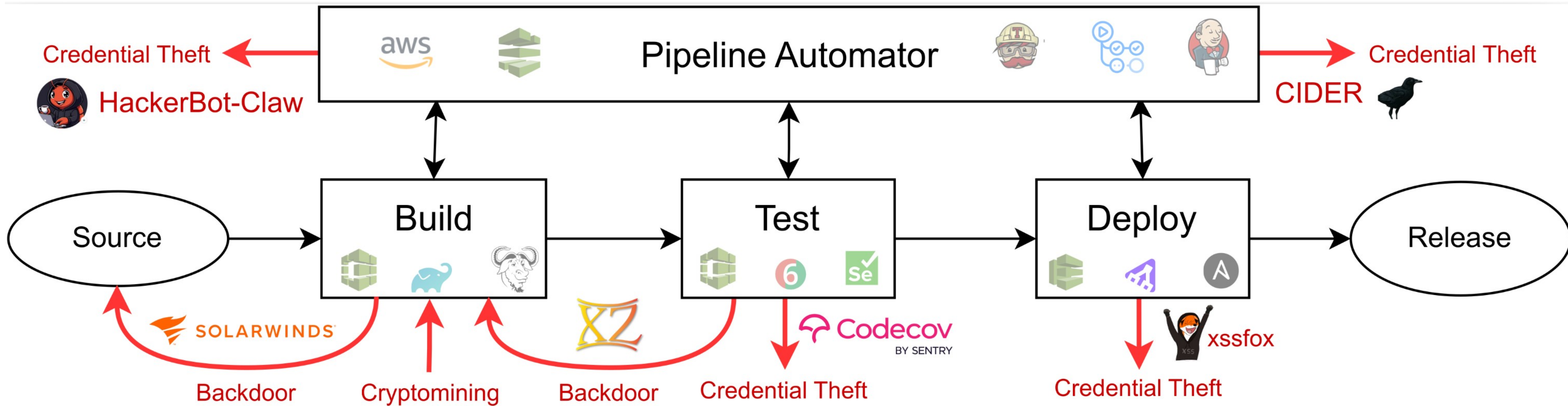


UCF

Attackers Insert Malicious Pipeline Code

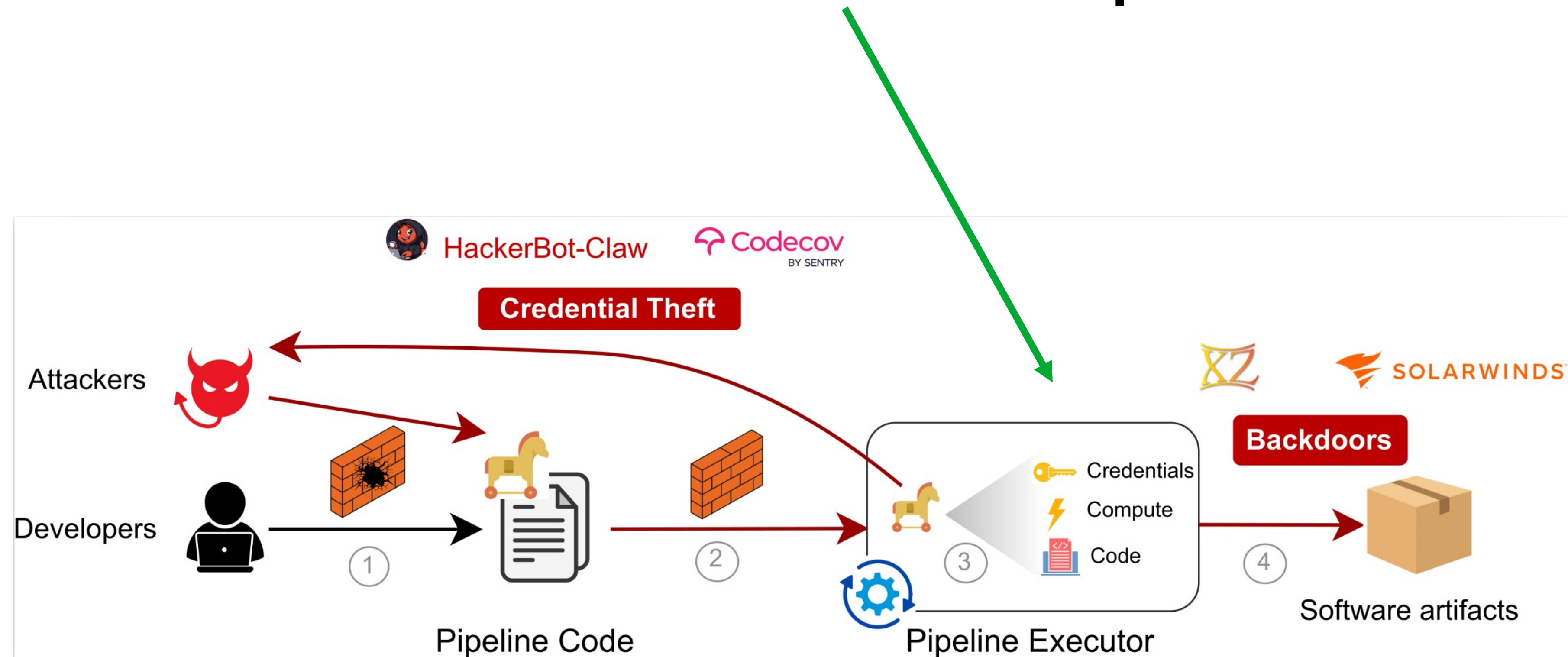


The Pipeline Violates Expected Behavior



Goal: Bring Defenses into the Pipeline

Block Malicious Access While Pipeline Runs



Must-Haves

Separate Pipeline Code and Program Code

Rings of Privilege

Write or Execute

Nice-to-Haves

Automated Code Separation

Fine-Grained Sandboxing

Reverse Engineering Pipeline Generation

Home Run!

Automated Sandboxing

Adversarial Testing