|  |
| --- |
| Team 14 |
|  |

# Incident Response – Backdoor on CentOS 7

**Date Incident Occurred**: February 18, 2023

**Attacker Source Address**: 10.4.4.4

**Target System Name**: Cent OS 7 Ecommerce

**Target System Address**: 172.20.241.30

**Type of Attack**: Backdoor

**Result of Attack**: Attacker had access to critical systems through reverse shell.

**Attack Discovery**: The backdoor was detected when monitoring active cron jobs.

**Remediation Actions/Controls**: The cron job was removed by clearing the active cron jobs. In addition, we are blocking the identified malicious IP (10.4.4.4) from accessing our network using the Palo Alto firewall.

**Result of Remediation**: We have removed the threat actor’s access to our network, and are taking other preventative measures to prevent that IP from accessing our network.

Image 1: Screen shot of active cron job before remediation