Log Analysis Is Tricky! Writeup

KAYNE

12/12/2025

Background: Myo-AI.org was recently hacked. We have no idea what happened. One day we all go to work in the morning. and not even our biometric reader at the datacenter works. We get the firemen to let us inside and everything is gone. Every windows device is empty, and every server is wiped. What in the world happened? We have no idea.

2025-03-01T02:04:35Z,mabel she has a login success from San Francisco here. which is not her usual Anne Arbor Michigan

2025-03-01T04:51:15Z,mabel she visits api.ipify.org which tells you your external IP

2025-03-01T05:53:45Z,mabel she visits hometownchick (Known trickbot domain) and downloads startr.ack (real trickbot download that is actually an exe file)

C2 connections (port 8082 is a known trickbot C2 non-standard outbound C2)

1. 2025-03-01T06:56:15Z 2. 2025-03-01T07:17:05Z 3. 2025-03-01T07:37:55Z 4. 2025-03-01T07:58:45Z	5. 2025-03-01T08:19:35Z 6. 2025-03-01T08:40:25Z 7. 2025-03-01T09:01:15Z 8. 2025-03-01T09:22:05Z