Mission Name

Indicators of Compromise

History Context

EUPHEA - Principal & Chancellor's office at Shanghai. The investigation leads to The Principal and the Chancellor. Ethan must place the bug.

Technical High-Level Overview

This is the first time that the player goes to connect to a live Windows machine to investigate. His purpose would be to locate how Ethan placed the bug into the machine and discover the SHA1 hash of itself. Considering the level of this challenge, bug was deployed using Windows tasks and is located at C:\Users\Administrator\AppData\Local\task\check_task.exe

Short Description

In previous missions, you had to check Ethan´s bug but this, you´re going to investigate how Ethan set up the bug, and your goal will be to get SHA1 hash of the bug (backdoor9

Mission Description

This is the first time that you go to connect to a live Windows machine to investigate. In previous missions, you had to check Ethan´s bug but this, you´re going to investigate how Ethan set up the bug, and your goal will be to get SHA1 hash of the bug (backdoor).

Location

EUPHEA FACULTY | THE PRINCIPAL'S QUARTERS

Tools

- Hash tool

Questions

Which is the name of the related task?

- UpdateWindows

Items

1. For this challenge, a bug, it would be a backdoor
2. Analyse all persistence artifacts.
3. Analyse Windows Tasks

Write Up

This challenge is based on the bug that was simulated in challenge in Mission 11 to check it´s hidden capababilites. This time, player must put in practice his forensic knowledge about locating how Ethan deployed the bug inside the machine. As we can see in the below image, Ethan set up a new task to hide the bug, located in C:\Users\Administrator\AppData\Local\task\check_task.exe

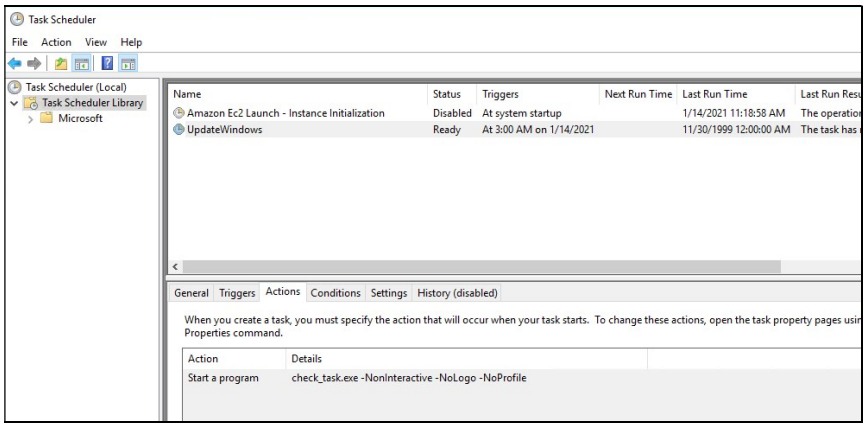

Figure 1

Finally player will have to get SHA1 hash of the binary check_task.exe: adcfcefe6516cd6596cd9dba2af4ce622b788e9d

Flag Information

flag{adcfcefe6516cd6596cd9dba2af4ce622b788e9d}