**Hunt Me II: Typo Squatters**

One of your software developers unknowingly installed a malicious software. Can you trace back the root cause?

Task 1 Introduction and Scenario

Scenario

Just working on a typical day as a software engineer, Perry received an encrypted 7z archive from his boss containing a snippet of a source code that must be completed within the day. Realising that his current workstation does not have an application that can unpack the file, he spins up his browser and starts to search for software that can aid in accessing the file. Without validating the resource, Perry immediately clicks the first search engine result and installs the application.



Last **September 26, 2023**, one of the security analysts observed something unusual on the workstation owned by Perry based on the generated endpoint and network logs. Given this, your SOC lead has assigned you to conduct an in-depth investigation on this workstation and assess the impact of the potential compromise.

Connection Details﻿

Deploy the attached machine by clicking the Start Machine button in the upper-right-hand corner of the task. The provided virtual machine runs an Elastic Stack (ELK), which contains the logs that will be used throughout the room.

Once the machine is up, access the Kibana console (via the AttackBox or VPN) using the following credentials below. The Kibana instance may take up to 3-5 minutes to initialise.

































































