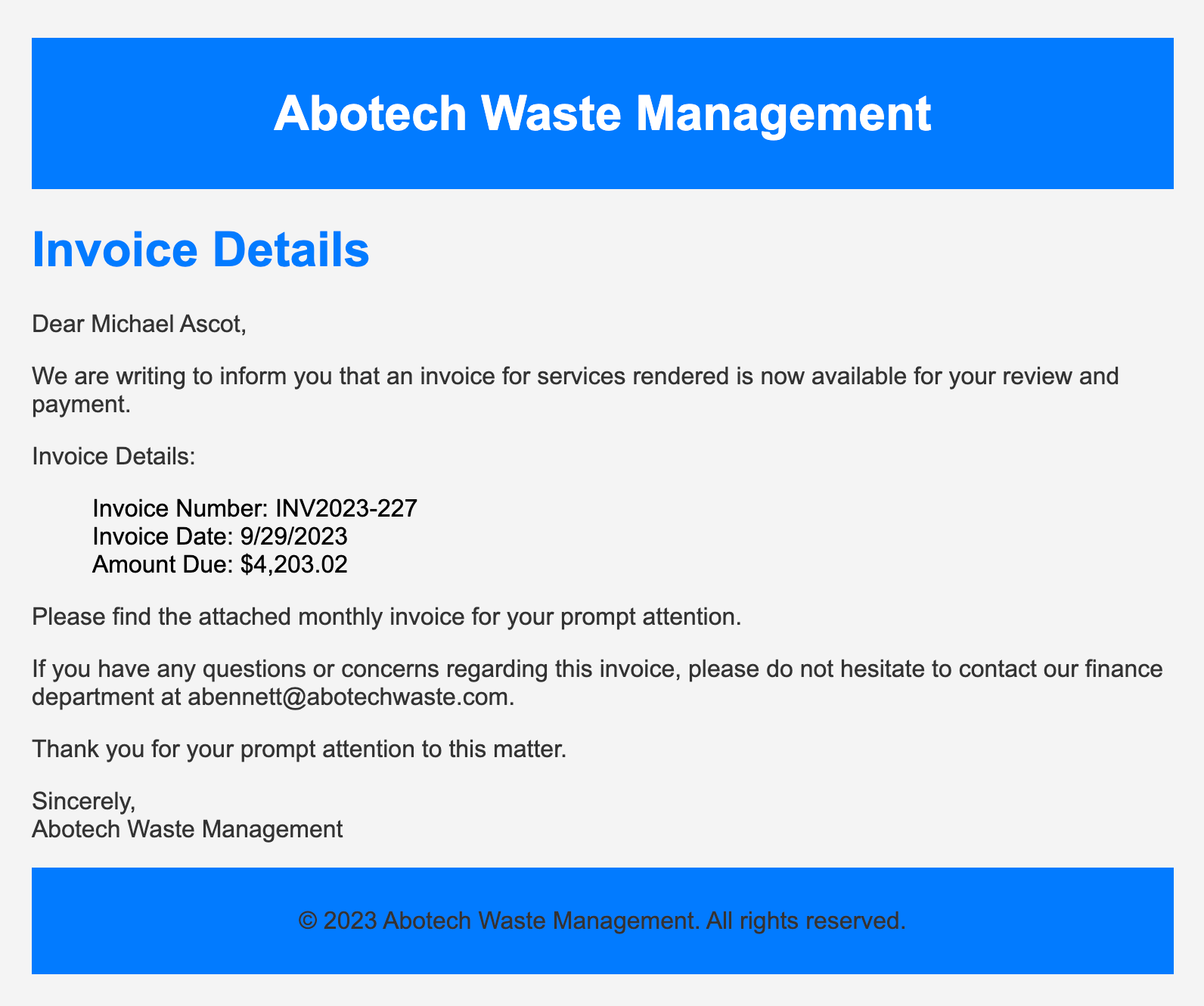
**Hunt Me I: Payment Collectors**

A Finance Director was recently phished. Can you hunt the logs and determine what damage was done?

Task 1 Introduction and Scenario

On **Friday, September 15, 2023**, Michael Ascot, a Senior Finance Director from SwiftSpend, was checking his emails in **Outlook** and came across an email appearing to be from Abotech Waste Management regarding a monthly invoice for their services. Michael actioned this email and downloaded the attachment to his workstation without thinking.



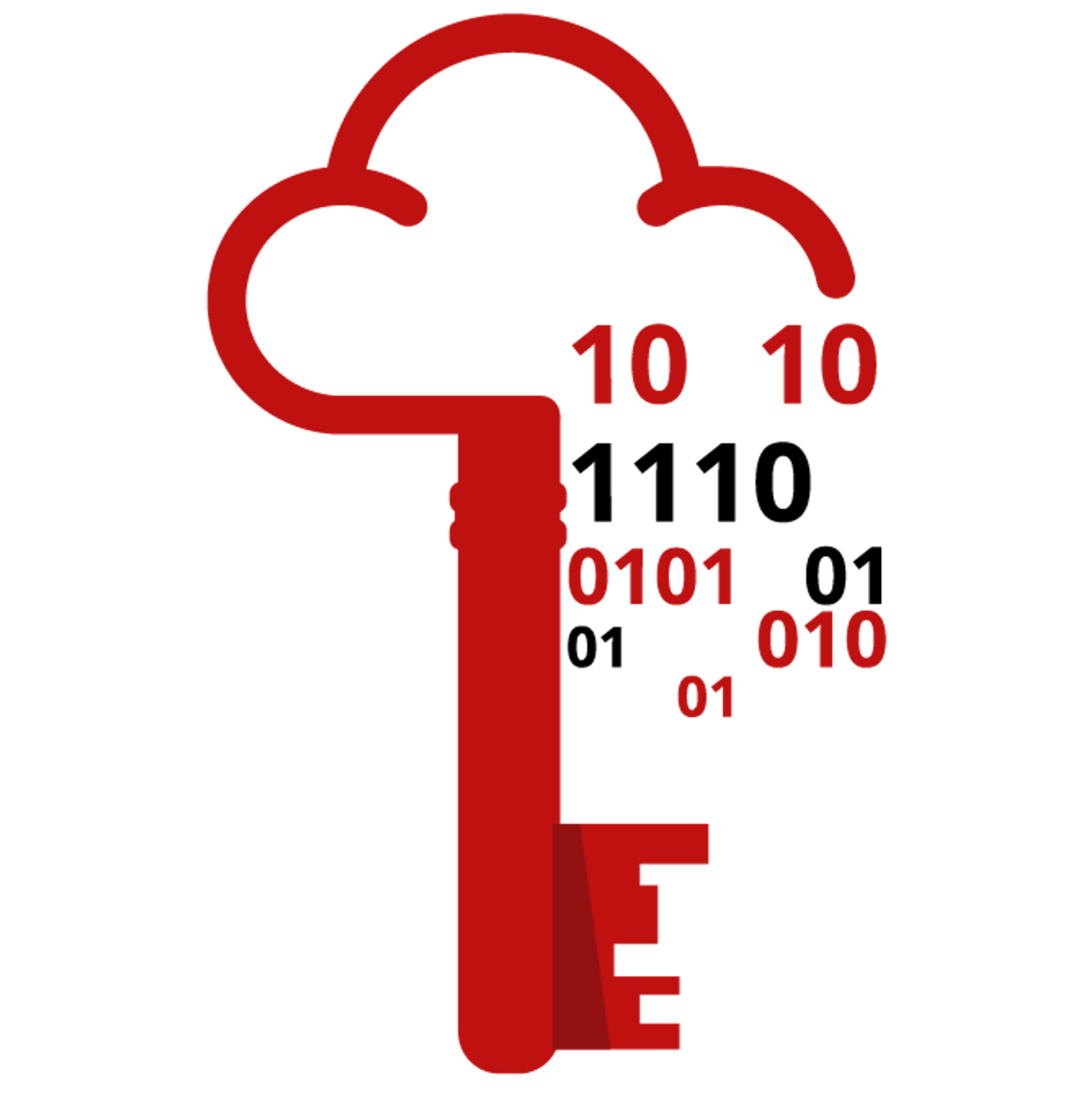
The following week, Michael received another email from his contact at Abotech claiming they were recently hacked and to carefully review any attachments sent by their employees. However, the damage has already been done. Use the attached Elastic instance to hunt for malicious activity on Michael's workstation and within the SwiftSpend domain!

Connection Details

First, click **Start Machine** to start the VM attached to this task. You may access the VM using the AttackBox or your VPN connection. You can start the AttackBox by pressing the **Start AttackBox** button on the top-right of this room. **Note:** The Elastic Stack may take up to 5 minutes to fully start up. If you receive any errors, give it a few minutes and refresh the page.

Once online, navigate to <http://10.10.249.140> using a web browser.

You should see the Elastic login page. Please log in using the following credentials:



|  |
| --- |
|  |
|  |

