**INCIDENT REPORT: 18516**

**Date: 02/14/24**

**Executive summary:**

**After an employee opened an infected email malware was loaded onto a company computer. I have been given the potentially infected emails to go over and identify what email was the host for the malware.**

**Victim details:**

* **IP address: 10.3.66.130**
* **MAC address: 78:19:f7:ac:01:7d**
* **Host name: JuniperNetwo\_ac**
* **User account name:**
* **Infected email:** [**eningeering@asahikosei.com**](mailto:eningeering@asahikosei.com)
* **Date and time of infection: 11/06/15 1348**

**Conclusion:**

**After going over the provided email I can say that the infected email that was opened by the employee was about an invoice. Upon opening the email there were several spelling mistakes and improper grammar used when writing the email. As well as a request to pay by check and to pay as soon as possible to avoid a “finance” fee of 15% being added to the total. It is safe to assume and say that this email was the email that infected the company computer when the employee clicked the link to open the invoice image.**