**Incident Report 11895: Defensive: Malicious Email**

**03/03/22**

**Executive Summary:**

There was a mail filter outage reported at a company that lasted for 24 hours. Fortunately, very few incidents were reported. But one example caught your eye.

During the mail filter outage, one of the company employees decided to play "email roulette." The employee opened one of the malicious emails from his inbox and treated it as a legitimate message.

You've acquired four malicious messages the employee received. You also received a pcap of traffic from his infected computer. Your task? Figure out which email was used to infect his computer.

In your incident report, include the following:

* Date and approximate time of the infection.
* The infected computer's IP address.
* The infected computer's MAC address.
* The infected computer's host name.
* Which email the employee opened.

**Results**

I analyzed the pcap of received network traffic using wireshark. There were four emails with potentially malicious content.

All four emails contained malicious attachments. Here is the information I found on the initial infection.

* Date and approximate time of the infection. Nov 6th 2015 at 1422PT
* The infected computer's IP address. 174.121.246.162
* The infected computer's MAC address. 00:24:e8:2d:90:81
* The infected computer's host name. Juniper
* Which email the employee opened. Arthur Stoyt

**Application Details:**

**Attack Narrative**

Emails were sent with attachments containing a trojan. The file was downloaded and then attempted to spread through the network through other email attachments.

**Conclusion:**

Virus signatures need to be updated to include this Trojan. Users need to be further educated on opening attachments in emails. A better solution would be to have non public facing network share or cloud sharing service for inner office documents. And have a policy to not download email attachments.