Splunk Analysis

Document/Log being reviewed:

buttercupgames_email_log.csv

Task :

Find possible **anomalies** that may indicate a phishing attack

Search Used:

source="buttercupgames_email_log.csv" host="email_logs" Sender="*@buttercupgames.com" | stats earliest(_time) latest(_time) by incoming_address | convert timeformat=" %m/%d/%y %H:%M:%S" ctime(earliest(_time)) AS earliest_time ctime(latest(_time)) as latest_time

What is the **incoming IP address?**

74.207.253.34

*** Who is the **Sender**?**

Address14@buttergames.com

*** Who is the **Recipient**?**

address37, address15@ buttercupgames.com

*** What is the **Subject** of the email?**

Phishing Subject 19

*** What is the **time** of the event?**

2/1/17 4:29:19.000 AM

*** Are there any **attachments**?**

Yes. Email Data is the attachment.