**Splunk Analysis**

**Document/Log being reviewed:**



**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](mailto: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.