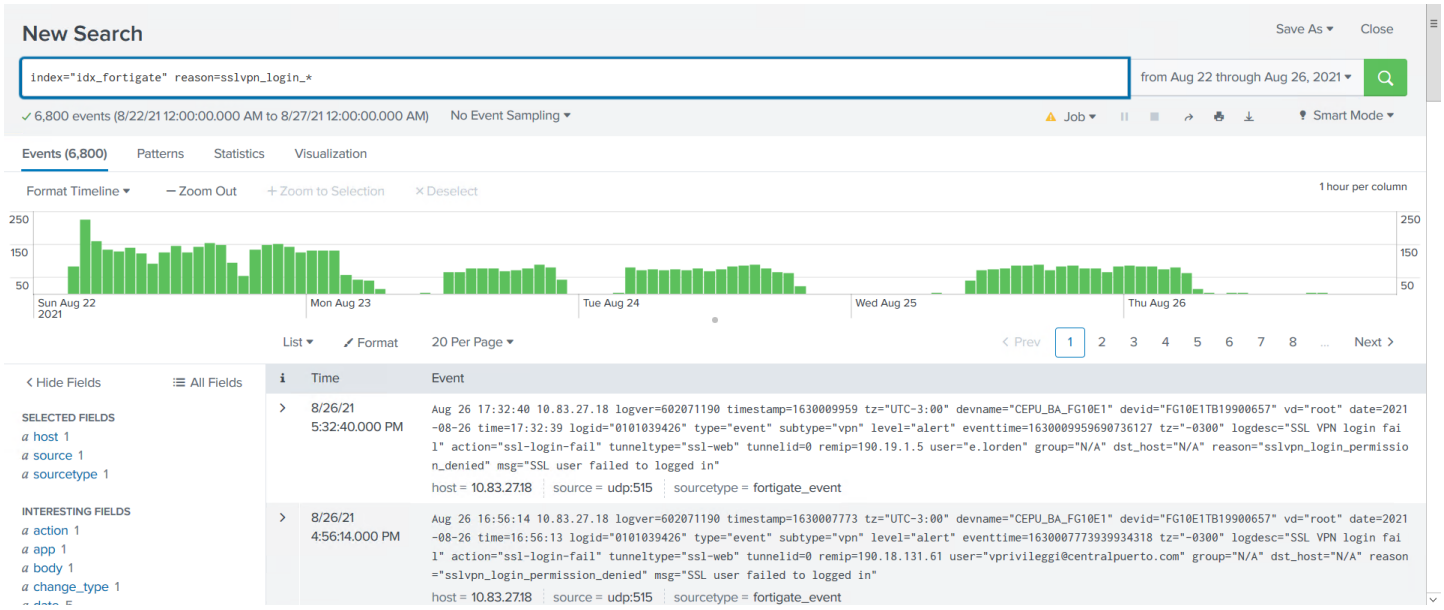
ANÁLISIS DE ALERTA

A continuación resumimos el análisis realizado.

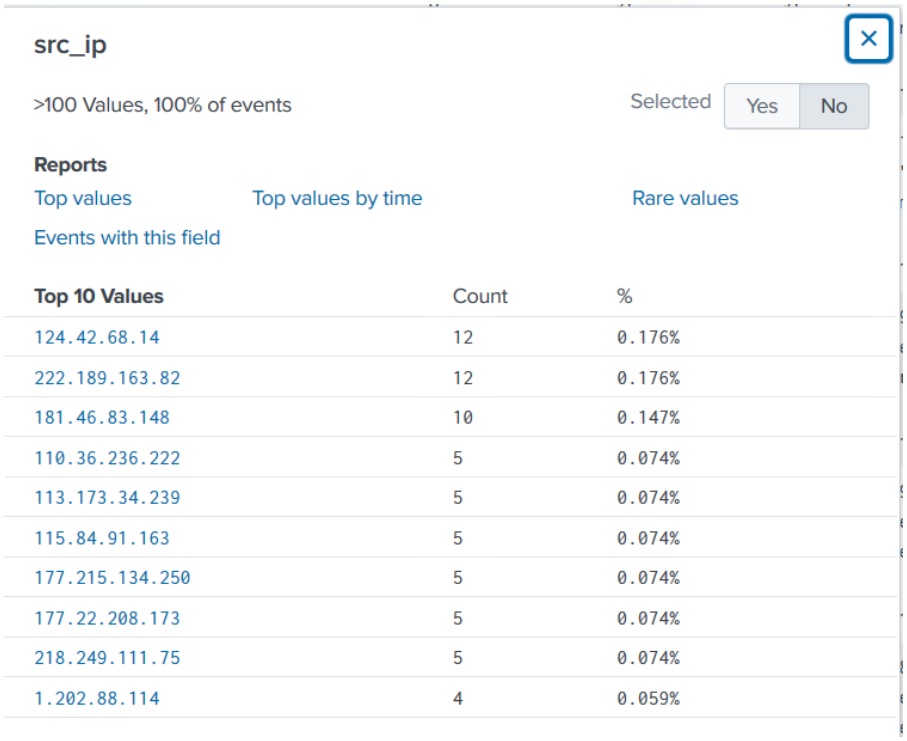
OBSERVACIONES

Se observó lo siguiente:

- Se detectó que entre los días 22/08 y 26/08 se realizaron excesivos intentos de login fallidos desde múltiples orígenes y usuarios.



- Las IPs son todas externas y se pasa a analizar la geolocalización y la reputación de las mismas



src_ip

>100 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
124.42.68.14	12	0.176%
222.189.163.82	12	0.176%
181.46.83.148	10	0.147%
110.36.236.222	5	0.074%
113.173.34.239	5	0.074%
115.84.91.163	5	0.074%
177.215.134.250	5	0.074%
177.22.208.173	5	0.074%
218.249.111.75	5	0.074%
1.202.88.114	4	0.059%

- Los usuarios involucrados evidencian que es un ataque del tipo Brute Force utilizando diccionario (salvando excepciones de usuarios legítimos):

user

>100 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
teste	190	2.794%
servidor	171	2.515%
usuario	171	2.515%
administrador	165	2.426%
remoto	89	1.309%
financeiro	70	1.029%
contabilidad	68	1%
sistemas	68	1%
contador	66	0.97%
fernando	65	0.956%

- Procedimos a analizar si de todas estas IPs, alguno de estos intentos de Brute Force tuvo éxito al acceder a la red interna.

- Y logramos dar con 1 solo registro, pero se validó que es un acceso legítimo.

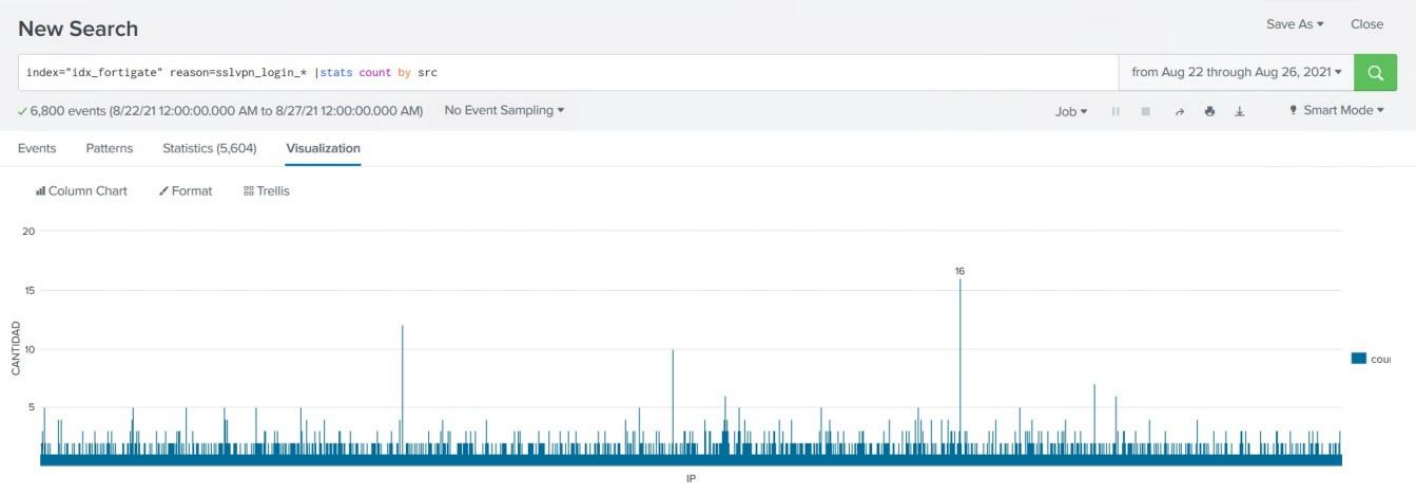
Central Puerto splunk> LT_Reporte de Brute Force

LT_Reporte de Brute Force

Reporte de IPs y usuario que se incorporaron a la lista negra de BRUTE-FORCE.CSV y que loguearon exitosamente durante el día de ayer

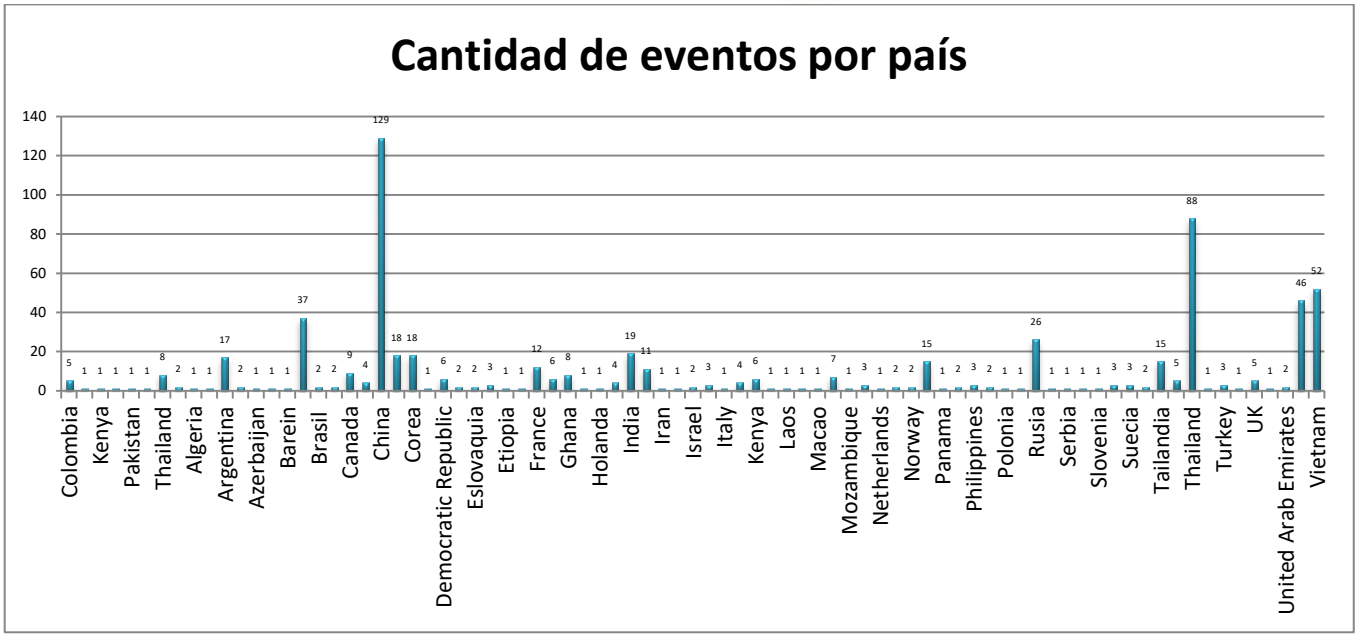
ip	user
186.22.17.209	dmari

Teniendo en cuenta la dispersión de IPs observadas y que se logró identificar que las IPs son de generación dinámica

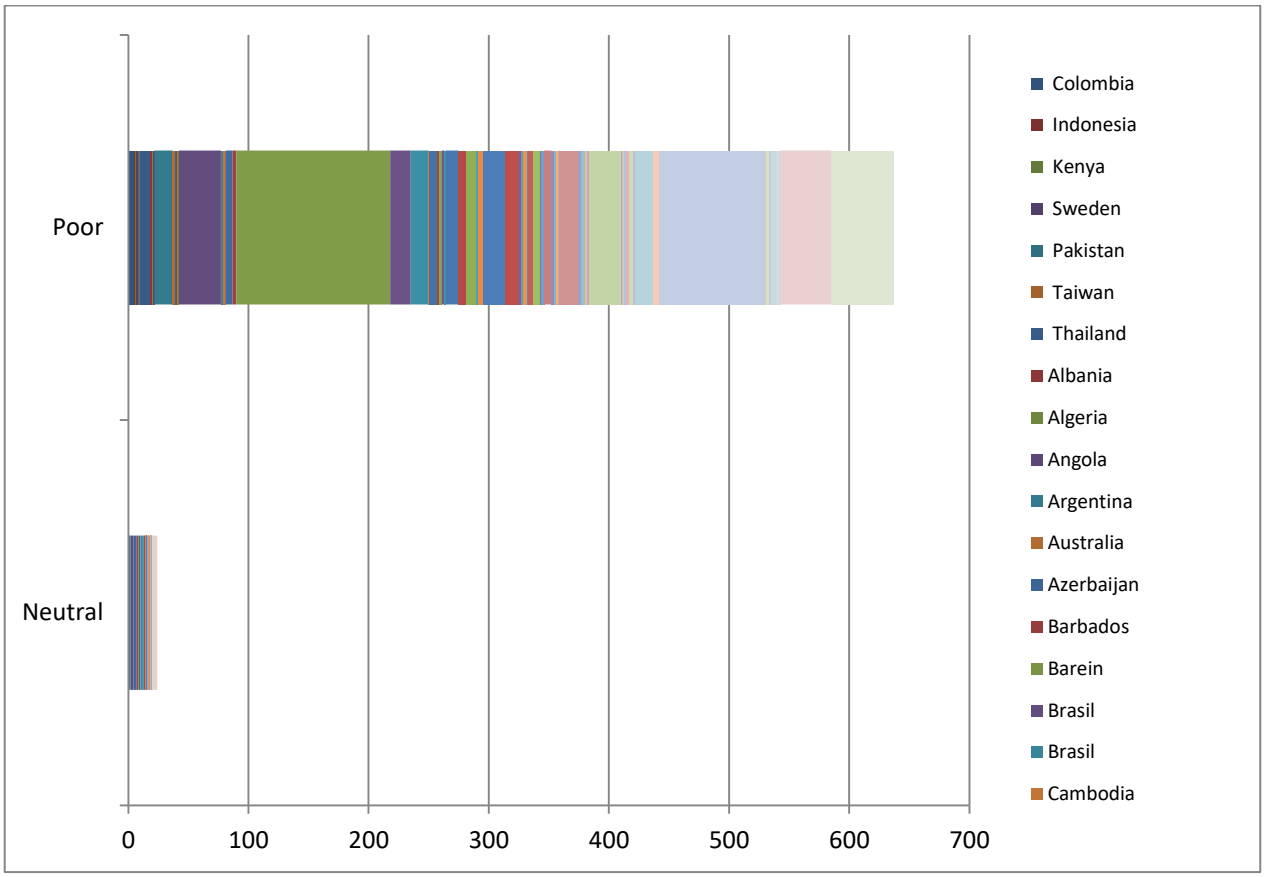


Se decidió tomar una muestra del 10% de las mismas para un análisis más detallado que reflejamos a continuación

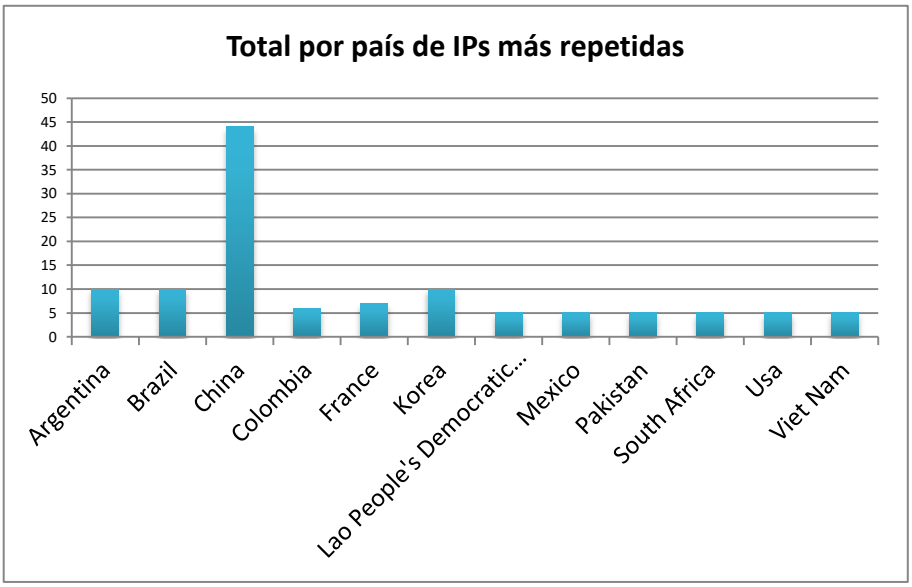
- Se identifica que provienen en su gran mayoría de China.

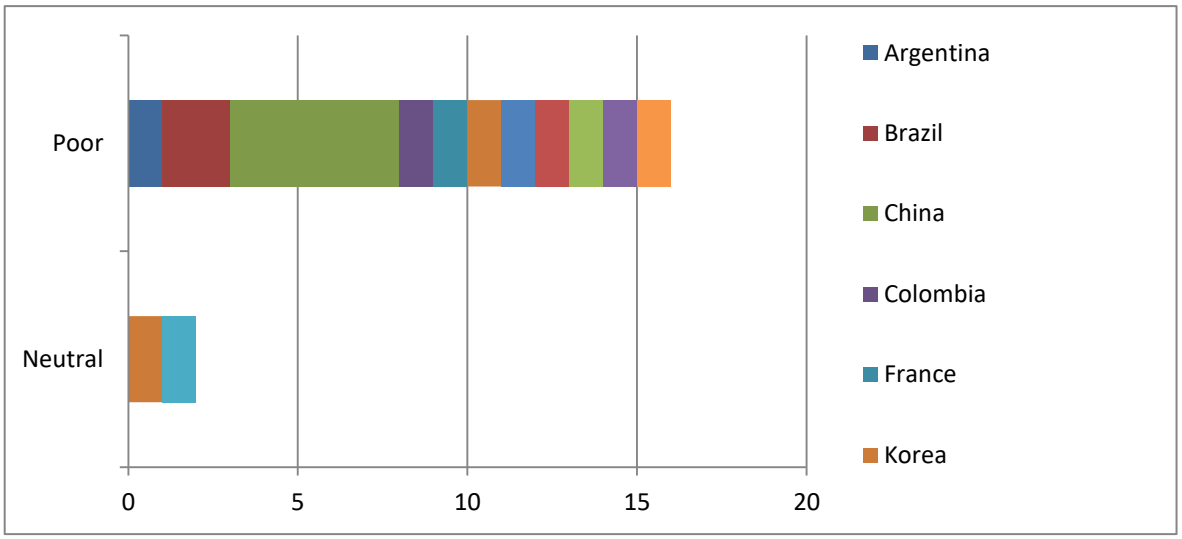


- Revisando la reputación de las IPs no se logra dar con alguna que tenga mala reputación, el que sean de generación dinámica complica este paso.



Además se analizaron las IPs con mayor recurrencia en el periodo analizado en cuyo caso se repite China como país de origen más reiterado.





Con reputaciones entre pobre y neutral.

CONCLUSIONES

De lo observado podemos concluir que:

1. Se trató de una actividad maliciosa del tipo Brute Force utilizando IPs dinámicas para no generar lockout.
2. Se analizaron las IPs y usuarios involucrados en el ataque, llegando a la conclusión de que ningún intento fue exitoso.
3. Se generaron nuevas alertas y nuevos reportes para tener un control más exhaustivo de este tipo de actividad.

En base a las conclusiones, nuestras recomendaciones son:

1. Se recomienda el uso de la geolocalización para bloquear regiones o países directamente, el bloqueo sobre IPs no serviría de mucho en este caso ya que son IPs generadas dinámicamente.

2. Avisar al SOC de Lightech si se toma la decisión de que es un falso positivo.