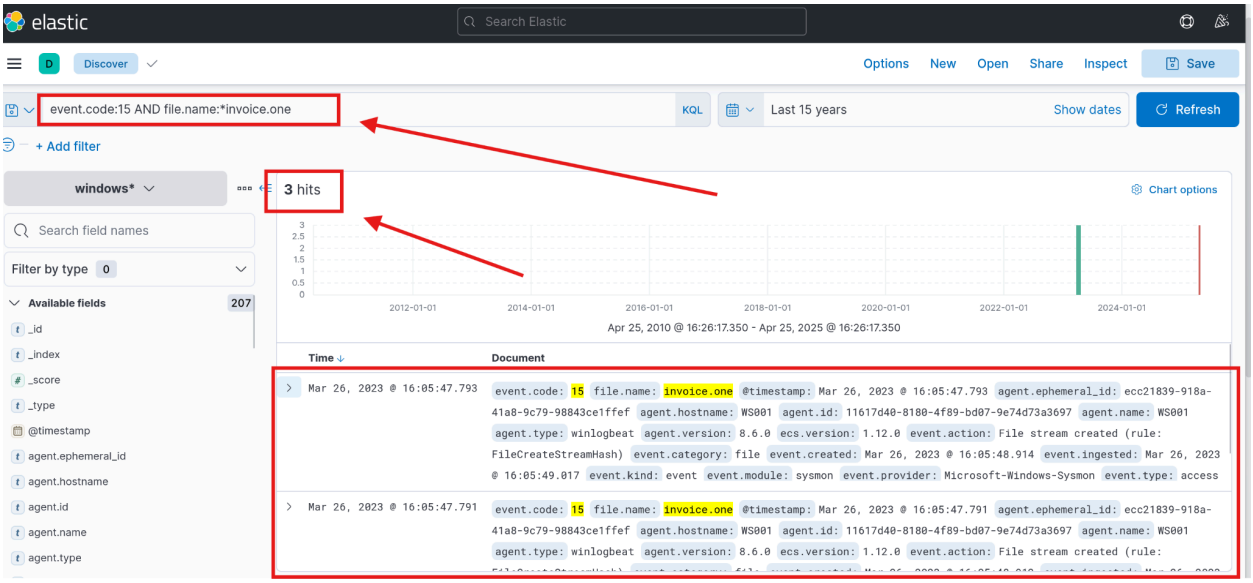
ELK | Attack Detection

Hypothesis - Attackers may have used different delivery techniques between the time the intelligence report was created and the present instead of Phishing email delivering ?

1. Search based on Sysmon Event ID 15 (FileCreateStreamHash), which Logs when an alternate data stream (ADS) is created, often used in hidden or malicious activity with the file name of “invoice.one”.



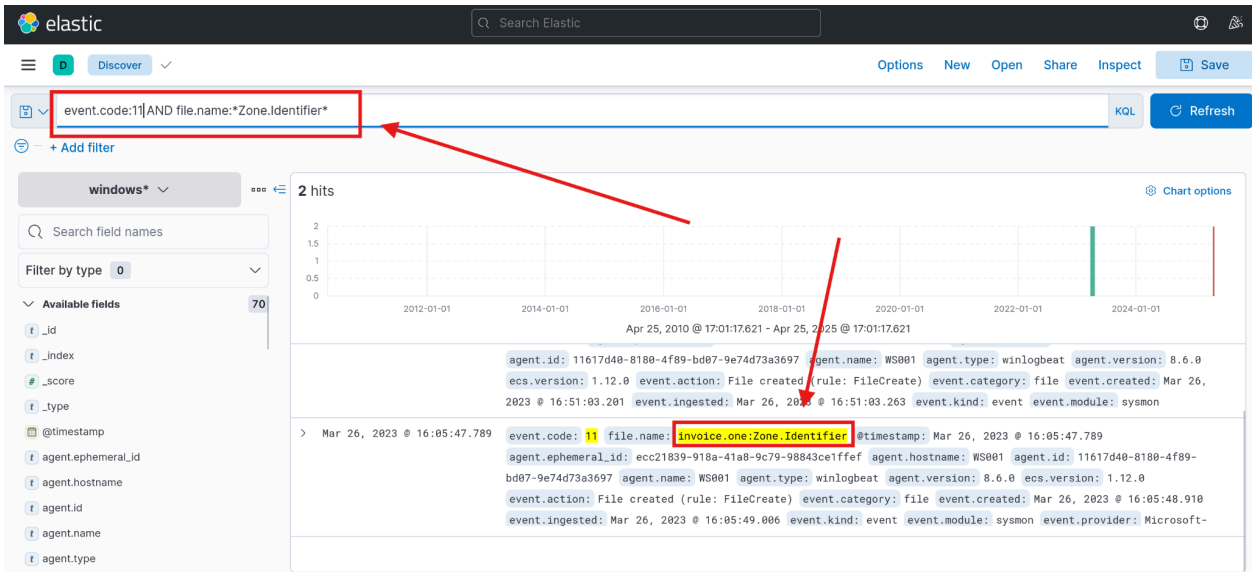
<u>Following details are extracted from the complete Log information -</u>

@timestamp	Mar 26, 2023 @ 16:05:47.793
agent.hostname	WS001
file.path	C:\Users\bob\Downloads\invoice.one
process.executable	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
process.name	msedge.exe

This information reveals that MSEdge was the application used to download the file, Which was stored in the Downloads folder of an employee named Bob.

It's not yet confirmed if this file is the same one mentioned in the report.

2. Use Zone.Identifier (ADS) creation to spot downloaded files.



This confirms that the above logged invoice.one file originated from the internet. (Downloaded from the MsEdge browser)

3. Using Zeek, Filter and examine the DNS queries that Zeek has captured from WS001 during the interval when the file was downloaded.