Scenario

You are working in a newly established SOC where still there is lot of work to do to make it a fully functional one. As part of gathering intel you were assigned a task to study a threat report released in 2022 and suggest some useful outcomes for your SOC.

Here are the extracted questions and their required formats from the image:

1. Name the supply chain attack related to Java logging library in the end of 2021.

Format: `AttackNickname`

2. Mention the MITRE Technique ID which affected more than 50% of the customers.

Format: `TXXXX`

3. Submit the names of 2 vulnerabilities belonging to Exchange Servers.

Format: `Vuln Nickname, Vuln Nickname`

4. Submit the CVE of the zeroday vulnerability of a driver which led to RCE and gain SYSTEM privileges.

Format: `CVEXXXXXXXXX`

5. Mention the 2 adversary groups that leverage SEO to gain initial access.

Format: `Group1, Group2`

6. In the detection rule, what should be mentioned as parent process if we are looking for execution of malicious JS files [Hint: Not CMD]?

Format: `ParentProcessName.exe`

7. Ransomware gangs started using affiliate model to gain initial access. Name the precursors used by affiliates of Conti ransomware group.

Format: `Affiliate1, Affiliate2, Affiliate3`

8. The main target of coin miners was outdated software. Mention the 2 outdated software mentioned in the report.

Format: `Software1, Software2`

9. Name the ransomware group which threatened to conduct DDoS if they didn't pay ransom.

Format: `GroupName`

10. What is the security measure we need to enable for RDP connections in order to safeguard from ransomware attacks?

Format: `XXX`

-