Blue Team Labs Online Challenge: The Report

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.

The Red Canary 2022 Threat Detection Report is an annual analysis that compiles and classifies the most frequently observed techniques, tactics, and procedures (TTPs) encountered by Red Canary teams across real-world enterprise environments. Its primary purpose is to help defenders better understand attacker behaviors and prioritize their detection and response strategies.

Main contents of the report:

1. **Top 10 most detected MITRE ATT&CK techniques**
   The report presents a ranking of the most common ATT&CK techniques observed in monitored environments. For example:
   - T1059 – Command and Scripting Interpreter (use of cmd, PowerShell, etc.)
   - T1566 – Phishing
   - T1027 – Obfuscated Files or Information
2. **Real-world use cases**
   The report provides practical examples of how specific techniques were detected in actual incidents, including the attack context, tools used, and the response actions taken.
3. **Emerging trends**
   It highlights changes in adversary behavior, such as:
   - Increased use of script loaders
   - Abuse of legitimate tools (LOLBins)
   - Expansion of Ransomware-as-a-Service (RaaS)
4. **Notable threats of the year**
   Includes high-impact cases such as:
   - The exploitation of vulnerabilities in Microsoft Exchange servers (ProxyLogon, ProxyShell)
   - Widespread exploitation of the Log4j vulnerability

    - Malware campaigns involving Qbot, IcedID, and BazarLoader

5. **Defensive recommendations**
   The report offers guidance for detection, response, and implementation of defensive controls, including Sigma rules, YARA signatures, and EDR queries.

The challenge provides you with the report and presents a series of 10 questions about its content, which guide you through the different sections of the document. The questions, along with their corresponding answers, are as follows:

Question 1) Name the supply chain attack related to Java logging library in the end of 2021 (Format: AttackNickname)

Answer: Log4j

Question 2) Mention the MITRE Technique ID which effected more than 50% of the customers (Format: TXXXX)

Answer: T1059 (Command and Scripting Interpreter)

Question 3) Submit the names of 2 vulnerabilities belonging to Exchange Servers (Format: VulnNickname, VulnNickname)

Answer: ProxyLogon, ProxyShell

Question 4) Submit the CVE of the zero day vulnerability of a driver which led to RCE and gain SYSTEM privileges (Format: CVE-XXXX-XXXXX)

Answer: CVE-2021-34527 (PrintNightmare)

Question 5) Mention the 2 adversary groups that leverage SEO to gain initial access (Format: Group1, Group2)

Answer: Gootkit, Yellow Cockatoo

Question 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)

Answer: wscript.exe

Question 7) Ransomware gangs started using affiliate model to gain initial access. Name the precursors used by affiliates of Conti ransomware group (Format: Affiliate1, Affiliate2, Afilliate3)

Answer: Qbot, Bazar, IcedID

Question 8) The main target of coin miners was outdated software. Mention the 2 outdated software mentioned in the report (Format: Software1, Software2)

Answer: JBoss, WebLogic

Question 9) Name the ransomware group which threatened to conduct DDoS if they didn't pay ransom (Format: GroupName)

Answer: Fancy Lazarus

Question 10) What is the security measure we need to enable for RDP connections in order to safeguard from ransomware attacks? (Format: XXX)

Answer: MFA (Multi Factor Authentication)