The Report

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

Log4j

Log4j is a popular Java logging library

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

NAME	TECHNIQUE RANK (SUB-TECHNIQUE RANK)	% OF CUSTOMERS AFFECTED
T1059: Command and Scripting Interpreter	**1**	**53.4%**
• T1059.001: PowerShell	(1)	(35.0%)
• T1059.003: Windows Command Shell	(2)	(28.1%)

Question 3) Submit the names of 2 vulnerabilities belonging to Exchange Servers

ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)
ProxyShell (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473)

Question 4) Submit the CVE of the zero day vulnerability of a driver which led to RCE and gain SYSTEM privileges

PrintNightmare (CVE-2021-34527)

On July 1, security researchers and Microsoft released details of a new vulnerability dubbed "PrintNightmare" (CVE-2021-34527). PrintNightmare permits an unprivileged user to remotely obtain elevated privileges on any system running the print spooler service, which is enabled by default. It abuses a vulnerability in how the print spooler service fails to properly authenticate users attempting to load a printer driver dynamic link library (DLL). This zero day affected all editions of Windows, allowing code execution with local SYSTEM-level privileges.

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

Adversaries behind both Gootkit and Yellow Cockatoo abuse search engine optimization (SEO) to display malicious content at the top of a victim's search results. Because compromised websites are displayed prominently

Question 6) In the detection rule, what should be mentioned as parent process if we are looking for execution of malicious js files

```
process == wscript.exe
&&
command_line_includes (.zip && .js)
&&
has_external_netconn
```

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

Qbot	Conti
Bazar	Conti
IcedID	Conti

Question 8) The main target of coin miners was outdated software. Mention the 2 outdated software mentioned in the report

TAKE ACTION

Compromises involving coinmining have been surprisingly consistent over the last few years, and many of the detection opportunities we have **shared previously** are still relevant. Focusing on post-exploitation activity should help, regardless of whether the initial access method is a weak SSH password, outdated web application, or exploitation of a vulnerability like **Log4Shell**.

The best defense against many of the coinminer compromises we observed is patch management. Many of the coinminers we saw exploited flaws in outdated applications like JBoss and WebLogic, so keeping systems updated will deter

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

Adversaries realized they could demand payment for more than just the threat of a data leak or encryption. An adversary known as **Fancy Lazarus** (no affiliation with Fancy Bear or Lazarus Group) extorted victims by threatening to conduct a distributed denial of service (DDoS) intrusion if they didn't pay.

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

TAKE ACTION

There is no one simple way to prevent ransomware. The same security approaches you take to prevent any malware also should help prevent ransomware. It's critical to regularly update software, as we often see ransomware after operators exploit a vulnerability in an internet-facing application. Additionally, internet-facing remote desktop protocol (RDP) connections without multi-factor authentication (MFA) are a common ransomware vector, making MFA for any accounts that can log in via RDP a high priority.