SCENARIO 1

In this task, you will be stepping into the role of a cybersecurity consultant here at Datacom. One of our leading tech corporation clients has fallen prey to a sophisticated cyberattack by a notorious Advanced Persistent Threat (APT) group known as APT34. The attack, believed to be sponsored by a foreign government, has left the organisation's network compromised, and valuable customer data and intellectual property has been stolen.

Your mission is to conduct initial research on this APT group, APT34, and assess the extent of the breach's impact on the organisation's information security. But fear not, for you will be provided with all the necessary tools required to understand cybersecurity concepts and principles, including cyberthreats, attack methods, and the importance of confidentiality, integrity and availability of information. In addition, you will also be familiarised with APT34's tactics, techniques and procedures (TTPs) and the common vulnerabilities they exploit to gain access to networks.

The objective of this task is to help our client conduct an initial investigation into APT34 and evaluate the potential impact of the attack on the organization. As a result, you will need to produce a comprehensive report documenting your findings and outlining key recommendations for improving the organisation's cybersecurity posture.

As you delve deeper into the world of cybersecurity, you will come to appreciate the critical role it plays in protecting organisations against cyberthreats. With the ever-increasing reliance on technology and the internet, cybersecurity has become a vital aspect of any organisation's operations. It is no longer a question of whether an organisation will be targeted but rather a question of when. This task provides you with an excellent opportunity to learn and gain practical experience in the cybersecurity field while making a positive impact on our client's security posture.

1. What is their history?

* HELIX KITTEN is likely an Iranian-based adversary group, active since at least late 2015

1. Which nation/state are they associated with?

* Iran-based

1. Do they target specific industries?

* Targeting organizations in the aerospace, energy, financial, government, hospitality and telecommunications business verticals, HELIX KITTEN actors were observed targeting entities in the Middle East.

1. What are their motives?

* HELIX KITTEN’s operations against organizations in the telecommunications industry could allow this adversary to conduct bulk data collection of large amounts of communications data that could be later leveraged in additional intelligence activities. Targeting telecommunications can also allow the adversary to be able to reroute communications to adversary-controlled infrastructure for data collection or malware delivery

1. What are the TTPs they use to conduct their attacks?

* This adversary group is most commonly associated with a custom PowerShell implant identified as Helminth. The Helminth implant is routinely delivered through macro-enabled Microsoft Office documents requiring user interaction to execute an obfuscated Visual Basic Script. Additionally, HELIX KITTEN actors have shown an affinity for creating thoroughly researched and structured spear-phishing messages relevant to the interests of targeted personnel

1. What security measures could the client implement to defend against cyberattacks conducted by this APT?

* Employee training
* Multifactor authentication
* End-point protection
* Network segmentation
* Incidence report plan

OSINT tools to gather information on APT34:

* Mandiant Security Blog: <https://www.mandiant.com/resources/blog>
* CrowdStrike: <https://www.crowdstrike.com/>
* Recorded Future: <https://www.recordedfuture.com/>
* CyberScoop: <https://www.cyberscoop.com/>
* Dark Reading: <https://www.darkreading.com/>
* The CyberWire: <https://thecyberwire.com/>
* SecureWorks - <https://www.secureworks.com/>
* ThreatConnect - <https://www.threatconnect.com>
* Kaspersky Lab: <https://www.kaspersky.com/>
* Symantec Threat Intelligence: <https://www.symantec.com/threat-intelligence>