Task 1: APT breach: analyzing the impact on Information Security

APT34

What is their history?

Advanced Persistent Threat (APT) group 34, also known as OilRig or HelixKitten, is a state-sponsored cyber espionage group that has been active since at least 2014. APT34 is believed to operate out of Iran and has been associated with the Iranian government, specifically the Islamic Revolutionary Guard Corps.

Which nation/state are they associated with?

APT34 is believed to be associated with the Iranian government. Some cybersecurity experts have linked the group to Iran's Islamic Revolutionary Guard Corps (IRGC), a powerful military organisation that is also involved in Iran's cyber operations.

Do they target specific industries?

APT34 is known for targeting a wide range of industries, including energy, finance, telecommunications and government agencies, mainly in the Middle East and the United States. The group's main objectives are to collect sensitive information and conduct cyber espionage activities on behalf of the Iranian government.

What are their motives?

The motives of APT34 are believed to be primarily espionage-related. They are known to target sensitive information such as intellectual property, financial data and government secrets. Some experts believe that APT34's activities are aimed at supporting Iran's strategic interests.

What are the TTPs (tactics, techniques and procedures) they use to conduct their attacks?

APT34 uses a variety of TTPs to conduct their attacks. Some of their known TTPs include spear-phishing, social engineering, malware delivery through malicious websites and password spraying. They have also been known to use custom malware, including a backdoor called POWRUNER. Once inside a target's network, APT34 uses various TTPs to maintain persistence and avoid detection. For example, the group often employs custom-built malware and command-and-control (C2) servers, and uses legitimate tools and software to evade detection.

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

To defend against cyberattacks conducted by APT34, clients could implement several security measures, including:

Employee training: providing regular cybersecurity awareness training to employees can help prevent spear-phishing attacks and other social engineering tactics used by APT34. - Multi-factor authentication (MFA): implementing MFA can prevent unauthorised access to sensitive data even if an attacker has gained access to login credentials.

Endpoint protection: deploying endpoint protection solutions such as anti-virus and anti-malware software can help detect and prevent malware infections.

Network segmentation: segmenting the network into smaller, isolated networks can help contain and prevent the spread of malware in case of a breach.

Incident response plan: having an incident response plan in place can help the client respond quickly and effectively in case of a security breach and minimise the impact of the attack.

By implementing these security measures, the client can better protect their networks and systems against APT34's attacks and other cyberthreats.

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

MITRE ATT&CK Framework (https://attack.mitre.org/): This is a widely used tool to categorise and identify cyberthreats. Students should familiarise themselves with the framework and understand how to apply it to develop a comprehensive defence strategy.

News and Other Resources: Students should stay up-to-date with the latest cybersecurity news and resources to gain a better understanding of the evolving cybersecurity landscape and new threats.

- Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/
- US-CERT: https://www.us-cert.gov/