**APT breach: analyzing the impact on information security**

1. **What is their history?**

APT34 is involved in a long-term cyber espionage operation largely focused on reconnaissance efforts to benefit Iranian nation-state interests and has been operational since at least 2014.

APT34 was formed in period of 2004-2007 by corporation of APT33 and Iranian government.

APT34 has targeted many of the same organizations as Advanced Persistent Threat 33, and APT34 is famously called Helix Kitten.

APT34 name was given by Trellix formally known as Fire Eye and was identified by Crowdstrike, APT34 uses a mix of public and non-public tools, often conducting spear phishing operations using compromised accounts, sometimes coupled with social engineering tactics.

1. **Which nation/state are they associated with?**

APT34 works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.

The group has reportedly targeted organizations in the financial, energy, telecommunications, and chemical industries, as well as critical infrastructure systems, They log into VPNs from Iranian IP addresses, adhere to normal Iranian business hours, their work has occasionally leaked Iranian addresses and phone numbers, and their efforts align with Iranian interests. Namely, targeting the country's adversaries.

1. **Do they target specific industries?**

This threat group has conducted broad targeting across a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East.

The group has reportedly targeted organizations in the financial, energy, telecommunications, and chemical industries, as well as critical infrastructure systems.

Beside this there particular interest is in aviation and energy sectors.

1. **What are their motives?**

There main motive are cyber espionage and cyber warfare against adversaries of Iranian nation.

The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea.

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

APT34 reportedly uses Microsoft Excel macros, Power Shell-based exploits and social engineering to gain access to its targets through Social engineering, Zero-days and Spear phishing and malware

The most successful and significant attack vector used by the Iranian APTs is the exploitation of known vulnerabilities in systems with unpatched VPN and RDP services.

1. **What security measures could the client implement to defend.**

**against cyberattacks conducted by this APT?**

1. Be cautious with emails from unknown sources. Do not open emails from strangers, such as those containing links, so as to prevent information disclosure or computer viruses.
2. Do not use weak passwords. Change passwords frequently and make sure strong enough passwords are used.
3. Fix vulnerabilities in time, especially those in border devices. Enable automatic update on not-frequently-used devices to keep the devices and their software latest.
4. Deploy border protection devices and an intelligence-based alerting system provided by security firms to nip security hazards in the bud.