Advanced Persistent Threat(APT) Group 34: Analysing the impact of information security

1) What is their history?

   Advanced Persistent Threat (APT) of group 34 also known as Helix Kitten, OilRig and Greenbug is a cybercriminal group that has attacked lots of organizations especially the Middle East and International Organizations. In 2017, they attacked an organization by exploiting Microsoft Office vulnerability using a custom PowerShell backdoor to achieve its objective.

2) Which nation/state are they associated with?

   It has been observed that APT34 works on behalf of the Iranian government based on infrastructure details that contain reference to Iran, use of Iran infrastructure, and targets that align with nation-state interests.

3) Do they target specific industries?

   The group has targeted a variety of industries, including information Technology, Financial, Government, Energy, Chemical and telecommunication and has largely focused its operation in the Middle East.

4) What are their motives?

   This group have been known to use various malware and tools to collect strategic and sensitive information that would benefit the economic and political interest of Iran. These attacks have been directly or indirectly connected to Iran's military, financial and political interests.

5) What are the TTPs they use to conduct their attacks?

   Most malwares used by this group are glimpse, webmask, twoface, valuevault etc. The most common attack vectors used are zero day attack, spam email, backdoor, spear phishing, remote code execution, malicious excel file

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

   What makes APTs terrifying is that once they have access to your system they will continue to quietly exploit your data over a period of time. Installing just antivirus software is not sufficient to protect against APT.

APTs differ from other types of cyber attack in that they are highly targeted and tailored to specific organizations or individuals. An extensive research is conducted on their target and sophisticated tactics are used to gain access to the network.

Prevention Tips

- Traffic Monitoring

To use Traffic Monitoring to defend against APTs, organizations can implement tools and technologies that allow them to monitor traffic in real-time and identify anomalies of malicious activity. Monitoring unusual activity on the database and watch for abnormality of data access requests. Usually this would require experienced teams and a strong IDS/IPS.

- Use of Endpoint Tools

One of the most preventive solutions to APTs is to make sure they never have access. Firewalls are security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. A strong antivirus should be an added layer of protection.

- Staff Training

One of the most important aspects of APT prevention is to train workers who have access to the system in the organization. They should be taught about security protocols such as how to browse securely, how to recognize phishing mails, tactics of social engineering and other attack vectors.

- Access Control

Access control is a security measure that involves limiting access to resources and systems to only authorized users. It can be used to defend against APT. Various technologies can be used such as user authentication which should be multi-factor authentication (MFA), role based access control (RBAC), access control lists (ACL) which is a list of permissions that specify which group of users or users can access specific resources or systems.