Peer Response by: Thomas Ranson

You make some excellent points Zihaad and thank you for the contribution.

I think the breach of the Marriott hotel chain through the acquired company, Starwood Hotels, opens a very interesting discussion on the importance of early detection in APT attacks.

It’s reported that about 57% of regional companies were subject to phishing attacks on their employees in 2018 (Positive Technologies, 2019). Of the different types of phishing, spear phishing is the most common method. This is a highly focused style of attack, personalised to the recipient. Gaining initial access to the target in this manner increases the APT group's likelihood of success and can be incredibly difficult to detect once executed.

It’s an interesting idea to explore for a hacker group to target smaller business groups that would have weaker security and less training for staff, thus increasing the likelihood of a phishing attempt being successful. For small to medium businesses, the cost of implementing cybersecurity measures could be as high as 4% of their operational budget (Meeuwisse, 2019). This is a cost that smaller businesses don’t want to pay, with the mindset that security breaches only happen at the big companies.

The danger of a company that is being acquired by a larger conglomerate being currently infected by an APT attack is very real in today's world, with the signs being almost invisible. When the two companies are merged and digital networks start to be connected it can open up the new parent company to the acquired company's vulnerabilities. With the general digital landscape lacking standardised security training it can never be assumed that any business is free from exploits.

References

Meeuwisse, R., 2019. Info Security. [Online]

Available at: https://www.infosecurity-magazine.com/blogs/effective-cybersecurity-expensive

[Accessed 23 August 2021].

Positive Technologies, 2019. Hack at all costs - Putting a price on APT attacks, s.l.: Positive Technoliges.