Cyber Security Alert

MIAA Technology Services January 2020

Cyber Vigilance

As you will be aware, there are heightened tensions in the Middle East with threats of attack and counter attack primarily involving Iran and the USA; though allies of the USA have also been referenced. While the attacks to date have been of a traditional military nature, there is no reason to suspect that this wouldn't extend, at some point, to cyber attack. There is significant evidence of Iranian based cyber activity from a number groups including:-

- **APT33 – also known as the Elfin Team, Refined Kitten and Magnallium** – who have been attributed with attacks on the defence, aerospace and petrochemical sectors in the USA, South Korea and Saudi Arabia using phishing as their primary route in to networks in order to wipe drives.

- **APT34 – also known as OilRig and HelixKitten –** who have launched attacks against the critical national infrastructure of numerous countries, using phishing, keylogging, and credential dumping to infiltrate networks. Details leaked regarding the group in 2019 specifically referenced three members of the Iranian Ministry of Intelligence amongst its membership.

- **APT35 – also known as Charming Kitten, ajax Security and NewsBeef** – who have been actively targeted government, military and technology secotrs in the USA, UK and Israel, using phishing and malware to extract data.

- **APT39** – who have focused on stealing personal data. Primarily targeting the travel and IT sectors in the USA, Turkey, Spain and middle eastern neighbours.

- **Cleaver –** who have targeted the military, aerospace and energy sectors in the USA, UK, Israel, France and Saudi Arabia primarily using social engineering a s a route to data theft.

- **CopyKittens** – who have attacked government, defence and academic institutions in the US, Israel, Germany and Saudi Arabia.

- **MuddyWater** - who have focused ion data extraction and have recently been seen to be actively targeting government, telecoms and oil sectors in Europe and North America.

While none of the above specifically reference attack on the health sectors, they do reference governments and wider public sectors. We should not assume that we are exempt from such activity either directly, or as WannaCry showed us, as collateral damage.

It is important that the messages of vigilance around taking care with unexpected email attachments, or links in emails, or social engineering are understood and that we all take time and take care with what we are doing to ensure that we don't fall victim to an attack.

ACTION REQUIRED

MIAA TechnologyServies recommend this alert is distributed to:

ALL STAFF for ACTION & AWARENESS

For further information on MIAA technology services visit miaa.nhs.uk

CONTACT
Tony Cobain
Assistant Director (Infomatics & Infrastructure)

07770 971006
tony.cobain@miaa.nhs.uk

MIAA
IMPROVE THE OUTCOME