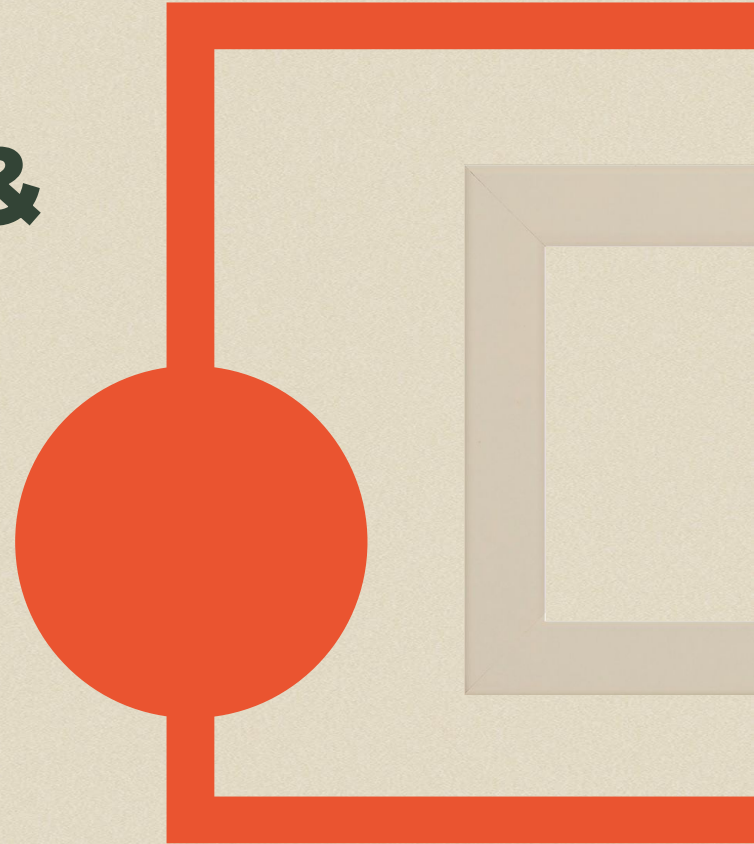


APT 41 (Barium) & Solar Systems

A practice on CKC and The Diamond Model from a blue team perspective





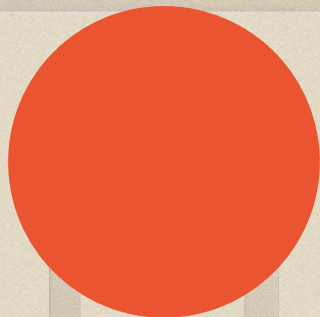
Problem statement

As a leader in manufacturing high efficiency solar systems, it has come to our attention that peers in our sector have been the victims of cyber espionage via nation-state actors, otherwise known as APTs(Advanced Persistent Threats). One APT in particular, APT41 (Barium) has been thought to be the threat based on artifacts found of intrusion.



Bottom Line Up Front (BLUF)

1. We must secure our systems and networks from intrusion and determine if we may have already been breached.
2. Maintaining confidentiality of our assets, namely research on solar systems is top priority.
3. Security awareness training to be done across entire company



Reconnaissance



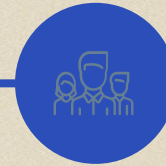
Determine Targets

Adversaries will be looking for leading manufacturers of solar system technology. Nothing can be done here



Determine Systems

Adversaries will be looking for easily targeted systems. We must ensure latest patches are installed.

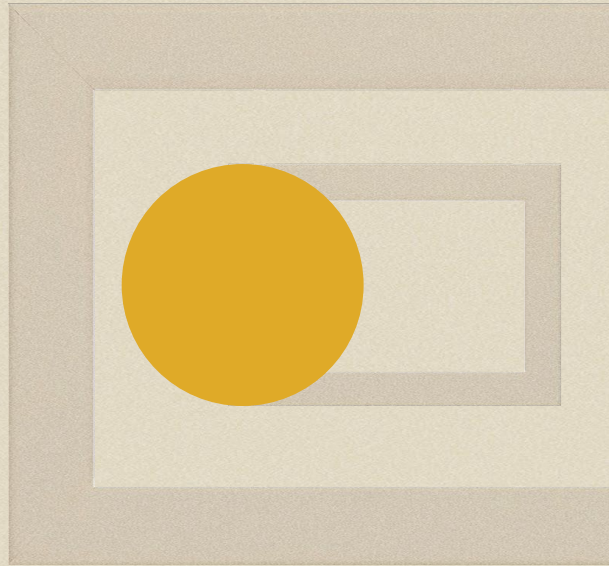


Determine Persons of interest

Adversaries will be looking at executives and engineering staff. Monitor public searches and limit information posted

Weaponization

During this phase there is not much to be done. Security awareness training will be given in order to keep all of our staff aware and capable of spotting the initial signs of phishing. Overall security awareness to be improved.



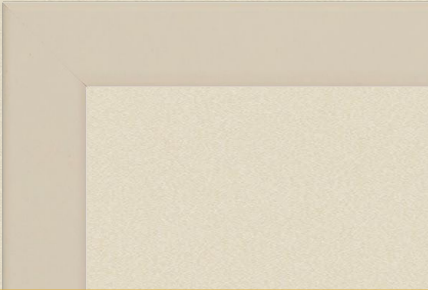

Delivery

Phishing and Vishing will be the most common form of delivery. Company wide training to authenticate callers to be conducted. E-mails with links attached or from unknown senders to be evaluated by infosec team. This will greatly reduce attack surface

Exploitation



Ensure Systems being run are updated and current. Ensure anti-virus is running and enabled. Ensure sensitive data is worked on secured systems to secure against exploitation. Air-gap from network to reduce attack surface.

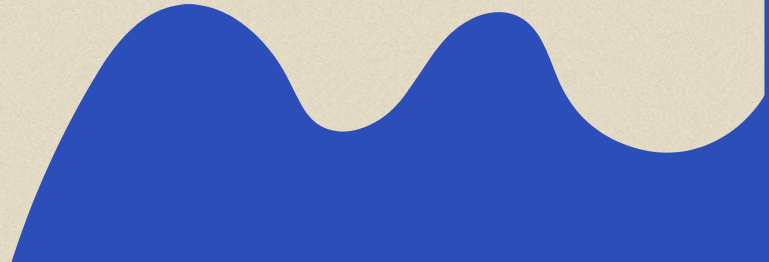
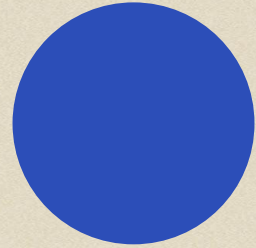


Installation

Abnormal behavior must be documented and investigated. Running processes that don't match the gold image or documented programs necessary for this system. Network activity is to be monitored for any abnormal traffic.

Command and Control(c2)

Systems/network has been confirmed compromised. From here we must hunt for abnormal outbound(beaconing) activity to stop and that can lead us to our adversary.



A decorative graphic consisting of a large yellow circle at the top, with two nested squares below it. The squares have a light beige, textured appearance. The title text is centered over the squares.

Actions on the objective

Properly trained incident response will now have to react to an incident that has just been identified or is persisting. Secure behaviors help to prevent us from getting here.

Conclusion

We must review our security processes and procedures for any improvements. Attacks on our sector have led to losses of confidential information and in order to prevent ourselves from becoming the next victim, we must actively practice our cyber defense.