Josiah Schmitz

Professor Darron Johnson

CEG-4420

September 9, 2025

Module 2 Assignment: APT3

APT3 is a group that is believed to be based in China, specifically associated with their Ministry of State Security. They have a history of attacking systems in America, though they seem to have shifted focus to Honk Kong over the past decade. They are also known as or heavily associated with names such as Gothic Panda, Threat Group-0110, and UPS.

Three of the techniques that they commonly use in their attacks are Brute Force: Password Cracking (T1110), Phishing: Spearphishing Link (T1566), and Remote Services: Remote Desktop Protocol (T1021). Brute Force: Password Cracking involves constantly trying a variety of possible passwords/hashes for a login in an attempt to gain access to a user’s credentials. This technique technically falls under the category of credential access, though it can also be thought of as an initial access technique, depending on the context of the attack. Phishing: Spearphishing Link is done by sending emails to carefully chosen targets instead of sending them en masse to hopefully have a user click a link containing malicious content or software of some kind. Spearphishing is often used as a method of getting initial access to a machine/system and is classified as such by MITRE. Remote Services: Remote Desktop Protocol is technique that requires the attacker to, through various methods, enable a remote desktop protocol (RDP) on a remote computer or server, allowing them to remotely and persistently access the targeted device. Similarly to Brute Force: Password Cracking, while this technique is not directly classified by MITRE as a persistence technique, instead being referred to as command & control, it does allow for persistent access to a system given the remote access nature of the technique.