(Notes) Cyber Kill Chain

Description

Some brief notes on the Cyber Kill Chain.

Notes

- Developed by Lockheed Martin.
- identifies what the adversaries must complete in order to achieve their objective.
- Enrich an analyst’s understanding of an adversary’s tactics, techniques and procedures.
- APT
    - A: *Advanced*
        - Targeted, Coordinated, Purposeful
    - P: *Persistent*
        - Month after Month, Year after Year
    - T: *Threat*
        - Person(s) with Intent, Opportunity, and Capability
- 7 steps to the Cyber Kill Chain
    - 1: *Reconnaissance*
        - Harvesting email addresses, conference information, etc.
    - 2: *Weaponization*
        - Coupling exploit with backdoor into deliverable payload
    - 3: *Delivery*
        - Delivering weaponized bundle to the victim via email, web, USB, etc.
    - 4: *Exploitation*
        - Exploiting a vulnerability to execute code on victim's system
    - 5: *Installation*
        - Installing malware on the asset
    - 6: *Command & Control (C2)*
        - Command channel for remote manipulation of the victim
    - 7: *Actions On Objectives*
        - With 'Hands on Keyboard' access, intruders accomplish their original goals

References

- Article: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html