1. **Adversary A** obtains list of users from Exchange Server and acquire access to the IT infrastructure with a valid username and password.

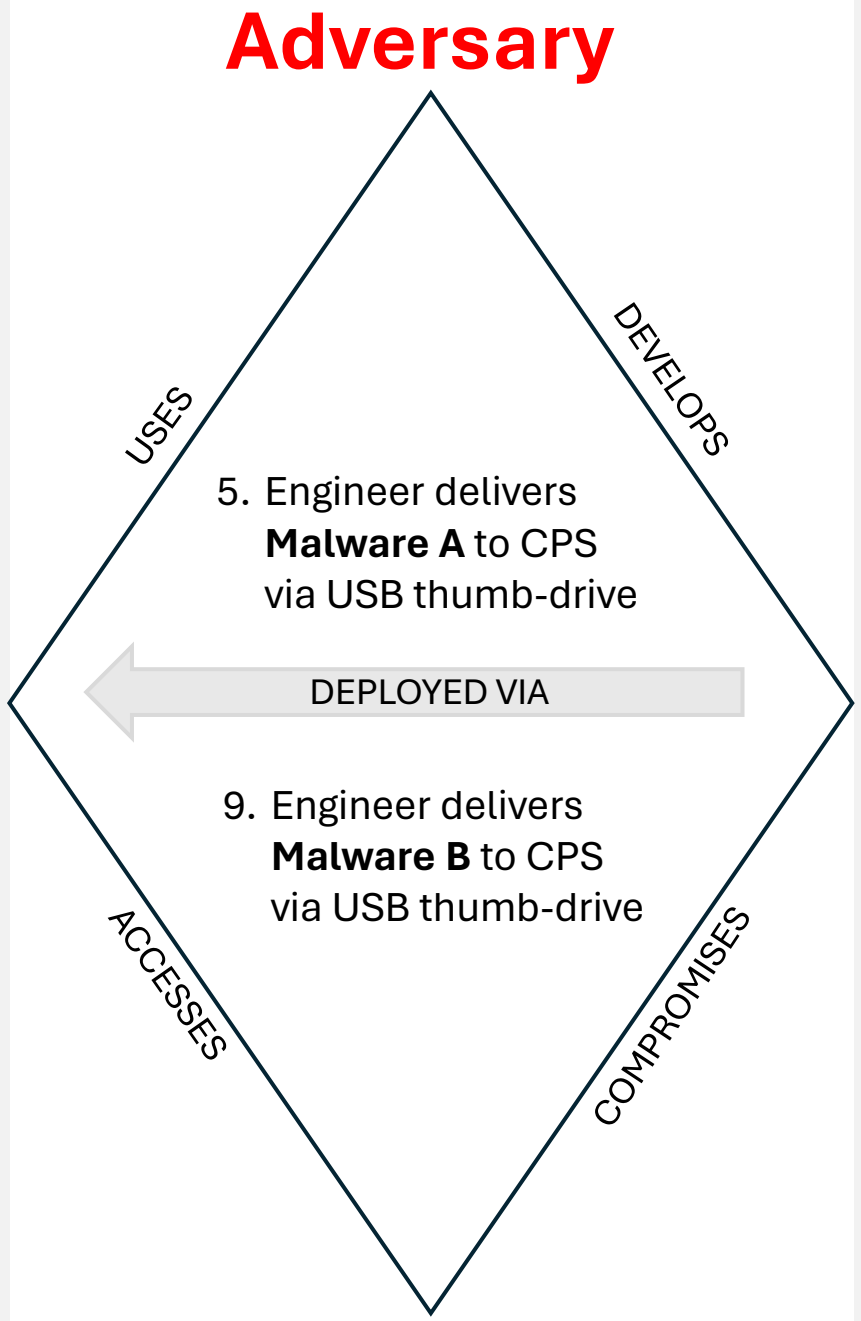
2. **Adversary A** performs lateral movement in the IT network, discovers and acquires remote access to the CPS engineer's computer.

Infrastructure

6. **Malware A** runs and collects network information. Saves it in engineer's thumb-drive at next access.

10. **Malware B** schedules task and hides in the background.

11. **Scheduled task manipulates connected RTUs causing physical damage.**



3. **Adversary B** customises **Malware A** to passively gather network information from CPS network.

4. **Adversary A** saves **Malware A** and autorun.inf in engineer's thumb-drive using social-engineering techniques to automatically install malware on CPS.

Capabilities (TTPs)

7. **Adversary B** customises **Malware B** to issue malicious commands to connected RTUs and suppress alarm reporting to central computer.

8. **Adversary A** saves **Malware B** and autorun.inf in engineer's thumb-drive using social-engineering techniques to automatically install malware on CPS.