-SolarWinds Attack Cyber Kill Chain-

- **RECONNAISSANCE**

  In early 2020, hackers secretly broke into Texas-based SolarWind's systems and added malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage IT resources. Solarwinds has 33,000 customers that use Orion, according to SEC documents.

- **WEAPONIZATION**

  Beginning as early as March of 2020, SolarWinds unwittingly sent out software updates to its customers that included the hacked code. The code created a backdoor to customer's information technology systems, which hackers then used to install even more malware that helped them spy on companies and organizations.

- **DELIVERY**

  The SolarWinds company sent a software update which contains malicious code dropped by hackers to their customers.

- **EXPLOITATION**

  When the customers of SolarWinds executed the update the code entered their systems immediately.

- **INSTALLATION**

  Hackers install the malicious code to the software update.

- **COMMAND AND CONTROL**

  Attackers had gained control when the code got into the companies systems and their goal was learning confidential information about the companies.

- **ACTIONS ON OBJECTIVES**

  Intruders accomplished their goals by infiltrating the company software and systems.