**Case Study**

**Title:** SolarWinds Supply Chain Attack

**Introduction:**

SolarWinds Corporation is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure. It is headquartered in Austin, Texas, with sales and product development offices in a number of locations in the United States and several other countries.

In December 2020, the SolarWinds supply chain was attacked and is considered one of the most significant cyber-attacks in recent history. It affected numerous government agencies and organizations worldwide. The attack was carried out by hackers believed to be affiliated with the Russian government, who were able to infiltrate the network of SolarWinds, a leading software company that provides network management tools to numerous government agencies and Fortune 500 companies. This case study will cover the methodology, impact, attribution, lessons learned, and conclusion of the SolarWinds supply chain attack.

**Attack Methodology:**

FireEye reported the hackers inserted "malicious code into legitimate software updates for the Orion software that allow an attacker remote access into the victim's environment" and that they have found "indications of compromise dating back to the spring of 2020". FireEye named the malware SUNBURST. Microsoft called it Solorigate.

The attackers were then able to exfiltrate sensitive data and cause significant damage. The scope of the attack is still being investigated, but it is believed to have affected numerous government agencies and organizations worldwide, including the U.S. Department of Justice, the Treasury Department, and Microsoft.

The attackers were highly sophisticated and used multiple tactics to avoid detection, including using legitimate credentials, hiding their activities within normal network traffic, and using encryption to conceal their communications. The attackers also used a technique known as "DNS tunneling" to send stolen data out of the network undetected.

**Impact:**

The SolarWinds supply chain attack had a significant impact on numerous government agencies and organizations worldwide. The attack allowed the attackers to gain access to sensitive data, including email communications and classified information. The attack also caused significant disruption to the affected organizations, with some government agencies temporarily shutting down their networks to contain the attack. Victims of this attack include the cybersecurity firm FireEye, the US Treasury Department, the US Department of Commerce's National Telecommunications and Information Administration, as well as the US Department of Homeland Security. Prominent international SolarWinds customers investigating whether they were impacted include the North Atlantic Treaty Organization (NATO), the European Parliament, UK Government Communications Headquarters, the UK Ministry of Defence, the UK National Health Service (NHS), the UK Home Office, and AstraZeneca.

**Attribution:**

The SolarWinds supply chain attack has been attributed to hackers believed to be affiliated with the Russian government. APT29, aka Cozy Bear, working for the Russian Foreign Intelligence Service (SVR), was reported to be behind the 2020 attack. The attack is believed to be part of a broader campaign of cyber espionage and disruption targeting U.S. government agencies and organizations.

**Lessons Learned:**

The SolarWinds supply chain attack highlights the significant risks posed by supply chain attacks and the importance of robust security measures, including regular security assessments and monitoring, for both software vendors and their customers. The attack also underscores the need for increased international cooperation and information sharing to combat cyber threats. The attack has also led to calls for increased regulation and oversight of software vendors to ensure the security of their products.

**Conclusion:**

The SolarWinds supply chain attack is a stark reminder of the significant risks posed by cyber threats and the need for robust security measures. The attack has highlighted the importance of regular security assessments and monitoring, increased regulation, and oversight of software vendors, and increased international cooperation to combat cyber threats. The SolarWinds supply chain attack is a wake-up call for organizations worldwide to take cybersecurity seriously and to take proactive measures to protect themselves from cyber threats.