Readme File for Teachers:  
Case Study on SolarWinds Hack

**Abstract:**In this case study, students will look into the detail of the SolarWinds supply chain attack happened in 2020. Students will learn how the attack take place from the beginning to the end. During the process of case analysis, a list of security topics reflecting different aspects of the breach is introduced. Through guided in-class discussion and hands-on lab assignments, student learning in lecture will be reinforced.

**Target audience:**Undergraduate, Graduate

**Objectives:**

* Describe the SolarWinds hack
* Explain themes in supply chain security
* Explain Advanced Persistent Threat (APT)
* List common defense mechanisms against cyber attacks
* Explain backdoors and how to prevent them

**Keywords:**Supply chain security, APT attack, backdoors

**Description:**This case study provides a comprehensive analysis of the sophisticated cyber-attack on SolarWinds, a major IT management software provider. The hack, attributed to Russian state-sponsored actors, involved compromising SolarWinds' Orion software updates, leading to the infiltration of numerous high-profile organizations, including U.S. federal agencies and Fortune 500 companies. The attackers gained unauthorized access by embedding a backdoor, known as SUNBURST, into the Orion platform updates, which were then distributed to SolarWinds' extensive client base. The presentation outlines the timeline of the breach, from the initial compromise in September 2019 to the public revelation and subsequent response actions in late 2020. It highlights the scale and complexity of the attack, demonstrating the vulnerabilities in software supply chains and the challenges in detecting and mitigating such advanced threats.

In addition to the incident details, the presentation emphasizes the broader implications of the SolarWinds hack for supply chain security and the evolving landscape of cyber threats. It discusses the critical role of Advanced Persistent Threats (APTs) in maintaining prolonged access and causing significant damage. The analysis extends to the defensive measures needed to combat similar attacks, including improving software development practices, enhancing threat detection capabilities, and strengthening international cybersecurity collaboration. The presentation concludes with a reflection on the lessons learned, urging organizations to adopt more robust security protocols to safeguard against future supply chain compromises.

**Cybersecurity topics:**Supply chain security, APT attack, backdoors

**Teaching resources for the case:**A study package with the following materials was developed for the case:  
a) A PowerPoint presentation explaining technical details and lessons learned for the case: used by the instructor to guide the classroom discussion.   
b) A list of discussion questions: It is suggested to ask students to finish the discussion questions before attending the in-class discussion.  
c) A video tutorial introducing the case: For instructors or online students.   
The video can also be used before the in-class discussion. Students will be asked to finish the video before attending the in-class discussion.

**Additional third-party resources for the case:**

* <https://en.wikipedia.org/wiki/SolarWinds>
* [https://web.archive.org/web/20201214092129/https://www.solarwinds.com/orion-platform](https://web.archive.org/web/20201214092129/https:/www.solarwinds.com/orion-platform)
* <https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html>
* <https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/>
* <https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack/>
* <https://www.theverge.com/2021/4/15/22385371/russia-sanctions-solarwinds-biden-white-house-putin-hack>
* <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>

**Language:**English

**Date created:**   
May 1, 2023

**Last update:**   
May 1, 2024