ENPM 686

Samridha Murali

3/28/2022

Current Event 8

Solarwinds is a Texas-based company that provides IT monitoring and management tools [1]. It's monitoring tools are used by more than 30,000 organizations including multinational companies and government agencies [2] . Attackers intruded into Solarwinds system as early as September 2019 and injected malicious code (sunburst) into Solarwinds' Orion platform in October 2019. In March 2020, Solarwinds sent software patches for Orion tool with malicious code hidden in it [2]. This was first detected by FireEye (a cyber security firm) in December 2020 [3]. Solarwinds notified its customers and sent upgrades to the platform. A Russian hacker group called Nobelium is believed to be behind this attack [4].

The malicious update was installed by around 18,000 customers around the world, including several government departments (like Homeland Security, State, Commerce and Treasury) and private companies (like FireEye, Microsoft, Intel, Cisco and Deloitte) [5]. Hackers gained access to the network and data of Solarwinds customers because of the backdoor delivered by Solarwinds. Solarwinds attack cost affected companies on average 11% of their annual revenue[6]. It cost insurance companies a loss of $200 million[7].

Hackers compromised Orion software using a compromised Microsoft 365 account [8], so strong password policies should be implemented. Additional care must be taken before sending software updates. Software updates and patches should undergo heavy security reviews and checks before getting published. All internal sensitive data should be kept encrypted using strong algorithms to prevent data from getting compromised.

References :

[1]. “It Management Software & Remote Monitoring Tools.” SolarWinds, https://www.solarwinds.com/.

[2]. Saheed Oladimeji, Sean Michael Kerner. “Solarwinds Hack Explained: Everything You Need to Know.” WhatIs.com, TechTarget, 16 June 2021, https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[3]. Baker, Pam. “The Solarwinds Hack Timeline: Who Knew What, and When?” CSO Online, CSO, 4 June 2021, https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.

[4]. Baker, Pam. “The Solarwinds Hack Timeline: Who Knew What, and When?” CSO Online, CSO, 4 June 2021, https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.

[5]. Combs, Veronica, et al. “Cybersecurity Study: Solarwinds Attack Cost Affected Companies an Average of $12 Million.” TechRepublic, 28 June 2021, https://www.techrepublic.com/article/cybersecurity-study-solarwinds-attack-cost-affected-companies-an-average-of-12-million/.

[6]. Trunkes, Virginia K. “Solarwinds Cyber-Attack Has Significant Implications for Developers and Contractors.” NewsBreak, National Law Review, 14 Jan. 2021, https://www.newsbreak.com/news/2144778563874/solarwinds-cyber-attack-has-significant-implications-for-developers-and-contractors.

[7]. Novinson, Michael. “SolarWinds Hack Could Cost Cyber Insurance Firms $90 Million.” CRN, 14 Jan. 2021, https://www.crn.com/news/security/solarwinds-hack-could-cost-cyber-insurance-firms-90-million.

[8]. Combs, Veronica, et al. “Cybersecurity Study: Solarwinds Attack Cost Affected Companies an Average of $12 Million.” TechRepublic, 28 June 2021, https://www.techrepublic.com/article/cybersecurity-study-solarwinds-attack-cost-affected-companies-an-average-of-12-million/.