SolarWinds Attack Case Study

SolarWinds/U.S Federal Government

Supply Chain Attack

- A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. - CrowdStrike

- Software supply chain attacks inject malicious code into an application in order to infect all users of an app, while hardware supply chain attacks compromise physical components for the same purpose. - CrowdStrike

- Below are some 2021 statistics from CrowdStrike's Global Security Attitude Survey:

  1. 84% believe that software supply chain attacks could become one of the biggest cyber threats to organizations like theirs within the next three years
  2. 45% of respondents' organizations experienced at least one software supply chain attack in the last 12 months, compared to 32% in 2018
  3. 59% of organizations that suffered their first software supply chain attack did not have a response strategy

- SolarWinds is a major software company based in Tulsa, Okla. Which provides system management tools and other technical services to hundreds of thousands of organizations around the world. Among these tools is an IT performance monitoring system called Orion. - TechTarget

- As an IT monitoring system, SolarWinds Orion has privileged access to IT systems to obtain log and system performance data. It is that privileged position and its wide deployment that made SolarWinds a lucrative and attractive target. - TechTarget

- The SolarWinds attack was a complex attack that injected malicious code into the software’s build cycle and initially infected about 18,000 customers downstream, including major firms and government agencies that were secured by the strongest cybersecurity tools and services available today. - CrowdStrike

Timeline

SolarWinds Attack

1. September 2019. Threat actors gain unauthorized access to SolarWinds network
2. October 2019. Threat actors test initial code injection into Orion
3. Feb. 20, 2020. Malicious code known as Sunburst injected into Orion
4. March 26, 2020. SolarWinds unknowingly starts sending out Orion software updates with hacked code
5. April 2020, The malware started to contact command-and-control servers, initially from North America and Europe and subsequently from other continents too

Vulnerabilities

The attack started with small tests such as integrating minor changes in code and taking advantage of the trust between SolarWinds and its customers via software updates. This, combined with loopholes in the supply chain, easy access through SSO's, and overtaking MFA systems allowed attackers to implant malware without setting off alarms.

Leveraging the supply chain

Attackers gained access to the company's development process and leveraged customer-vendor trust to gain access to thousands of systems

Taking advantage of single sign-on systems

Attackers leveraged the use of SSO's by the compromised organizations to gain access to the administrative accounts within the organizations

Exposing traditional multifactor authentication systems

Attackers gained access to several critical servers within the compromised organizations with a username and password and bypassed MFA

Taking advantage of U.S Based IP Addresses

By using U.S based IP addresses for C2, the attackers were able to evade detection by Einstein, a cybersecurity system operated by the Department of Homeland Security

Costs

- Around 18,000 users installed the compromised versions, including the U.S government.
- SolarWinds said it spent 18 million to 19 million to "investigate and remediate the cyber incident"
- Companies in the U.S. reported an average of a 14% impact on annual revenue.
- Fewer than 10 U.S. agencies were potentially compromised by follow-on activity.
- "The true cost could be hundreds of billions of dollars," Jake Williams a Cybersec Firm owner said, when asked about the total cost of the breaches
- SolarWinds claimed that its clients included 425 of the Fortune 500 companies

Prevention

- Implement a Zero Trust Architecture
- Implement Honeytokens
- Secure Privileged Access Management
- Identify and protect vulnerable resources
- Minimize access to sensitive data
- Assume you will suffer a data breach