What is a Supply Chain Attack?

By: Jack Gerbs, Quanexus

The SolarWinds attack in the news has brought up many new terms that may not be familiar to business owners.Today we are going back-to-basics to discuss supply chain attacks.

Every business uses third party software and hardware. Even the smallest business has to communicate with vendors and customers, receive, ship, bill, and inventory. A supply chain attack occurs when criminals infiltrate your system through an outside partner or provider with access to your systems and data. When a supply chain attack occurs, hackers have access to the same data and permissions the software infiltrated has access to.

Attackers target software developers and suppliers looking for access to source code, or update tools. The goal is to infect a legitimate piece of software and use that software to distribute malware to customers. Hackers break into manufacturers' servers and hide malware in softwareupdates. When these updates are pushed out by trusted vendors, the updates are certified as safe.Customers who are following sound IT practices patch and update their systems regularly, and unknowingly add the malware to their systems.

> **"The goal is to infect a legitimate piece of software and use that software to distribute malware to customers."**

The SolarWinds attack is greatly con-sequential for two reasons. First, the Orion tool is a Network ManagementSystem, meaning the hackers gained access at the network level, and had the same permissions the management tool had. This allowed attackers to change network settings, move laterally through the network, and also target the user level. Second, the Orion tool is used

by large corporations, and the US Government. The SolarWinds Network ManagementSystem is used by 425 of the US Fortune 500.

Many of the large cyberattacks that make the news are supply chain attacks. The Target breach in 2014 was blamed on a third party vendor, as well as the Equifax breach in 2017. The SolarWinds attack is the largest and most consequential supply chain attack we have seen, but it follows a pattern well established in the cybercrimelandscape.