Flynet Vitality Brief:
Protecting Against Supply Chain Attacks

Situation
Supply Chain Attacks are on the rise. This type of cyberattack targets an organization's systems through compromised third-party software and their prevalence has grown by 42% in early 2021.

Obstacle
Many organizations may be vulnerable to Supply Chain Attacks without realizing it, as it can be hard to detect which elements of the supply chain are compromised.

This can be especially challenging for users of terminal emulators. Some organizations don't mandate or standardize which technology end users should use, giving them complete flexibility and freedom in what emulators they use to access systems.

If some users are using insecure terminal emulators that require the java applet, downloads, or plugins it can increase an organization's threat surface to Supply Chain Attacks.

Implication
Supply Chain Attacks can potentially cause significant problems for organizations and individuals such as: the leaking of customer data, ransom demands, data deletion, unexpected downtime, and a plethora of other potential threats.

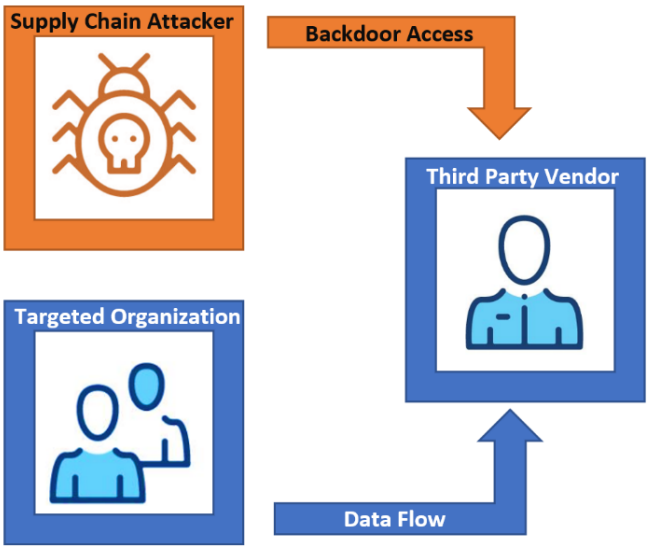
For example: the networks, systems and infrastructure software firm Kaseya were the victim of a ransomware attack in 2021 which caused widespread downtime to over 1,000 companies relying on their software.

The SolarWinds attack of 2020 compromised the company's Orion software. It targeted high-level government and private organizations, causing an international incident, and went unnoticed for months before detection.

Solution
The best prevention method against a Supply Chain Attack is to make sure an organization's software estate is as secure as possible. For users of terminal emulators this means ensuring a standardized terminal emulator across all users, internal and external, with no gaps or inconsistencies.

Furthermore, it means ensuring the terminal emulator is secured end-to-end, and is fully plugin, download and applet free.

Using a terminal emulator with these traits, such as Flynet Viewer TE, will ensure that all users accessing the organization's vital business systems have the same high level of security: reducing the threat surface for Supply Chain Attacks.



Conclusion
An end-to-end secure terminal emulator like FlynetViewer TE is an effective way of defending your organization from Supply Chain Attacks.

www.flynetviewer.com

Learn More | Download | Contact