Supply Chain Attact

供應鍊是指參與其中的流程、人員、組織和分銷商的生態系統。

最終解決方案或產品的創建和交付5

.在網絡安全方面，供應鏈涉及廣泛的

資源（硬件和軟件）、存儲（雲或本地）、分發機制（Web 應用程序、在線

商店）和管理軟件。

底下有四項供應鏈的要素

1. 供應商：是向另一個實體提供產品或服務的實體

2. 供應商資產：供應商用於生產產品或服務的有價值的元素

3. 客戶：是消費供應商生產的產品或服務的實體

4. 客戶資產：是目標擁有的有價值的元素

供應鏈攻擊是一種以軟體發展人員和供應商為目標的新興威脅。 目標是要存取原始程式碼、建立程式或更新機制，方法就是感染合法應用程式來散佈惡意程式碼。

攻擊者會搜尋不安全的網路通訊協定、未受保護的伺服器基礎結構，以及不安全的編碼作法。 他們入侵、變更原始程式碼，以及隱藏在建立和更新流程中的惡意程式碼。

由於軟體是由信任的廠商建立和發行，因此這些應用程式和更新會經過簽署和認證。 在軟體供應鏈攻擊中，廠商可能不知道他們的 App 或更新在發佈給大眾時受到惡意程式碼感染。 惡意程式碼接著會以與應用程式相同的信任和許可權執行。

供應鏈攻擊類型

遭到入侵的軟體建建工具或更新的基礎結構

使用開發人員公司身分識別的遭竊程式碼簽署憑證或已簽署的惡意應用程式

已出貨至硬體或固件元件之特殊程式碼遭到入侵

在裝置上預先安裝的惡意 (相機、USB、手機等)

如何防範供應鏈攻擊

部署強大的程式碼完整性原則，只允許授權的應用程式執行。

使用端點偵測和回應解決方案，自動偵測及補救可疑活動