資財四乙 107AB0719 王永龍

網路系統與安全期中報告

A.9 APACHE NETBEANS:DEVELOPMENT PLATFORM

從文章中可以知道這是一起開源軟體供應鏈攻擊事件，GitHub上的大量NetBeans代碼庫被惡意軟體Octopus Scanner感染成為傳染點，Octopus Scanner是專門為感染NetBeans專案而設計的後門，它直接感染了GitHub上的開發工具，這些工具隨後感染了他們正在從事的所有專案，性質要比常見的將GitHub平臺作為惡意軟體C2伺服器嚴重得多。

Octopus Scanner惡意軟體證實了分析代碼中二進位檔的重要性，而不僅僅依靠清單。Octopus Scanner如此危險的原因在於它具有感染專案中其他JAR檔的能力，因此開發人員最終使用"有毒"代碼並將其分發給他們的團隊或開放原始程式碼用戶社區。

GitHub 的安全事件回應團隊 （SIRT）收到了來自安全研究員JJ的一組存儲庫的初始通知，這些存儲庫為受惡意軟體感染的開源專案提供服務。SIRT 通常會接收和分類有關不良行為者濫用 GitHub 儲存庫來主動託管惡意軟體或試圖將 GitHub 平臺用作命令和控制 （C2） 基礎結構的一部分的報告。但這份報告有所不同。存儲庫的所有者完全不知道他們正在將後門代碼提交到其存儲庫中。

一旦使用者被 Octopus 掃描程式感染，它就會繼續搜索在開發系統上使用 NetBeans IDE 的跡象。如果不是這樣，它就不會採取任何進一步的行動。但是，如果發現，惡意軟體將通過以下機制繼續進行 NetBeans 項目構建的後門：

1. 它確保每次構建專案時，任何生成的JAR文件都會感染所謂的滴管。dropper 是一種將某些內容「丟棄」到文件系統以執行的機制。執行時，dropper 有效負載可確保本地系統持久性，並隨後生成一個遠端管理工具 （RAT），該工具連接到一組 C2 伺服器。
2. 它嘗試阻止任何新專案生成替換受感染的專案生成，以確保其惡意生成專案保留在原位。

防止Octopus Scanner的方法:

1.不使用NetBeans

2.幫助檢測依賴項中的問題，使用依賴關係圖，易受攻擊依賴項的安全警報以及自動安全更新等功能