資財三乙 108AB0722 郭韋彤

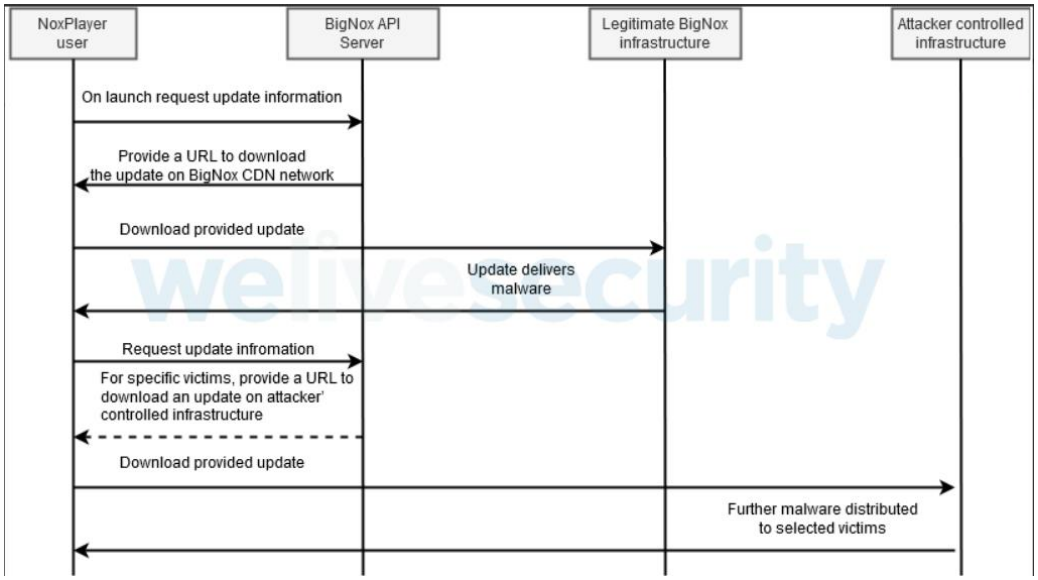
BIGNOX NOXPLAYER: ANDROID EMULATOR FOR PCS AND MACS

一、事件描述：

知名 Android 遊戲模擬器 NoxPlayer（夜神模擬器）的更新機制遭到駭客危害，使得駭客得以藉由 NoxPlayer 用戶更新時，植入惡意程式，一旦安裝在 Windows 或 macOS 上，就能於個人電腦上執行 Android 遊戲。根據調查，駭客是在 2020 年 9 月滲透了 NoxPlayer 的更新機制，且儘管 NoxPlayer 擁有廣大的用戶，卻只有極少數的使用者遭到駭客鎖定，在 10 萬名用戶中，只有 5 名使用者收到了惡意更新，而這 5 名受害者分別位於臺灣、香港與斯里蘭卡，此外，駭客在這些惡意更新中所植入的惡意程式並非用來獲利，而是專注於監控。

二、攻擊手法：

當時揭露這起攻擊行動的防毒廠商 ESET，近期公開了駭客的身分與手法，背後發動攻擊的 APT 駭客組織，被命名為 Gelsemium。對於 Gelsemium 擅長的手法而言，ESET 認為是藉由微軟 Office 的漏洞與釣魚郵件，來散布用來攻擊的惡意軟體，並且利用 Exchange 伺服器的 RCE 漏洞，來進行水坑式攻擊。攻擊者入侵了該公司的官方 API( api.bignox.com)和文件託管服務器 ( res06.bignox.com)之一，一旦在目標基礎設施中立足，他們就篡改了 API 服務器中 NoxPlayer 更新的下載 URL 提供受污染的更新。關於該更新渠道，ESET 稱他們有足夠的證據表明 BigNox 基礎結構被篡改並用於託管惡意軟體。入侵流程圖如下，攻擊者通過未知手段能夠過濾目標的請求，從而精確針對目標進行木馬下發。




三、後續處理與改善：

BigNox 更新了 NoxPlayer 版本，新版本將會查驗先前安裝的夜神模擬器檔案是否完整。針對 NoxPlayer 供應鏈攻擊，BigNox 採取以下 3 項防護措施：

1.僅透過 HTTPS 提供更新軟體，降低域名劫持(Domain Hijacking)與中間人攻擊之風險。

2.透過 MD5 雜湊值與檔案簽名檢查進行完整性驗證。

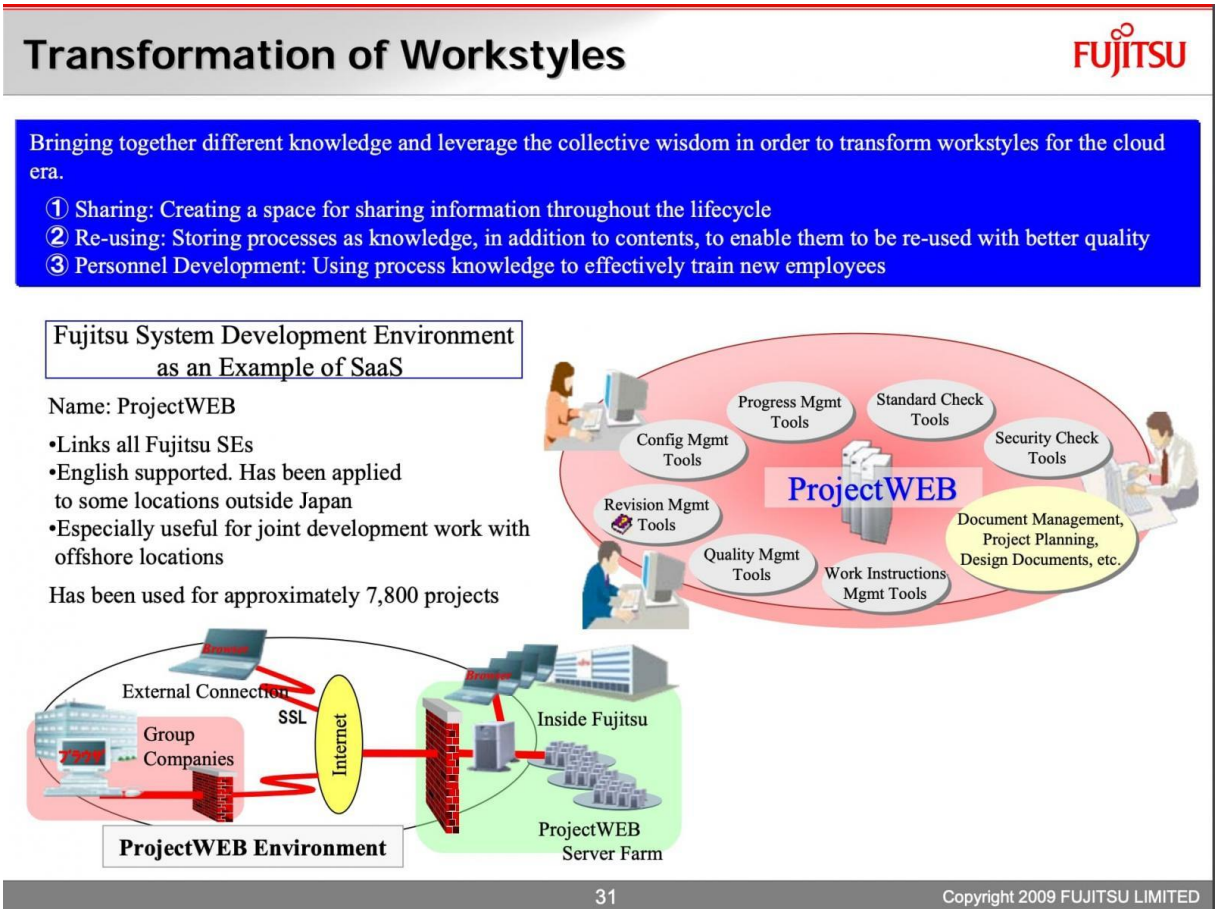
3.採取其他措施，特別對敏感資料進行加密，避免洩漏使用者個人資訊。

FUJITSU PROJECTWEB：COLLABORATION AND PROJECT MANAGEMENT SOFTWARE

日本富士通(Fujitsu)於 5 月 24 日證實，日本政府與企業廣泛使用之雲端共享資料平台 ProjectWEB 遭駭客入侵，導致軟體用戶數據資料外洩，受駭單位包括成田國際機場、國土交通省及國家資訊安全中心等。

雲端共享資料平台 ProjectWEB 為富士通提供之軟體即服務(Software-as-a-Service, SaaS)，富士通接受客戶委託建構業務系統或客戶運用其服務時，其系統工程師與合作人員等可透過 ProjectWEB 平台共享該專案相關資料。

被盜數據包括政府僱員存儲在 ProjectWEB 上的文件，ProjectWEB 是富士通於 2000 年代中期推出的基於雲的企業協作和文件共享平台，如今已被日本政府機構廣泛使用。國土交通省於 5 月 26 日公布，至少有 7 萬 6000 名轄下公務員與業務相關人員之電子郵件帳號、內部電子郵件系統資通系統架構等資訊外洩。甚至日本政府中負責資訊安全對策的「內閣網路安全中心」也是受害單位，中心內資訊系統所使用的機器設備與組成等相關數據也遭竊。ProjectWEB 漏洞是在日本政府機構今年早些時候成為類似攻擊的目標之後發生的。之前的攻擊針對的是 Soliton 製造的 FileZen 文件共享服務器，這些服務器也被日本政府機構廣泛使用。內閣網路安全中心表示，將會針對遭竊的資料研擬對策，防止遭到網攻並加強警戒。




上圖為富士通 ProjectWEB 概述說明信息共享工具的不同使用情況