Operation NightScout

NoxPlayer 是一個跨平台的 Android 模擬器軟體，能於個人電腦上執行 Android 應用，在全球 150 個國家擁有 1.5 億名用戶。NoxPlayer 母公司 BigNox 總部位於香港，也使得該軟體在亞洲地區特別熱門。

ESET 於 2021 年 2 月 1 日指出，知名 Android 遊戲模擬器 NoxPlayer 的更新機制遭到駭客入侵。他們發現 3 個不同的惡意軟體從訂製的更新中，發送給五位選定的特定目標，但並沒有發現任何經濟利益的跡象，只是專注於監控使用者，包括鍵盤紀錄與使用者敏感資訊，ESET 將此波攻擊行動命名為「Operation NightScout」。

根據 ESET 的調查，駭客於 2020 年 9 月滲透了 NoxPlayer 的更新機制，透過攻擊與竄改 NoxPlayer 的供應鏈，讓使用者在更新軟體時，下載到惡意軟體。且 ESET 表示，此事件不太可能是遭到中間人攻擊，因為受害者分布在不同國家，而且研究人員已經從 BigNox 的基礎設施下載了惡意程式的樣本，因此可以確定 BigNox 的基礎設施已經被駭客進駐。

針對 NoxPlayer 供應鏈攻擊，BigNox 目前採取以下 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，如加密機敏資訊等，避免用戶個人機敏資訊外洩。