期中報告　供應鏈資安 攻擊案例

A.5 ABLE DESKTOP: CHAT SOFTWARE

Able 是一家總部位於蒙古的公司，為該地區的政府機構和企業提供軟件解決方案。2020 年 6 月，攻擊者似乎訪問了 Able 的後端並破壞了向所有客戶提供軟件更新的系統。攻擊者將惡意軟件添加到“Able Desktop”應用程序（為 Able 的主要產品提供即時消息的附加組件）。雖然不知道供應商是如何受到攻擊的，但攻擊者能夠強迫用戶安裝惡意軟件。然後使用惡意軟件從受感染的客戶設備中竊取信息。攻擊歸因於 APT TA428。

一個中國國家資助的黑客組織，也被稱為 APT，被懷疑入侵了一家蒙古軟件公司，並破壞了數百個蒙古政府機構使用的聊天應用程序。最初的攻擊圍繞向 Able Desktop 聊天應用程序添加惡意軟件，並通過電子郵件傳播應用程序安裝程序的木馬版本，希望誘使員工感染自己。這些攻擊中的有效載荷包括 HyperBro 後門和 PlugX 遠程訪問木馬。

但是，儘管這些攻擊取得了成功，但 ESET 表示，事情在 2020 年 6 月發生了變化，當時攻擊者似乎在 Able 的後端找到了一種方法，並破壞了向所有 Able 軟件應用程序提供軟件更新的系統。ESET 研究人員表示，攻擊者至少兩次濫用該系統，通過官方更新機制提供帶有惡意軟件的 Able Desktop 聊天應用程序。對於這些攻擊，入侵者再次交付了 HyperBro 後門，但他們從 PlugX 改 Tmanager 作為遠程訪問組件。

為了防止進一步的攻擊，Able Soft 停止了 Able Desktop 更新，並且他們觀察到的此類攻擊最後一次發生是在 2020 年 7 月。