Gmail Amber <a47u0905@gmail.com>

(no subject)

Amber <a47u0905@gmail.com> Fri, Sep 12, 2025 at 12:22 PM
To: Amber <a47u0905@gmail.com>

中國駭客集團大舉攻擊台灣半導體產業　四個未知APT組織展開多重攻勢

2025 / 07 / 18 編輯部

網路安全公司Proofpoint最新研究揭露，中國國家級駭客組織已將台灣半導體產業列為重點攻擊目標，並在2025年3月至6月期間展開大規模網路攻擊行動。該公司識別出四個先前未被記錄的中國先進持續威脅（APT）組織，分別以不同手法對台灣晶片產業進行滲透。

攻擊目標涵蓋整個半導體生態

根據Proofpoint威脅研究員Mark Kelly的說法，過去五年中，針對台灣半導體產業的攻擊案例相對稀少，「可能一年只有一兩次，甚至只看到一家組織被攻擊」。然而，今年的攻擊量明顯激

增，顯示中國對台灣半導體產業的網路間諜活動已大幅升級。

這些攻擊並非僅限於半導體製造商本身。攻擊目標涵蓋了從晶片設計、封裝、測試到供應鏈服務的整個產業生態系統，甚至延伸到專精於台灣半導體市場的金融投資分析師。Kelly指出，「這種針對性顯示攻擊者可能對新興市場資訊感興趣，包括特定公司的動向、是否有特殊或新的產品線，或是可能改變全球半導體供應鏈競爭格局的新業務模式。」

三大未知APT組織各顯神通

UNK_FistBump組織採用就業主題的釣魚攻擊手法，偽裝成研究生向目標公司的招聘和人力資源部門發送求職郵件。這些郵件很可能來自被入侵的帳戶，內含偽裝成PDF文件的惡意LNK檔案。一旦受害者開啟，將觸發多階段攻擊序列，最終部署Cobalt Strike或名為Voldemort的客製化後門程式。

值得注意的是，雖然Voldemort過去僅被APT41（又稱TA415、Double Dragon、Brass Typhoon）使用，但Proofpoint認為UNK_FistBump與APT41有所區別，因為在載入器和指令控制方法上存在差異。

UNK_DropPitch組織則將攻擊重點轉向大型投資銀行，特別針對從事台灣半導體產業投資分析的專業人士。該組織在2025年4月和5月發送的釣魚郵件中嵌入PDF文件連結，誘使受害者下載包含惡意DLL載荷的ZIP檔案。這個名為HealthKick的後門程式能夠執行指令、捕獲執行結果並將資料外洩至C2伺服器。

在5月下旬的另一次攻擊中，該組織使用相同的DLL側載技術建立TCP反向殼層，與攻擊者控制的VPS伺服器45.141.139[.]222建立連線。這個反向殼層為攻擊者提供了進行偵察和發現步驟的途徑，並可能部署Intel端點管理助手（EMA）進行遠程控制。

UNK_SparkyCarp組織則專精於憑證釣魚攻擊，針對一家未具名的台灣半導體公司使用客製化的中間人（AitM）攻擊套件。該組織於2025年3月發動攻擊，釣魚郵件偽裝成帳戶登入安全警告，包含指向攻擊者控制的憑證釣魚域名accshieldportal[.]com的連結。

除了上述三個組織外，Proofpoint還觀察到**UNK_ColtCentury**（又稱TAG-100和Storm-2077）組織的活動。該組織向台灣半導體組織的法務人員發送表面上無害的郵件，試圖建立信任關係，最終目標是部署名為Spark RAT的遠程存取木馬。

Proofpoint的進一步分析揭示了這些威脅行為者與中國的明確聯繫。**研究人員發現，其中兩台伺服器被配置為SoftEther VPN伺服器，這是一套經常被中國駭客組織採用的開源VPN解決方案**。此外，其中一台C2伺服器重複使用的TLS憑證，過去曾與MoonBounce和SideWalk（又稱ScrambleCross）等惡意軟體家族相關聯。

鹽颱風組織攻擊美國國民警衛隊

值得注意的是，在針對台灣半導體產業展開攻擊的同一時期，另一個中國國家級駭客組織鹽颱風（Salt Typhoon，又稱Earth Estries、Ghost Emperor和UNC2286）也對美國關鍵基礎設施發動了攻擊。雖然這兩起攻擊行動分別由不同威脅組織執行且針對不同目標，但在時間上的重疊現象顯示了中國網路間諜活動正呈現整體升級的態勢。

鹽颱風組織在2024年3月至12月期間，對至少一個美國州的國民警衛隊進行了長達九個月的滲透。

根據美國國防部2025年6月11日的報告，鹽颱風組織「大舉入侵了美國一個州的陸軍國民警衛隊網路，並收集了其網路配置以及與其他美國各州和至少四個美國領土的對應網路的資料流量。」該威脅行為者還外洩了與其他美國政府和關鍵基礎設施實體相關的配置檔案。

戰略意義與未來威脅

台灣的半導體產業不僅是經濟支柱，更是全球科技供應鏈中不可替代的關鍵環節。Proofpoint表示，這些攻擊活動「很可能反映了中國實現半導體自主化和減少對國際供應鏈和技術依賴的戰略優先級，特別是考慮到美國和台灣的出口管制措施。」

SOCRadar的首席資訊安全官Ensar Seker指出，鹽颱風組織對美國國民警衛隊網路維持近一年的存取權限，他強調，「這是網路領域的嚴重升級。這不僅僅是機會主義的入侵，而是反映了有意的長期間諜活動，目的在悄悄提取戰略情報。」

Proofpoint透露，約有15至20家台灣組織（從中型企業到大型跨國企業）成為這些攻擊活動的目標。Proofpoint已通知所有受影響的組織，並表示目前並未發現任何因這些攻擊活動而導致的成功入侵案例。

這些新興威脅行為者持續展現出與中國國家利益一致的長期目標模式，以及歷史上與中國網路間諜活動相關的戰術、技術和程序（TTP）和客製化能力。隨著中美科技競爭持續加劇，台灣半導體產業面臨的網路威脅預計將持續升級，相關企業應加強資訊安全防護措施，特別是針對釣魚攻擊和社交工程手法的防範。

[Quoted text hidden]