Datasheet

ThreatVision

TEAMT5

APT 威脅情資

深度解析亞太 APT 攻擊行動與技術

亞太地區長期是全球網路攻防最激烈的戰場。從鎖定南韓能源業的長期滲透攻擊、入侵東南亞金融供應鏈，到針對台灣高科技業的跨境監控，背後均涉及具備國家級資源的進階持續性威脅（APT）組織。
APT 攻擊具備長期潛伏、精準鎖定、持續演進的特性，能隨情勢快速調整戰術與技術。不僅造成資料外洩與營運中斷，更可能引發地緣政治與經濟層面的連鎖衝擊。在威脅升高下，持續監測、分析與預判 APT 行動已成為防禦成敗的關鍵。

從跡象到脈絡

APT 攻擊不是單一事件，而是由多階段、跨事件行動構成。僅憑片段觀察難以掌握全貌，組織必須整合零散跡象，建立完整脈絡，才能準確識別攻擊者模式與意圖，及早行動防止威脅升級。
ThreatVision「APT 威脅情資」匯聚 TeamT5 在亞太的長期觀察與研究，整合攻擊行為、慣用工具與入侵指標（IoC），提供兼具時效、廣度與深度的情資，協助組織在威脅擴大前制定有效防禦策略。

全方位解構 APT 威脅

ThreatVision 提供三種類型的報告，全方位解析 APT 威脅，滿足組織從即時應變到長期戰略的各階段需求：

APT 威脅情資週報
（APT in Asia Flash Reports，又稱 Flash Report）

提供即時、準確且可執行的 APT 情資，是 TeamT5 團隊的獨家研究成果。每份報告詳細剖析單一 APT 攻擊事件的來龍去脈，同時包含所有關鍵的 IoC，協助組織快速掌握威脅動態，立即部署防禦。
Flash Report 每週發佈兩次，一年至少 100 份。

APT 威脅情資月報
（APT in Asia Monthly Reports，又稱 Monthly Report）

提供可執行的亞太區域策略性情資。每份報告針對 13–16 起 APT 攻擊事件進行深入分析，涵蓋重要 IoC、惡意樣本與基礎架構活動。內容包含威脅趨勢觀察、惡意程式與詳細技術剖析等，協助組織全面掌握威脅動態並制定防禦策略。
Monthly Report 每月發佈一次，一年共 12 份。

APT 威脅族群追蹤季報
（APT Campaign Tracking Reports，又稱 CTR）

深度剖析特定攻擊族群或行動的長期發展軌跡，內容涵蓋過去兩至三年的戰術、技巧與程序（TTP）、攻擊工具與目標範圍，為組織的溯源調查與長期防禦策略奠定基礎。
CTR 每季發佈兩次，一年共 8 份；而第二季與第四季末時，其中一份報告將呈現過去半年內的 APT 威脅概況，涵蓋重大攻擊事件、受害產業與常見攻擊手法等內容。

強化不同層級防禦效能

ThreatVision APT 威脅情資提供不同職能團隊可直接應用的資訊：

安全營運中心與事件應變團隊

即時取得最新 IoC 與 TTP，快速更新規則與封鎖措施，縮短反應時間。

威脅狩獵人員

透過模式關聯與技術分析，識別潛在威脅，精準鎖定可疑活動。

資安長與策略主管

掌握攻擊手法與工具趨勢，據以規劃優先順序與資源配置。

法遵與風險管理人員

結合威脅與地緣政治脈絡，支援合規與風險評估，提升治理效能。

APT 威脅情資的核心價值

從亞太視角連結全球威脅

追蹤中國、俄國、北韓等 APT 行動，結合跨境攻擊模式以評估威脅與風險。

事件與時間的關聯分析

透過週報、月報、季報，將不同時間與事件關聯整合，重建攻擊行動的全貌。

可即時部署的實用工具

提供 IoC 與偵測工具，可直接導入既有系統，加快應變速度。

專家驗證的第一手情資

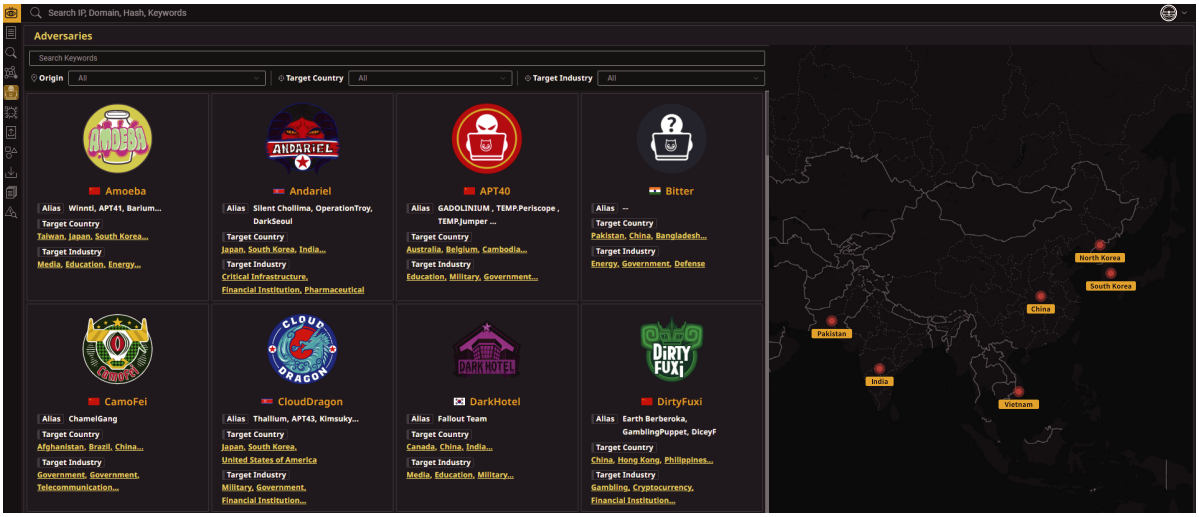
結合 TeamT5 原始遙測數據，經多層驗證，確保精確性與可信度。

在威脅演變中保持優勢

APT 攻擊的戰術與技術持續演進，行為模式也不斷變化。ThreatVision APT 威脅情資結合即時告警、深度分析與可實際運用的技術成果，協助組織同時具備快速反應與長期追蹤能力，在複雜威脅環境中維持防禦韌性與主動權。

ThreatVision 平台一覽

多元情資支援不同角色與任務，協助組織全面掌握攻擊族群的行為模式、預先部署防禦策略，是從資安戰略規劃到第一線防禦的最佳助力。



如何開始使用 ThreatVision

請聯繫 TeamT5 業務並申請 14 天的 ThreatVision 試用帳戶。如果希望了解產品相關的進一步資訊，請發送電子郵件至 sales@teamt5.org。我們期待與您合作，協助您的組織免受網路威脅。

關於 TeamT5

v.202605

廣受全球 550 家以上客戶信賴，橫跨政府單位、科技、製造、金融、醫療、軍事、電信等產業。

頂尖專家團隊

團隊成員常在世界級資安會議中發表最新頂尖研究，包含臺灣 HITCON、美國 Black Hat、日本 Code Blue / AVTOKYO、德國 Troopers，及國際組織辦理的 Hack In The Box 與 FIRST，於威脅情資研究與資安先進技術領域擁有世界領先地位。

外界肯定

獲得美國 Bloomberg 及 CNN、日本產經新聞及朝日新聞、韓國 ET News 等採訪報導。更於 2022 年獲得日本三大巨頭投資，包含日本最大創投 JAFCO 集富集團、日本最大跨國企業並在全球皆有商業投資的 ITOCHU 伊藤忠商事，與日本最大資安解決方案提供商 MACNICA。

Tel 02-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA